Cybersecurity

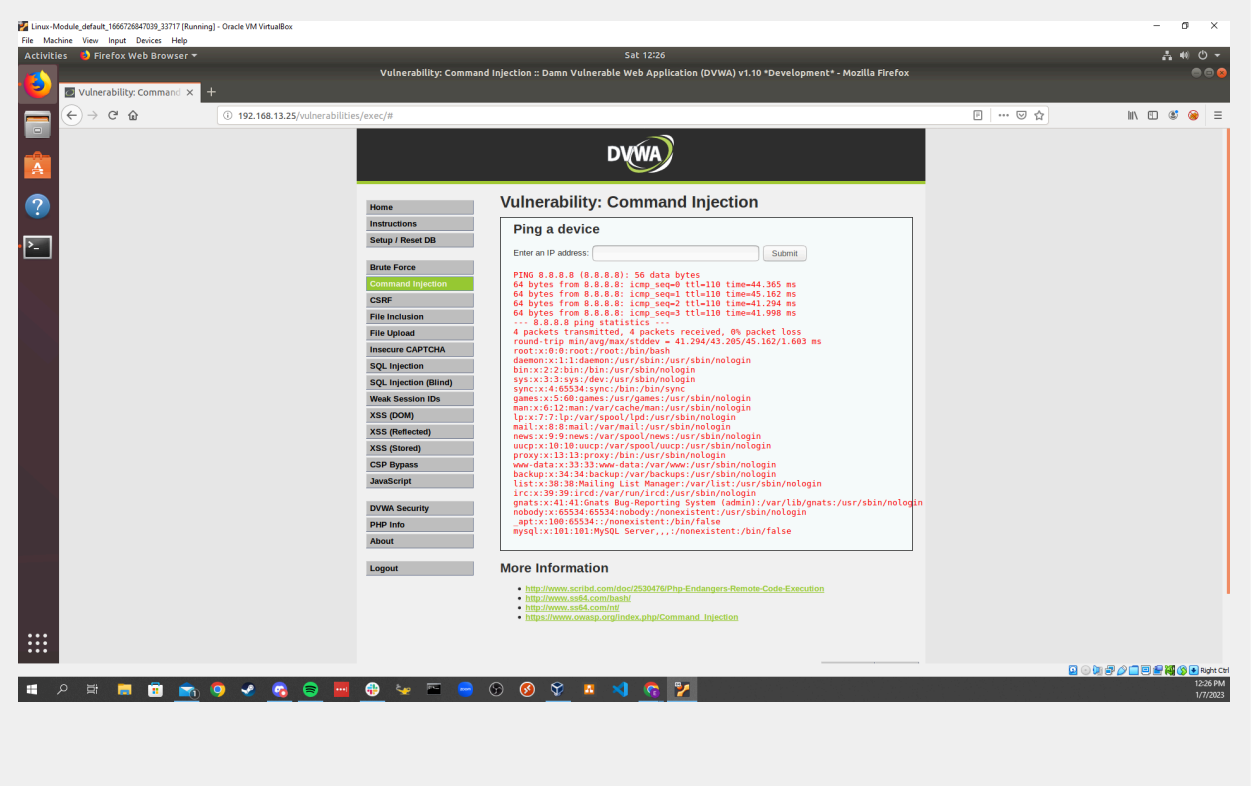
Module 15 Challenge Submission File

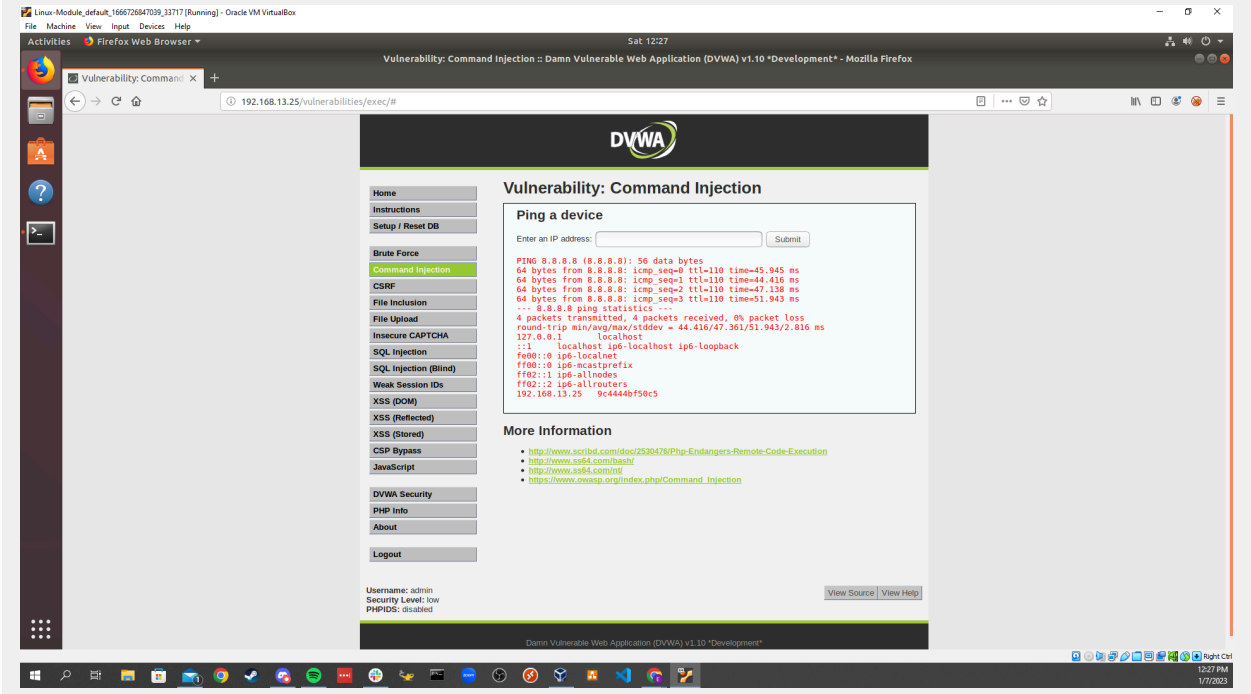
Testing Web Applications for Vulnerabilities

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:



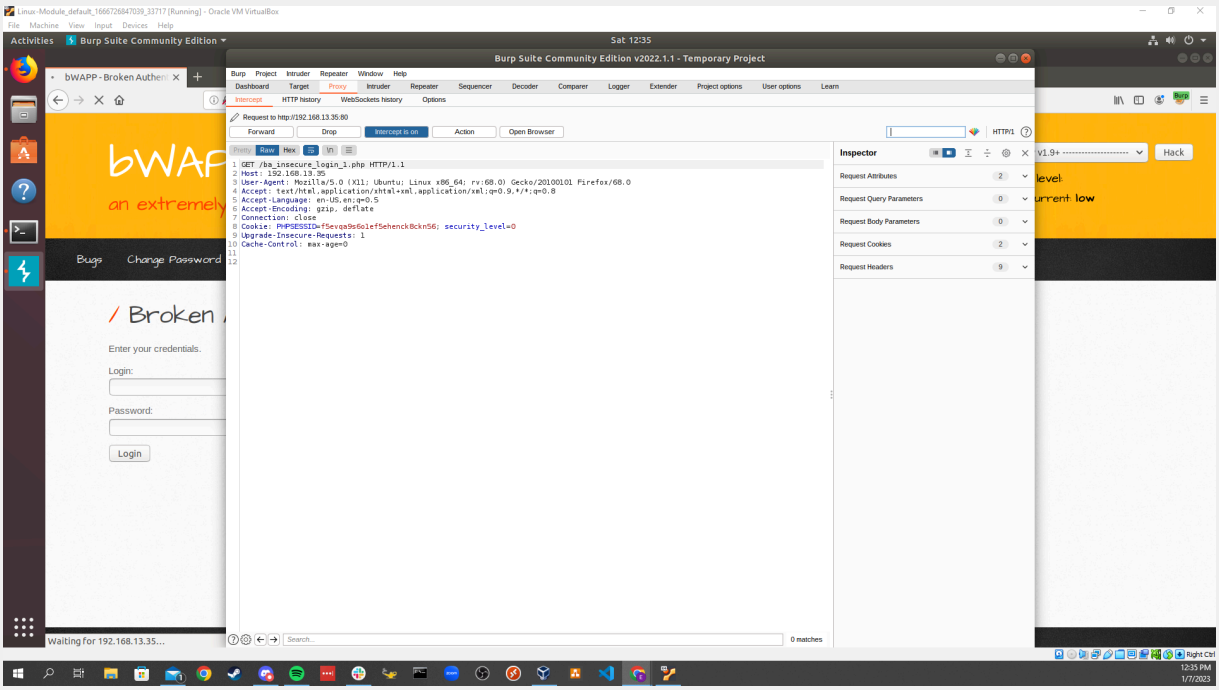


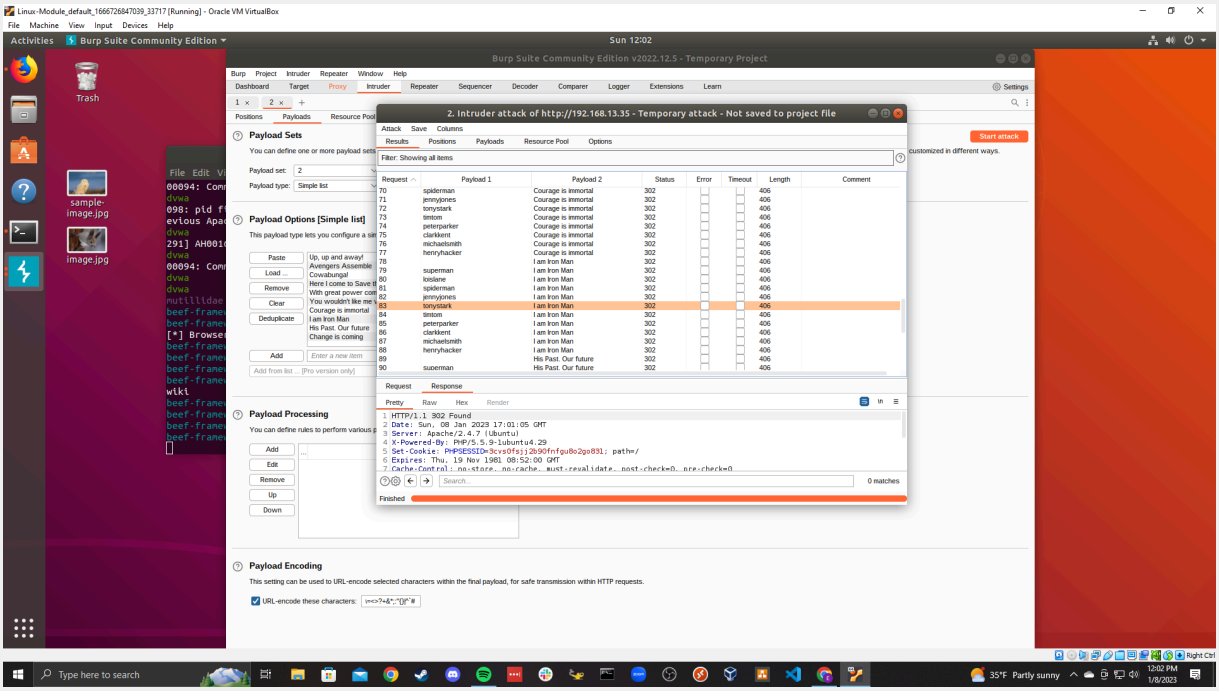
Write two or three sentences outlining mitigation strategies for this vulnerability:

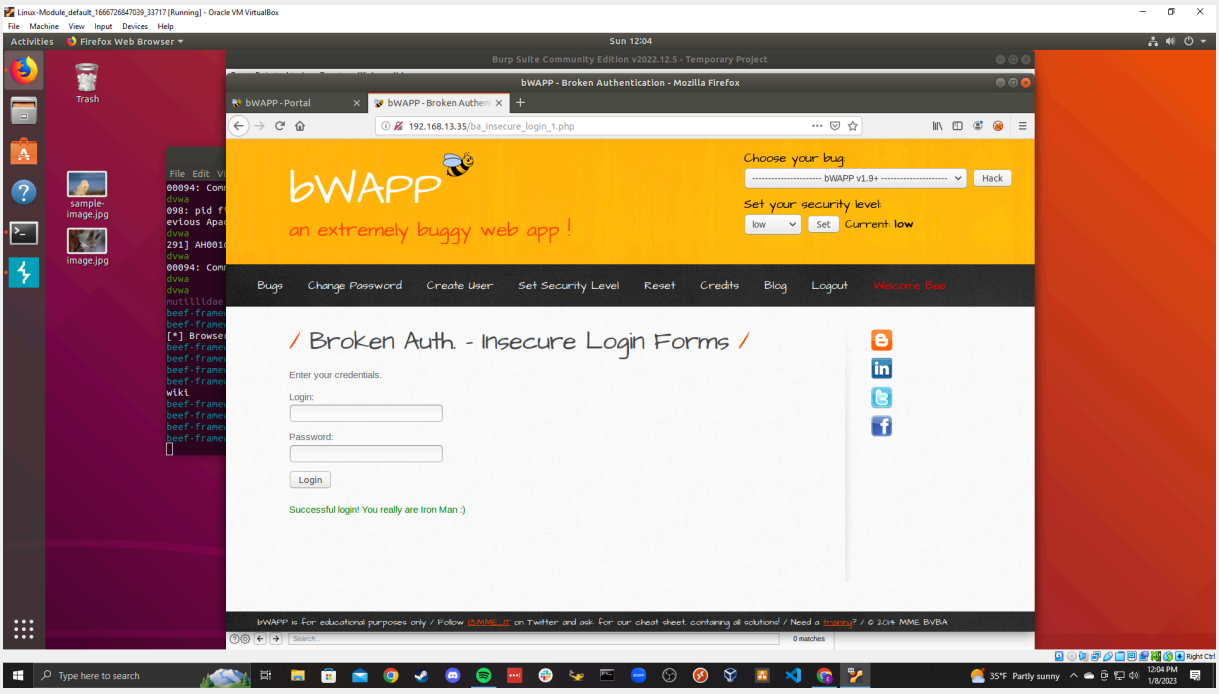
```
The first way to combat a command injection is to prevent user input as much as possible. Also, to have automatic testing be ran to prevent unwanted characters.
```

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

Provide a screenshot confirming that you successfully completed this exploit:


Linux-Module_default_1666726847039_33717 [Running] - Oracle VM VirtualBox
Activities
Burp Suite Community Edition
Sat 12:35
Burp Suite Community Edition v2022.1.1 - Temporary Project
bWAPP - Broken Authen
Request to http://192.168.13.35:80
Forward
Drop
Intercept is on
Action
Open Browser
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Hack
Bugs
Change Password
Enter your credentials.
Login:
Password:
Login
Waiting for 192.168.13.35...
0 matches


Linux-Module_default_1666726847039_33717 [Running] - Oracle VM VirtualBox
Activities
Burp Suite Community Edition
Sun 12:02
Burp Suite Community Edition v2022.12.5 - Temporary Project
Trash
sample-image.jpg
image.jpg
2. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Start attack
Finished
Type here to search
35°F Partly sunny

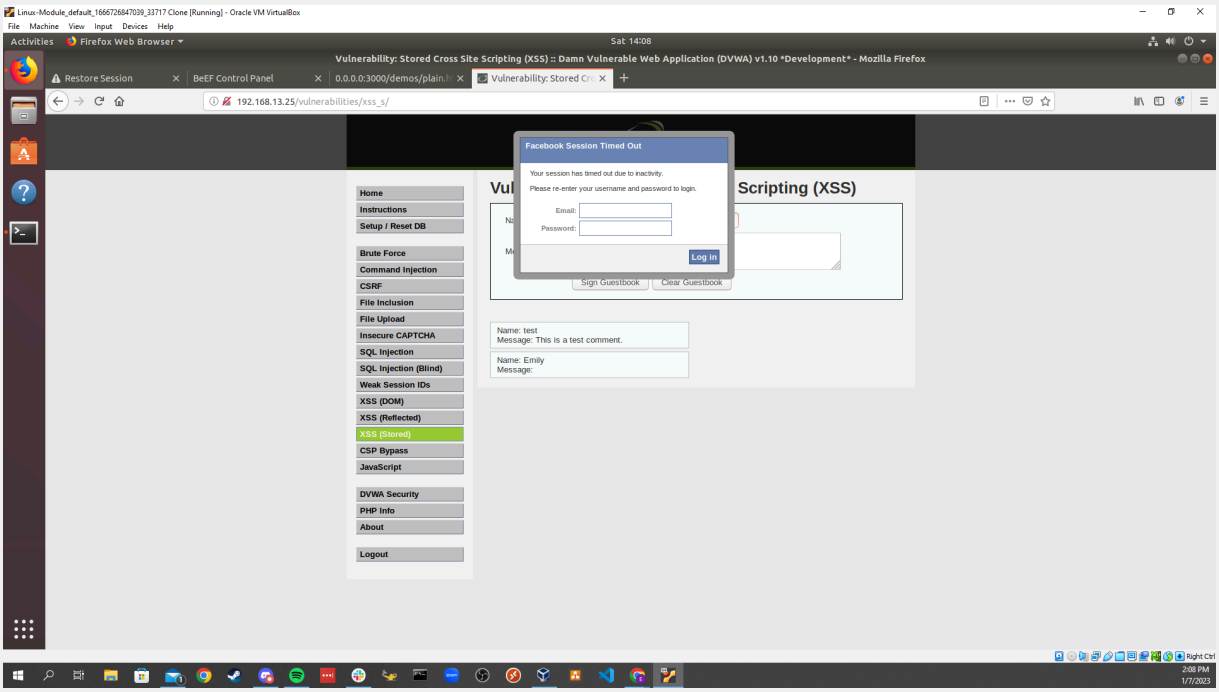


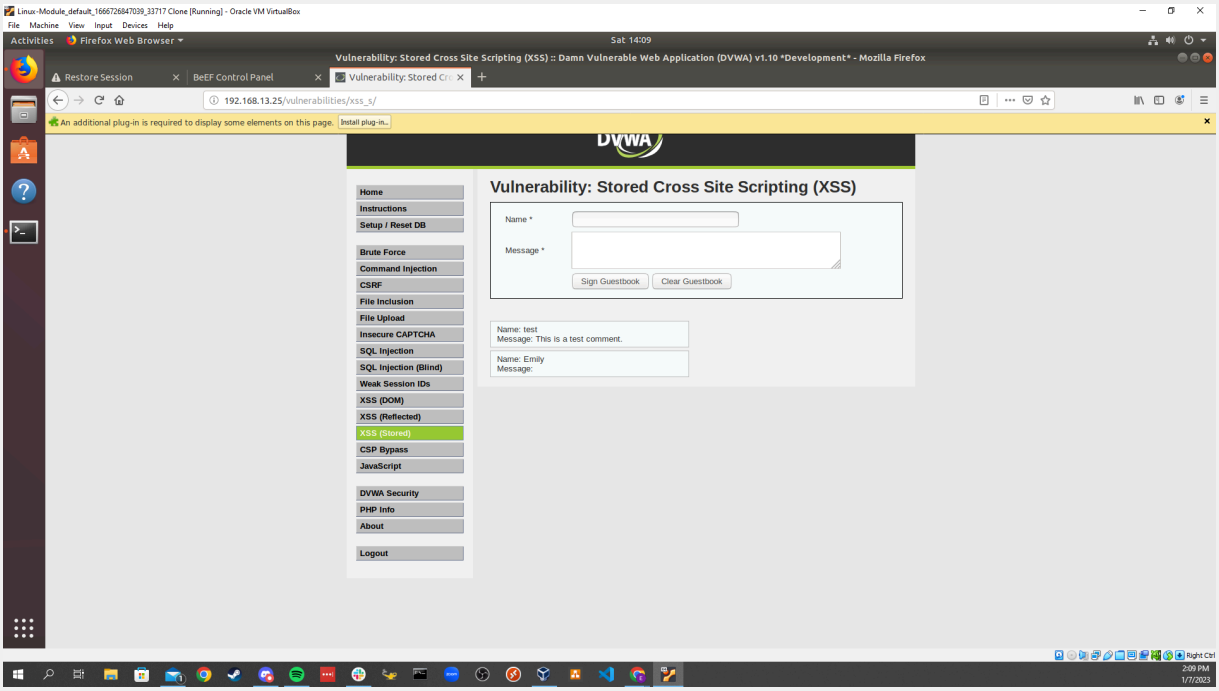
Write two or three sentences outlining mitigation strategies for this vulnerability:

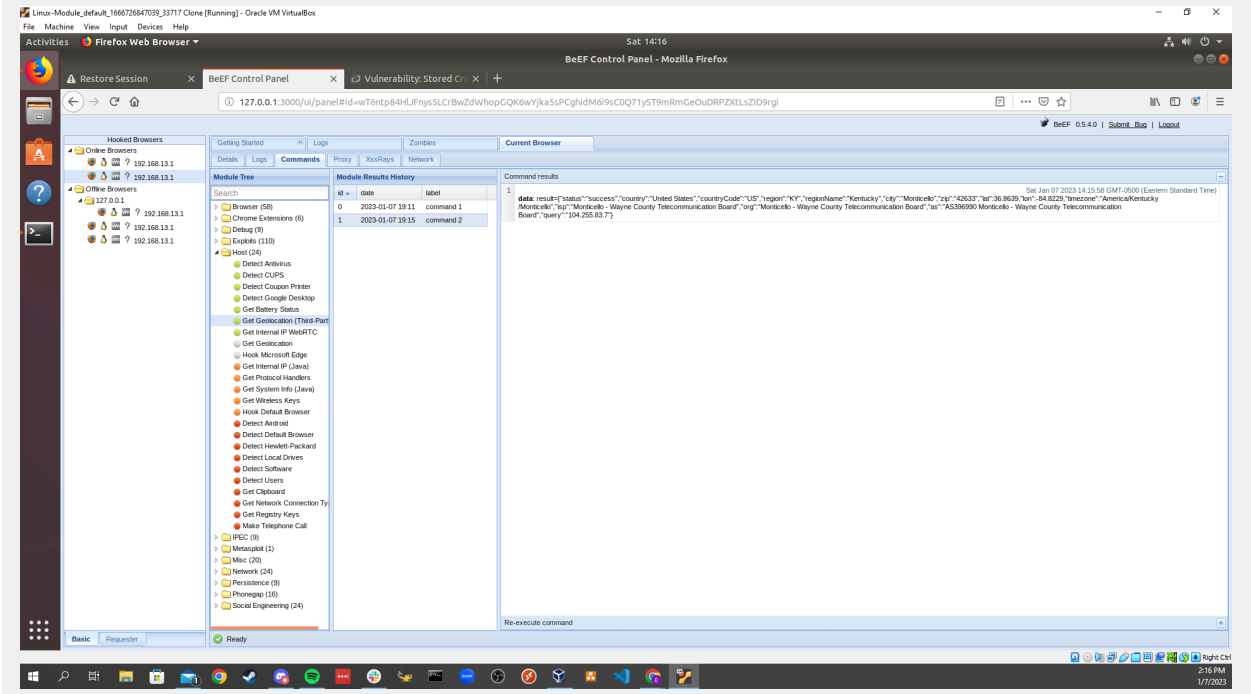
```
There are many ways to mitigate brute force. The main one is to use strong
passwords. Another way would be to use two factor authentication. Also,
limiting login attempts could prevent brute force.
```

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

Provide a screenshot confirming that you successfully completed this exploit:


Linux-Module_default_1666726847039_33717 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Sat 14:08
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Restore Session
BeEF Control Panel
0.0.0.0:3000/demos/plain.h
Vulnerability: Stored Cr
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
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
Scripting (XSS)
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: Emily
Message:
Right Ctrl
2:08 PM
1/7/2023


Linux-Module_default_1666726847039_33717 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Sat 14:09
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Restore Session
BeEF Control Panel
Vulnerability: Stored Cr
192.168.13.25/vulnerabilities/xss_s/
An additional plug-in is required to display some elements on this page.
Install plug-in...
DVWA
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 test comment.
Name: Emily
Message:
Right Ctrl
2:09 PM
1/7/2023



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

```
A way to mitigate cross site scripting would be to limit what someone can do. Also, to validate what is being added to make sure it is correct. The final way would be to remove all unwanted data.
```