



# 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:

The screenshot displays the DVWA web application interface. The top header features the DVWA logo. On the left, a sidebar contains a list of navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, and SQL Injection (Blind). The main content area is titled "Vulnerability: Command Injection". Below this title, there is a section "Ping a device" with a form that says "Enter an IP address:" followed by a text input field containing "127.0.0.1 && pwd" and a "Submit" button. Below the form, the output of the command injection is displayed in red text: "PING 127.0.0.1 (127.0.0.1): 56 data bytes", followed by four lines of ping results showing 64 bytes from 127.0.0.1 with various icmp\_seq and time values. This is followed by a summary line: "4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max/stddev = 0.039/0.053/0.066/0.000 ms". The final line of the output is the command executed: "/var/www/html/vulnerabilities/exec". At the bottom of the main content area, there is a link labeled "More Information".



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

## 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=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.066 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.044/0.055/0.066/0.000 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: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
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
```



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)

## 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=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.041/0.052/0.063/0.000 ms
127.0.0.1      localhost
::1           localhost ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
192.168.13.25 253225506c21
```

### More Information

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

Some strategies to help mitigate this type of vulnerability: Input Validation and Sanitization, Parameterized Queries and Prepared Statements, Whitelisting, Application Firewalls, Regular Security Testing and Continuous Monitoring.

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

Provide a screenshot confirming that you successfully completed this exploit:

VulnerabilitybWAPP - PortbWAPP - Bx

FoxyProxy L

192.168.13.35/ba\_insecure\_login\_1.php

 Choose your bug:  
----- bWAPP v1.9+ ----- Hack

Set your security level:  
low Set Current: low

an extremely buggy web app!

BugsChange PasswordCreate UserSet Security LevelResetCredits

# / Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

Login

SequencerDashboard2 x5 x...DecoderTargetProxyIntruderProject optionsRepeaterUser options

PositionsPayloadsResource PoolOptions

Choose an attack typeStart attack

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.13.35

Update Host header to match target

Add SClear SAuto SRefresh

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:109.0) Gecko/20100101 Firefox/119.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;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: 28

9 Origin: http://192.168.13.35

10 Connection: close

11 Referer: http://192.168.13.35/ba\_insecure\_login\_1.php

12 Cookie: PHPSESSID=jncuq4ke4iopbmme2lu3s4b4; security\_level=0

13 Upgrade-Insecure-Requests: 1

14

15 Login=\$test-user&password=\$test-password&form=submit

1 x2 x...

SequencerDashboard

Decoder

ComparerTarget

LoggerProxy

Extender

Project optionsIntruder

User optionsRepeater

Positions

Payloads

Resource Pool

Options

?

Payload Sets

Start attack

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:2

Payload count:11

Payload type:Simple list

Request count:0

?

Payload Options [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

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.

Enter a new item



Hooked Browsers

Online Browsers

127.0.0.1

🔍 📄 📄 192.168.13.1

Offline Browsers

BasicRequester

Getting StartedLogsZombiesCurrent Browser

DetailsLogsCommandsProxyXssRaysNetwork

Module Tree

Search

Metasploit (1)

Misc (20)

Network (24)

Persistence (9)

Phoneygap (16)

Social Engineering (24)

Text to Voice

Clickjacking

Lcamtuf Download

Spoof Address Bar (data UR)

Clippy

Fake Flash Update

Fake Notification Bar

Fake Notification Bar (Chrom

Fake Notification Bar (Firefo

Fake Notification Bar (IE)

Google Phishing

Pretty Theft

Replace Videos (Fake Plugi

Simple Hijacker

TabNabbing

Edge WScript WSH Injection

Fake Evernote Web Clipper

Fake LastPass

Firefox Extension (Bindshell

Firefox Extension (Dropper)

Firefox Extension (Reverse

HTA PowerShell

SiteKiosk Breakout

User Interface Abuse (IE 9/1

Module Results History

iddatelabel

The results from executed command modules will be listed here.

Google Phishing

Description: This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will show the Google favicon and a Gmail phishing page (although the URL is NOT the Gmail URL).

Id: 163

XSS hook URI: http://0.0.0.0

Gmail logout interval (ms): 10000

Redirect delay (ms): 1000

Execute

Ready



127.0.0.1:3000/demos/butcher/index.html



New to Google Mail?

[CREATE AN ACCOUNT](#)

## Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:



### Lots of space

Over 2757.272164 megabytes (and counting) of free storage.



### Less spam

Keep unwanted messages out of your inbox.



### Mobile access

Get Google Mail on your mobile phone. [Learn more](#)

[About Google Mail](#)

[New features!](#)

[Switch to Google Mail](#)

[Create an account](#)



### Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?

Get business email, calendar, and online docs @your\_company.com.

[Learn more](#)

### Sign in

**Username**

**Password**

[Sign in](#)

☐ Stay signed in

[Can't access your account?](#)



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

Getting Started | Logs | Zombies | **Current Browser**

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

**Module Tree**

Search

- Metasploit (1)
- Misc (20)
- Network (24)
- Persistence (9)
- Phoneygap (16)
- Social Engineering (24)**
  - Text to Voice
  - Clickjacking
  - Lcamtuf Download
  - Spoof Address Bar (data URI)
  - Clippy
  - Fake Flash Update
  - Fake Notification Bar
  - Fake Notification Bar (Chrome)
  - Fake Notification Bar (Firefox)
  - Fake Notification Bar (IE)
  - Google Phishing
  - Pretty Theft
  - Replace Videos (Fake Plugins)
  - Simple Hijacker
  - TabNabbing
  - Edge WScript WSH Injection
  - Fake Evernote Web Clipper

**Module Results History**

id	date	label
0	2023-11-06 04:35	command 1
1	2023-11-06 04:35	command 2

**Command results**

1 Mon Nov 06 2023 04:36:45 GMT+0000 (Coordinated Universal Time)  
**data:** result=Username: hackeruser Password: hackerpass

192.168.13.25/vulnerabilities/xss\_s/

**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](#)

**Vulnerabilities**

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

Name: test  
Message: This is a test comment.

Name: Bob  
Message:

← → ↻ 127.0.0.1:3000/ui/panel#id=AAyH3nPDZg9CgdC9MCJl

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

Hooked Browsers

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

Getting Started | Logs | **Zombies** | **Current Browser**

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

**Module Tree**

Search

- 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
  - Lcamituf Download
  - Spoof Address Bar (data UR)
  - Clippy
  - Fake Flash Update
  - Fake Notification Bar
  - Fake Notification Bar (Chrom
  - Fake Notification Bar (Firefo
  - Fake Notification Bar (IE)
  - Google Phishing
  - Pretty Theft
  - Replace Videos (Fake Plugi
  - Simple Hijacker
  - TabNabbing
  - Edge WScript WSH Injection

**Module Results History**

id	date	label
0	2023-11-06 04:51	command 1

**Command results**

1	Mon Nov 06 2023 04:52:46 GMT+0000 (Coordinated Universal Time) <b>data:</b> answer=bob@email.com:cybersecurity
---	--

← → ↻ 192.168.13.25/vulnerabilities/xss\_s/

This website wants to run the following applet: 'java' from 'Microsoft Inc.'. To continue using this website you must accept the following security popup

**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

## Vulnerability: Stored Cross Site Scripting (XSS)

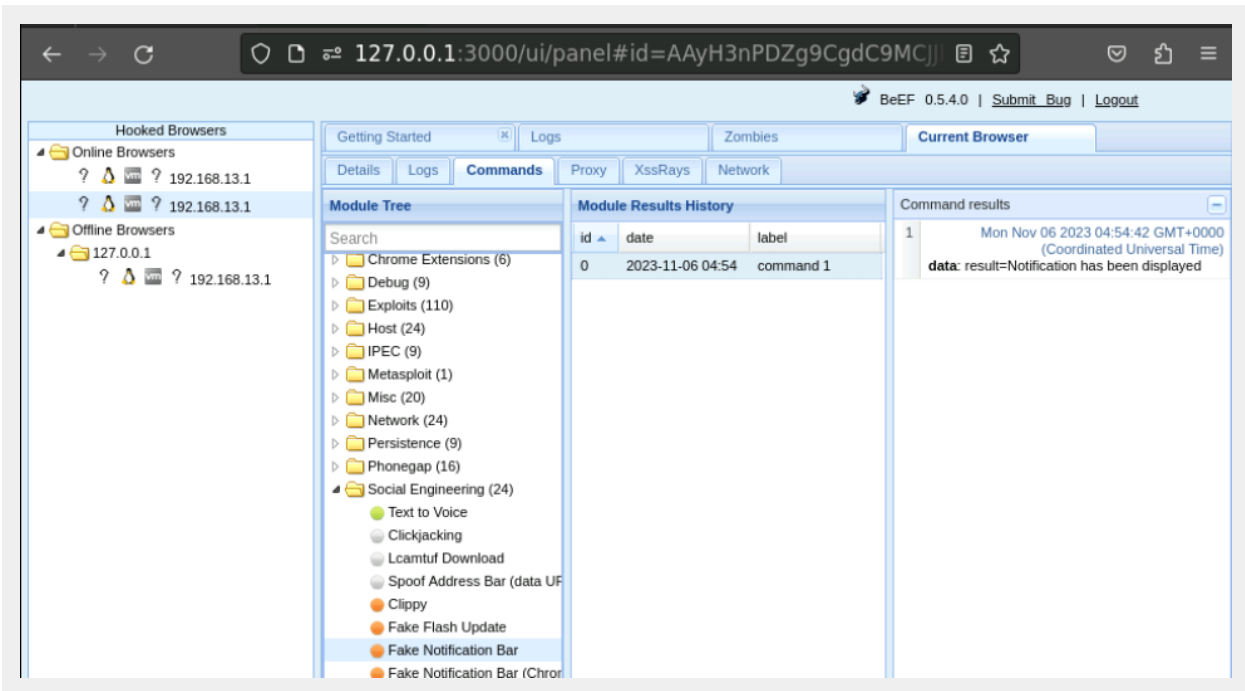
Name \*

Message \*

Sign Guestbook Clear Guestbook

Name: test  
Message: This is a test comment.

Name: Bob  
Message:



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

We can implement Web Application Security: Regularly test and secure your web applications against common vulnerabilities, such as Cross-Site Scripting and Cross-Site Request Forgery, which can be exploited by BeEF. Implement a CSP for your web applications. Ensure that you have updated antivirus and anti-malware software installed on your systems. Use network firewalls and IDPS to detect and block unauthorized network traffic, including traffic generated by BeEF. Deploy a Web Application Firewall to detect and mitigate malicious traffic, including requests originating from BeEF.