



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*

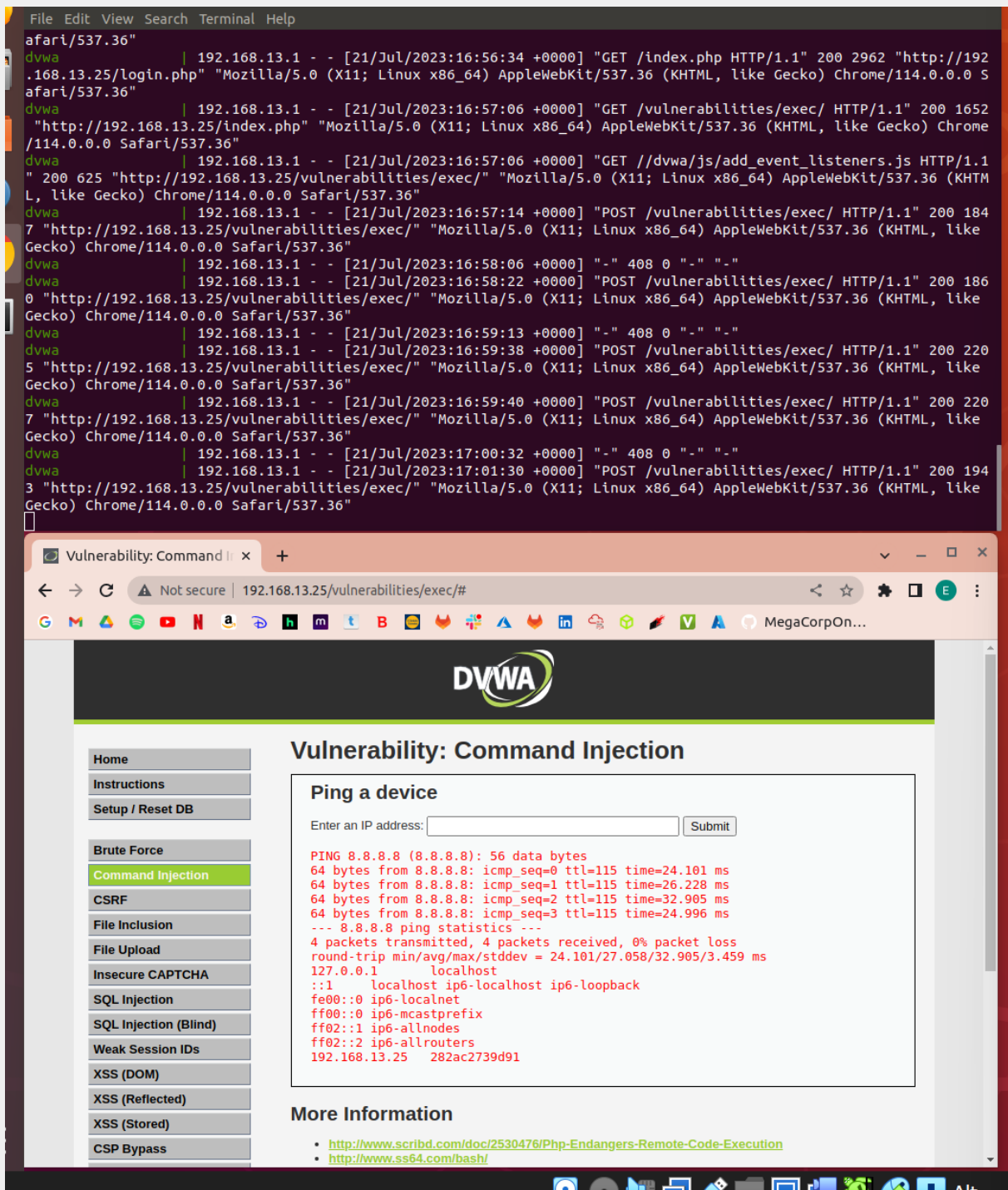
Provide a screenshot confirming that you successfully completed this exploit:

it

The screenshot shows a Linux desktop environment. The top panel includes icons for the Dash, Home, and Applications menus, along with a system status area showing the date and time. The main workspace contains two windows:

- Terminal Window:** Displays a series of network traffic logs. The logs show HTTP requests and responses between a client (192.168.13.1) and a server (192.168.13.25). The requests include GET requests for /login.php, /index.php, /vulnerabilities/exec/, and /vulnerabilities/exec/ HTTP/1.1. The responses show status codes (200, 2962, 200, 187, 200, 187, 200, 225, 200, 225) and headers (Mozilla/5.0, AppleWebKit/537.36, Chrome/114.0.0.0, Safari/537.36).
- Web Browser Window:** Displays the DVWA (Damn Vulnerable Web Application) interface. The browser's address bar shows the URL `192.168.13.25/vulnerabilities/exec/#`. The page title is "Vulnerability: Command Injection". The left sidebar contains a list of navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), 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, and About. The main content area shows the "Ping a device" section, which includes a text input field for "Enter an IP address:" and a "Submit" button. Below the input field, the output of a ping command is displayed:

```
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=25.804 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=28.398 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=48.742 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=27.077 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 25.804/32.505/48.742/9.419 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:Mail 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
```



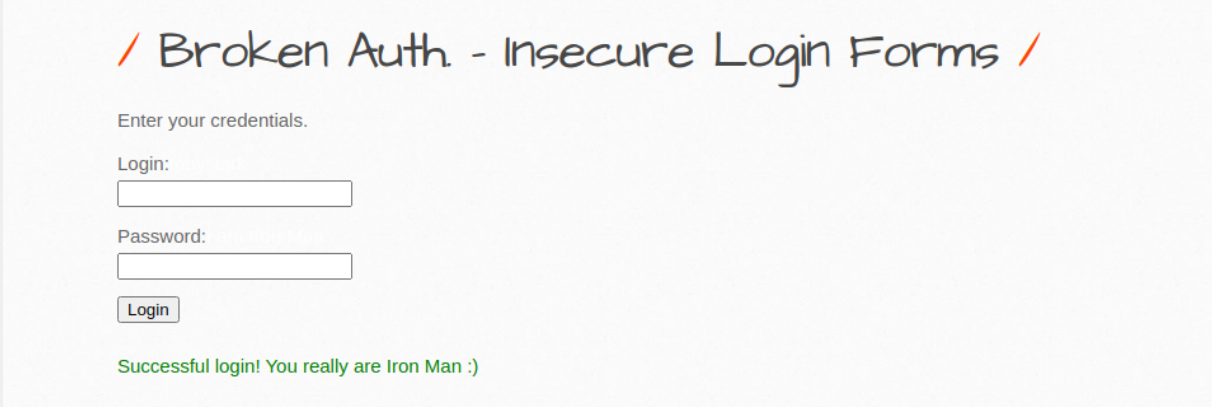
8.8.8.8 && cat <file>

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

To mitigate this issue, user inputs should be monitored and sanitized. Disallowing script like language, and commands.

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

Provide a screenshot confirming that you successfully completed this exploit:



The screenshot shows a web application interface with a title in a handwritten font: */ Broken Auth - Insecure Login Forms /*. Below the title, it says "Enter your credentials." followed by two input fields labeled "Login:" and "Password:". A "Login" button is positioned below the password field. At the bottom, a green message reads: "Successful login! You really are Iron Man :)".

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

Improving password security, making them longer and more complex would help mitigate this issue. Multi factor authentication would also decrease this risk.

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

Provide a screenshot confirming that you successfully completed this exploit:

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: Stored Cross Site Scripting (XSS)

Name *
Message *

Sign Guestbook

Clear Guestbook

Name: test
Message: This is a

Name: Emily
Message:

More Information

- <https://owasp.org/secure-wiki/>
- <https://owasp.org/secure-wiki/>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:

Log in

Username: admin

Security Level: low

View Source

View Help

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

Getting Started

Logs

Zombies

Current Browser

Details

Logs

Commands

Proxy

XssRays

Network

Module Tree

Module Results History

Command results

Hooked Browsers

Online Browsers

192.168.13.1

192.168.13.1

Offline Browsers

192.168.13.1

192.168.13.1

Browser (58)

Chrome Extensions (6)

Debug (9)

Exploits (110)

Host (24)

Detect Antivirus

Detect CUPS

Detect Coupon Printer

Detect Google Desktop

Get Geolocation (Third-Party)

Hook Default Browser

Get Geolocation

Get System Info (Java)

Get Wireless Keys

Hook Microsoft Edge

id

date

label

0

2023-08-19 00:04

command 1

1

2023-08-19 00:04

command 2

2

2023-08-19 00:05

command 3

1

Fri Aug 18 2023 20:05:00 GMT-0400 (Eastern Daylight Time)

data: result=[{"status":"success","country":"United States","countryCode":"US","region":"CA","regionName":"California","zip":"94109","lat":37.7958,"lon":-122.4203,"time":1692444300,"org":"Comcast Cable Communications, LLC","as":"AS33651 Comcast Cable Communications, LLC","query":"24.7.56.39"}]

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

To mitigate this issue, user inputs should be monitored and sanitized. Disallowing script like language, and commands.

