



# 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:

Vulnerability: x

bWAPP - Unre x

pastie.org/p/ x

gist.githubuse x


+

-

□

×

← → ↻ ⚠ Not secure 192.168.13.25/vulnerabilities/exec/# ☆ 🗄 📄 J ⋮



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

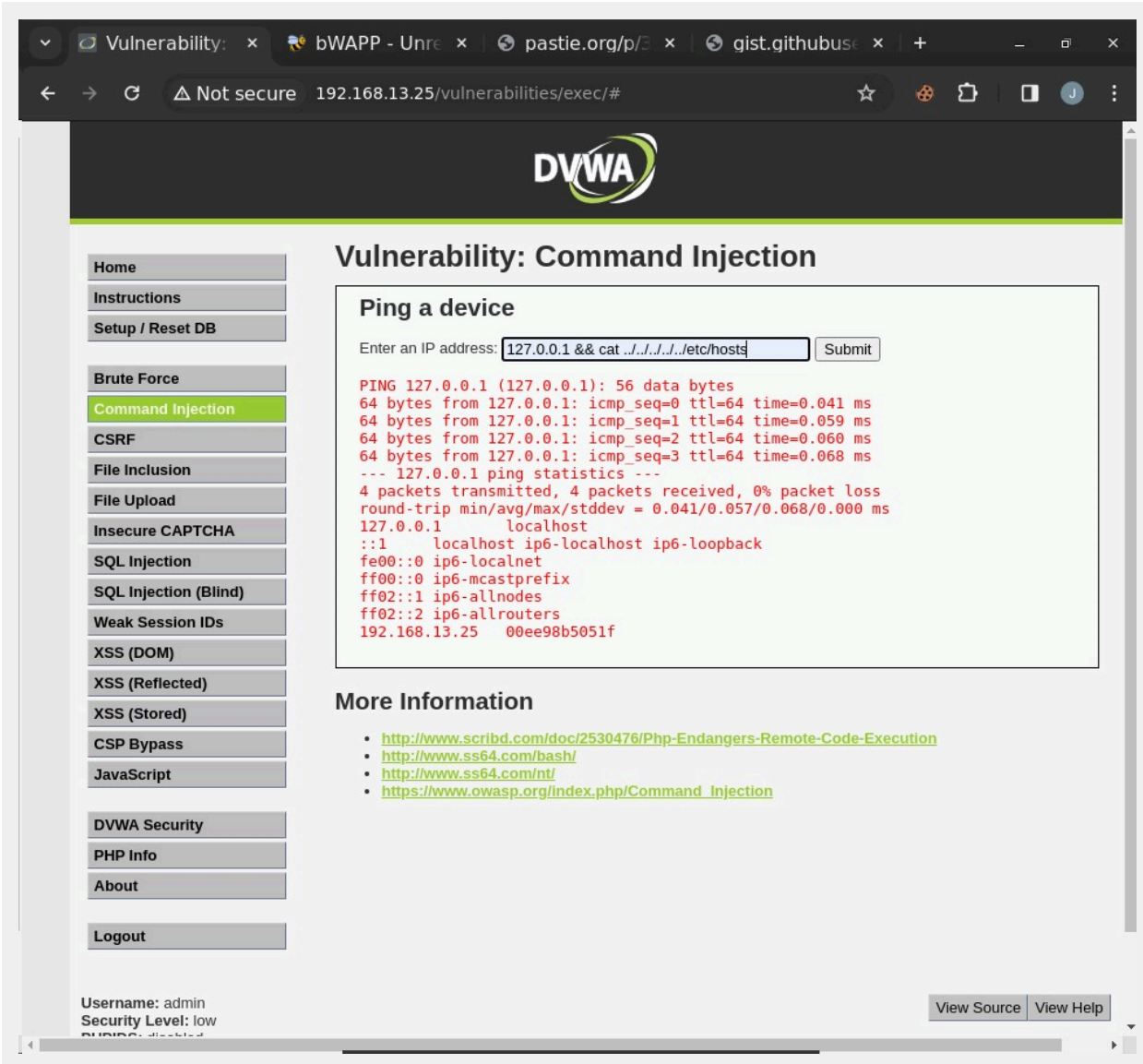
### Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.042 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.065 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.042/0.057/0.066/0.000 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](https://www.owasp.org/index.php/Command_Injection)



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

Create a server side validation limiting the types of allowed characters to #s and the period. This would prevent someone from being able to type in the necessary commands for this exploit. The confidential data could also be housed in a separate server from the web app so that even if the exploit were attempted, the data would not be there to take.

## Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

5. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file

AttackSaveColumns

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
75	tonystark	I am Iron Man	200			11827	
0			200			11801	
1	superman	Up, up and away!	200			11801	
2	loislane	Up, up and away!	200			11801	
3	spiderman	Up, up and away!	200			11801	
4	jennyjones	Up, up and away!	200			11801	
5	tonystark	Up, up and away!	200			11801	
6	timtom	Up, up and away!	200			11801	
7	peterparker	Up, up and away!	200			11801	
8	clarkkent	Up, up and away!	200			11801	
9	michaelsmith	Up, up and away!	200			11801	
10	henryhacker	Up, up and away!	200			11801	
11	superman	Avengers Assemble	200			11801	
12	loislane	Avengers Assemble	200			11801	
13	spiderman	Avengers Assemble	200			11801	

RequestResponse

PrettyRawHexRender

BugsChange PasswordCreate UserSet Security LevelResetCreditsBlogLogout

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

Login

Successful login! You really are Iron Man :)

Finished

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

To mitigate the likelihood of a brute force attack in this scenario, I would recommend a lockout after 3 failed attempts, requirement of multi-factor authentication, and require all employees to change passwords as soon as it was known this list was leaked. The combination of MFA and lockout should all but eliminate this risk.

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

Provide a screenshot confirming that you successfully completed this exploit:

BeEF Control Panel x Vulnerability: Stored x +

127.0.0.1:3000/ui/panel#id=sKWF7jSy0mNkyH8P0sPMbPiPWk91mg61Xg...

BeEF 0.5.4.0 | [Submit Bug](#) | [Logout](#)

Hooked Browsers

- Online Browsers
  - 192.168.13.1
- Offline Browsers
  - 127.0.0.1
    - 192.168.13.1
    - 192.168.13.1

Getting Started | Logs | **Commands** | Proxy | XssRays | Network

Details | Logs | **Commands** | Proxy | XssRays | Network

**Module Tree**

Search

- Exploits (110)
- Host (24)
- IPEC (9)
- Metasploit (1)
- Misc (20)
- Network (24)
- Persistence (9)
- Phonegap (16)
- Social Engineering (24)
  - Text to Voice
  - Clickjacking
  - Lcamtuf Download
  - Spoof Address Bar (data
  - Clippy
  - Fake Flash Update
  - Fake Notification Bar

**Module Results History**

id	date	label
0	2023-12-16 21:43	command 1

**Command results**

- Sat Dec 16 2023 21:43:52 GMT+0000 (Coordinated Universal Time)  
**data:** result=Notification has been displayed
- Sat Dec 16 2023 21:43:55 GMT+0000 (Coordinated Universal Time)  
**data:** result=User has clicked the notification

BeEF Control Panel x Vulnerability: Stored x +

127.0.0.1:3000/ui/panel#id=sKWF7jSy0mNkyH8P0sPMbPiPWk91mg61Xg...

BeEF 0.5.4.0 | [Submit Bug](#) | [Logout](#)

Hooked Browsers

- Online Browsers
  - 192.168.13.1
- Offline Browsers
  - 127.0.0.1
    - 192.168.13.1
    - 192.168.13.1

Getting Started | Logs | **Commands** | Proxy | XssRays | Network

Details | Logs | **Commands** | Proxy | XssRays | Network

**Module Tree**

Search

- Browser (58)
- Chrome Extensions (6)
- Debug (9)
- Exploits (110)
- Host (24)
- IPEC (9)
- Metasploit (1)
- Misc (20)
- Network (24)
- Persistence (9)
- Phonegap (16)
- Social Engineering (24)
  - Text to Voice
  - Clickjacking
  - Lcamtuf Download
  - Spoof Address Bar (data
  - Clippy
  - Fake Flash Update
  - Fake Notification Bar
  - Fake Notification Bar (Cr
  - Fake Notification Bar (Fir
  - Fake Notification Bar (IE)
  - Google Phishing
  - Pretty Theft

**Module Results History**

id	date	label
0	2023-12-16 21:43	command 1

**Command results**

- Sat Dec 16 2023 21:43:20 GMT+0000 (Coordinated Universal Time)  
**data:** answer=admin:password

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

One way to mitigate this vulnerability would be server side validation limiting the type of characters that can be entered in this field. For example, allow letters, numbers, and very specific special characters. Specifically, the < & / should not be included in those characters allowed. You could also use http response headers to prevent a malicious script from being able to run.