Cybersecurity

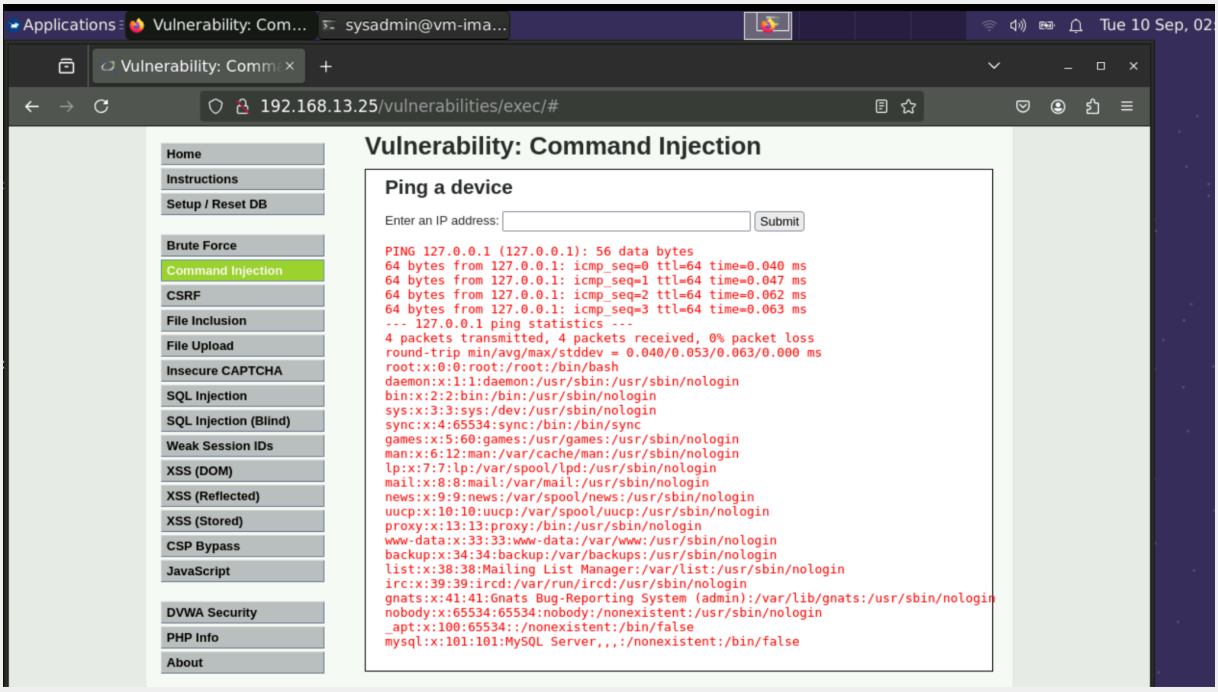
Module 15 Challenge Submission File

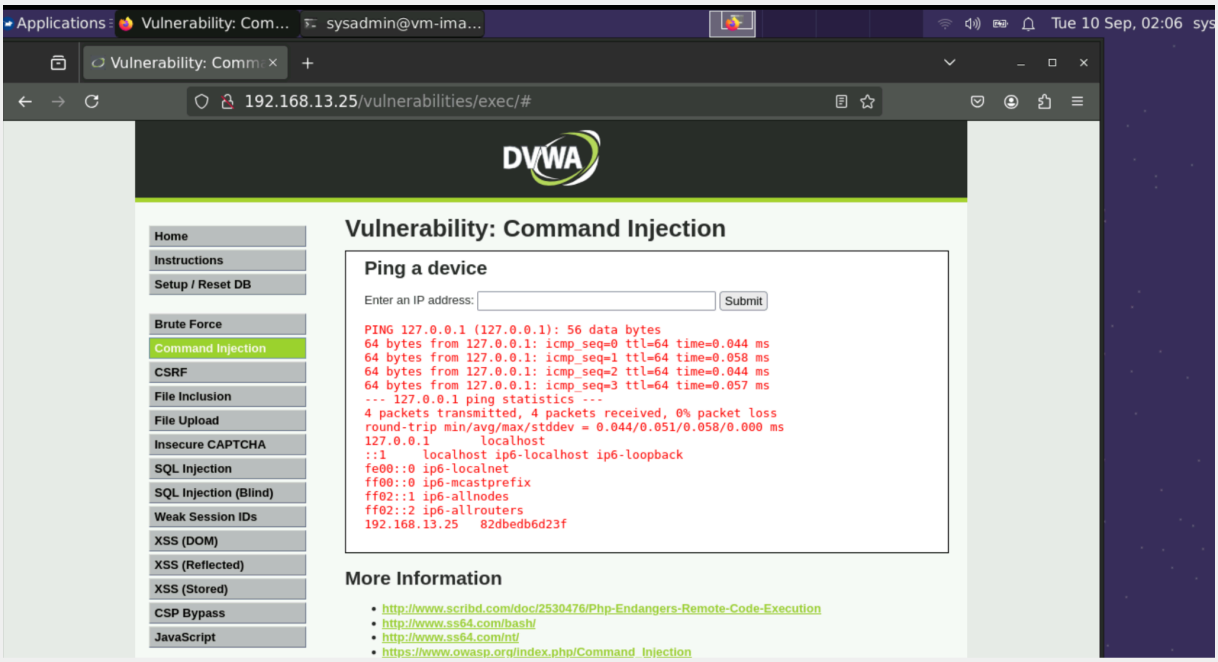
Testing Web Applications for Vulnerabilities

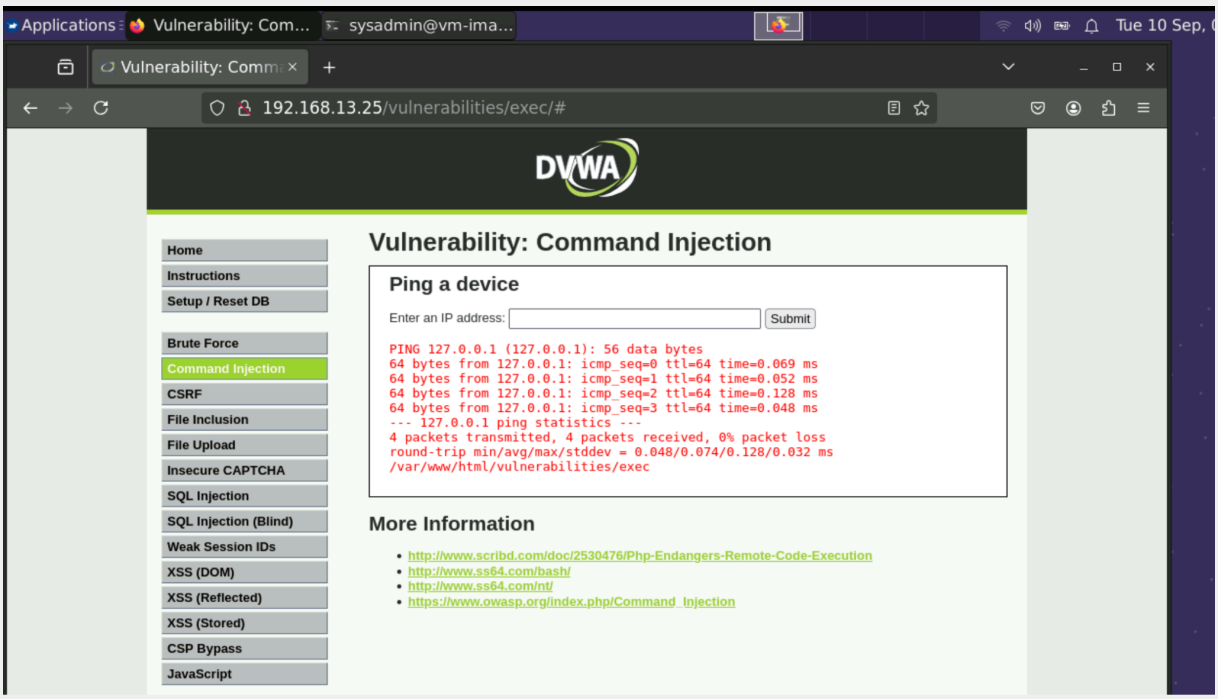
Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

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

Provide a screenshot confirming that you successfully completed this exploit:


Applications
Vulnerability: Com...
sysadmin@vm-ima...
Tue 10 Sep, 02
Vulnerability: Comm
192.168.13.25/vulnerabilities/exec/#
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:
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=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.047 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=0.063 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.040/0.053/0.063/0.000 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


Applications
Vulnerability: Com...
sysadmin@vm-ima...
Tue 10 Sep, 02:06
Vulnerability: Comm
192.168.13.25/vulnerabilities/exec/#
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
Vulnerability: Command Injection
Ping a device
Enter an IP address:
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=0.044 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=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.044/0.051/0.058/0.000 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 82dbedb6d23f
More Information
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://www.owasp.org/index.php/Command_Injection

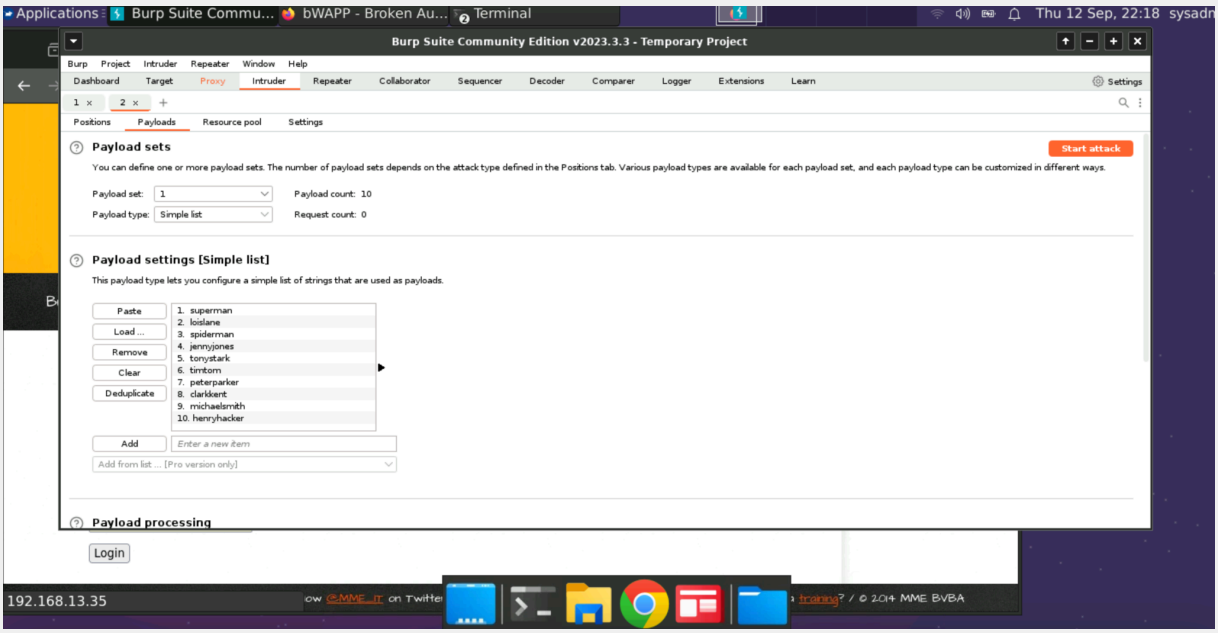


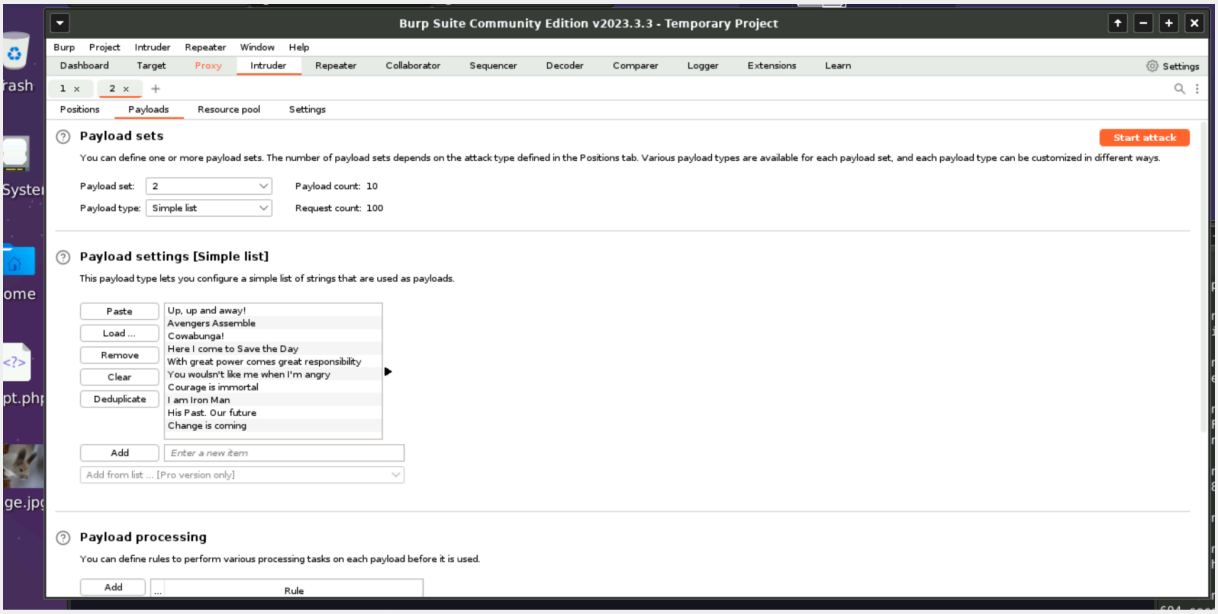
Write two or three sentences outlining mitigation strategies for this vulnerability:

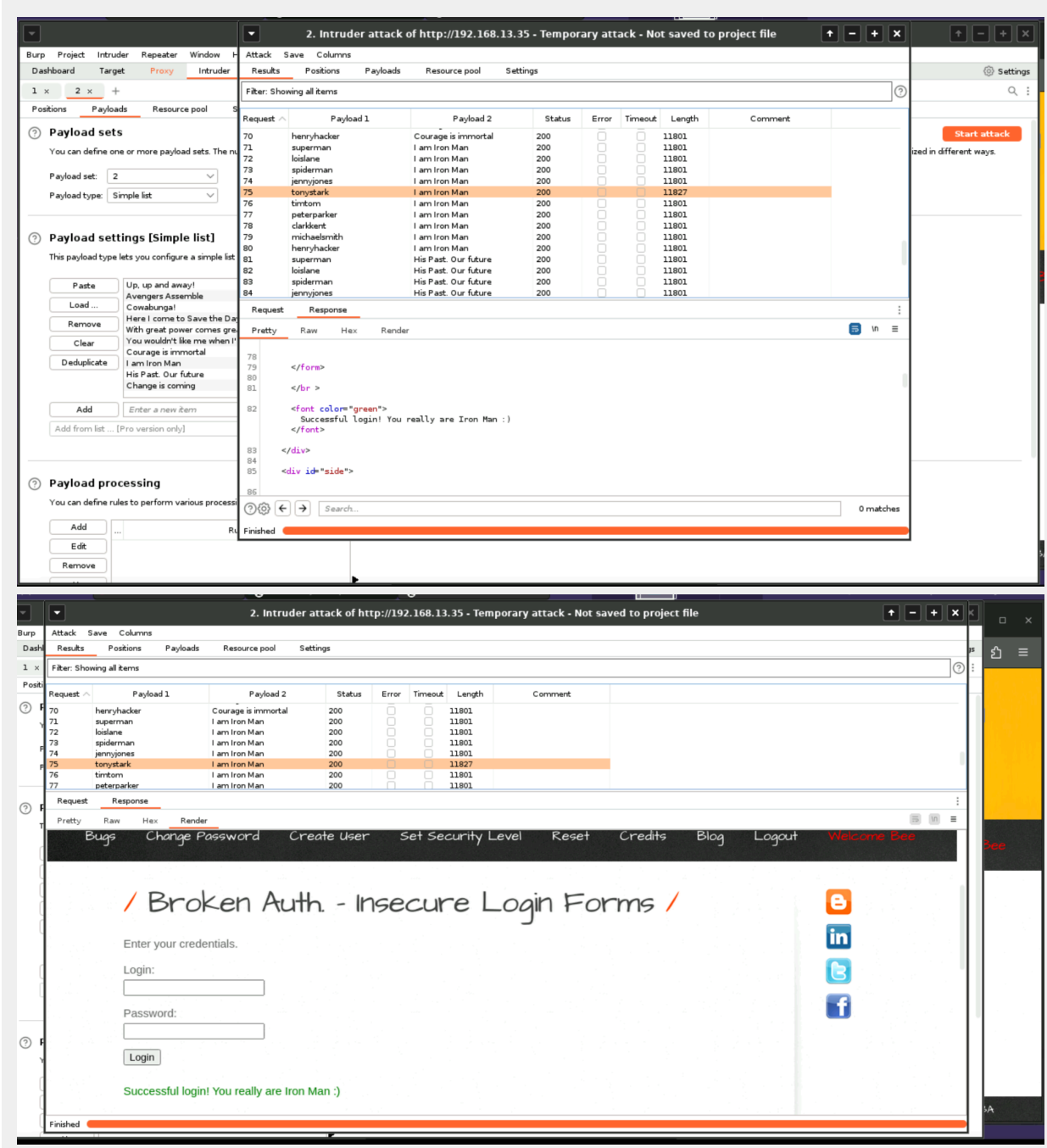
```
1.Server-side validation that does not allow selection of unintended files.
2.Segregation of confidential files from the web server and accessible
directories.
3.Permissions to restrict web server account accessibility.
```

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

Provide a screenshot confirming that you successfully completed this exploit:


Applications
Burp Suite Commu...
bWAPP - Broken Au...
Terminal
Thu 12 Sep, 22:18
Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
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: 1
Payload count: 10
Payload type: Simple list
Request count: 0
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
1. superman
2. loislane
3. spiderman
4. jennyjones
5. tonystark
6. timtom
7. peterparker
8. clarkkent
9. michaelsmith
10. henryhacker
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing
Login
192.168.13.35
© 2014 MME BVBA


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
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: 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 wouldn't like me when I'm angry
Courage is immortal
I am Iron Man
His Past. Our future
Change is coming
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Rule



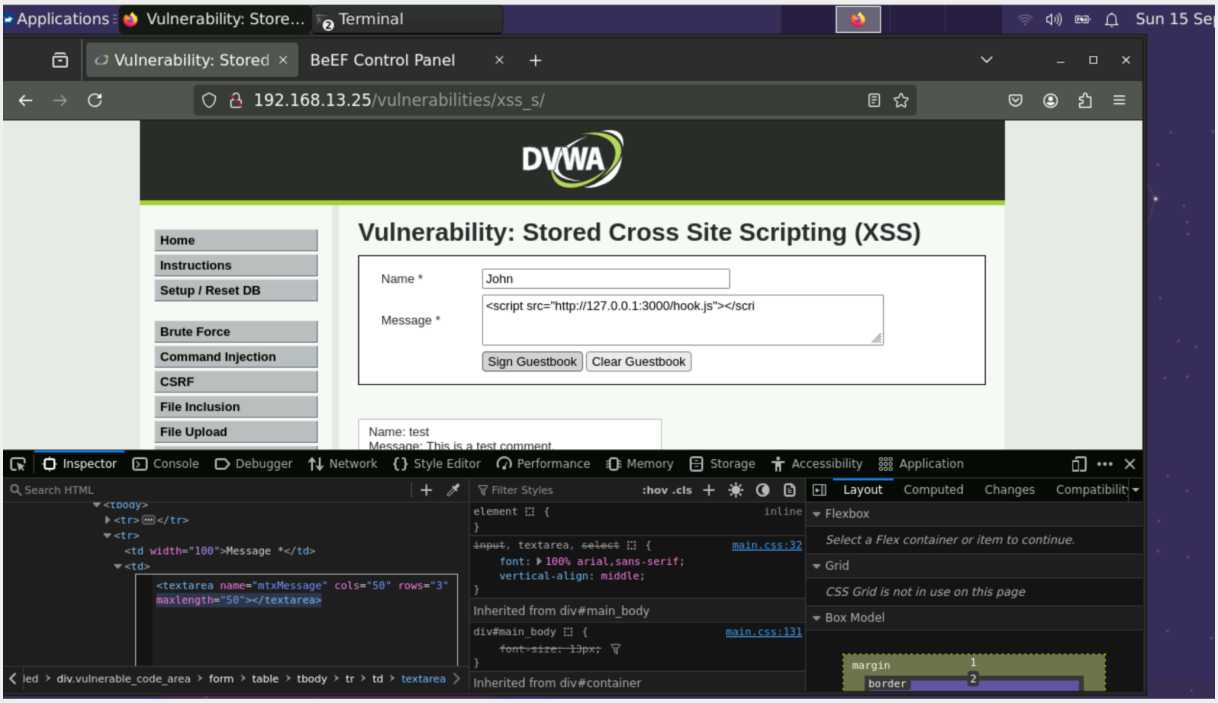
Write two or three sentences outlining mitigation strategies for this vulnerability:

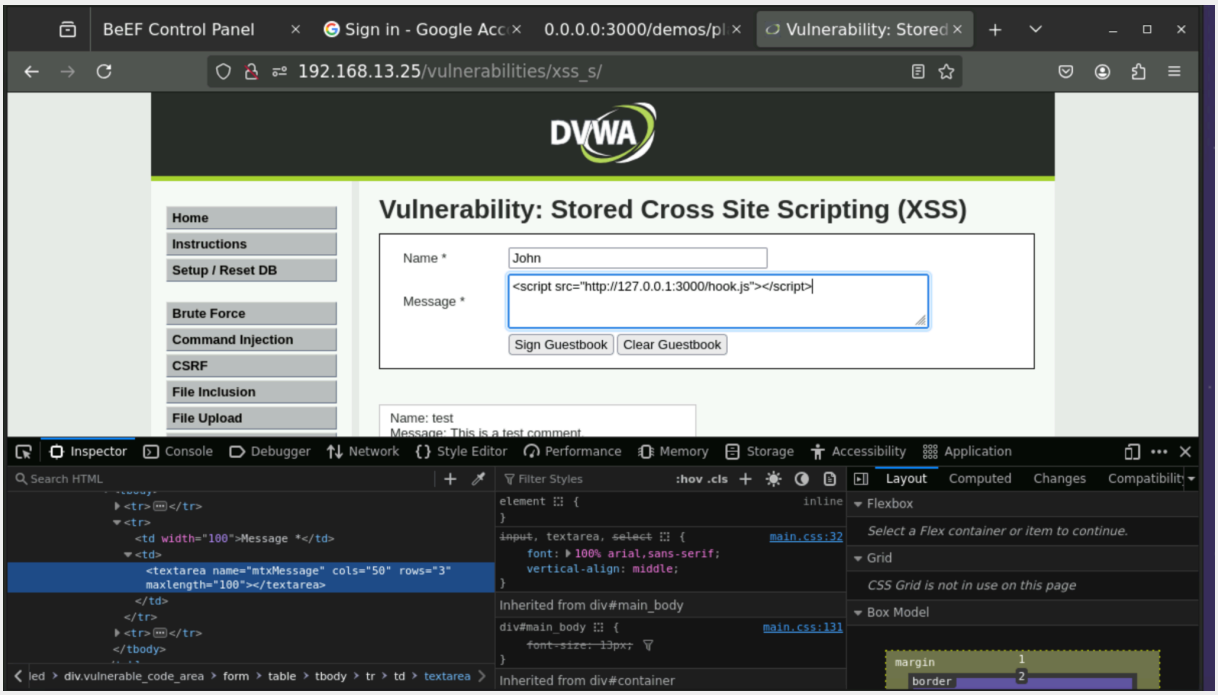
Mitigations can include requiring complex usernames and passwords, using multi-factored authentication and enabling a lockout after a certain amount of failed login attempts.

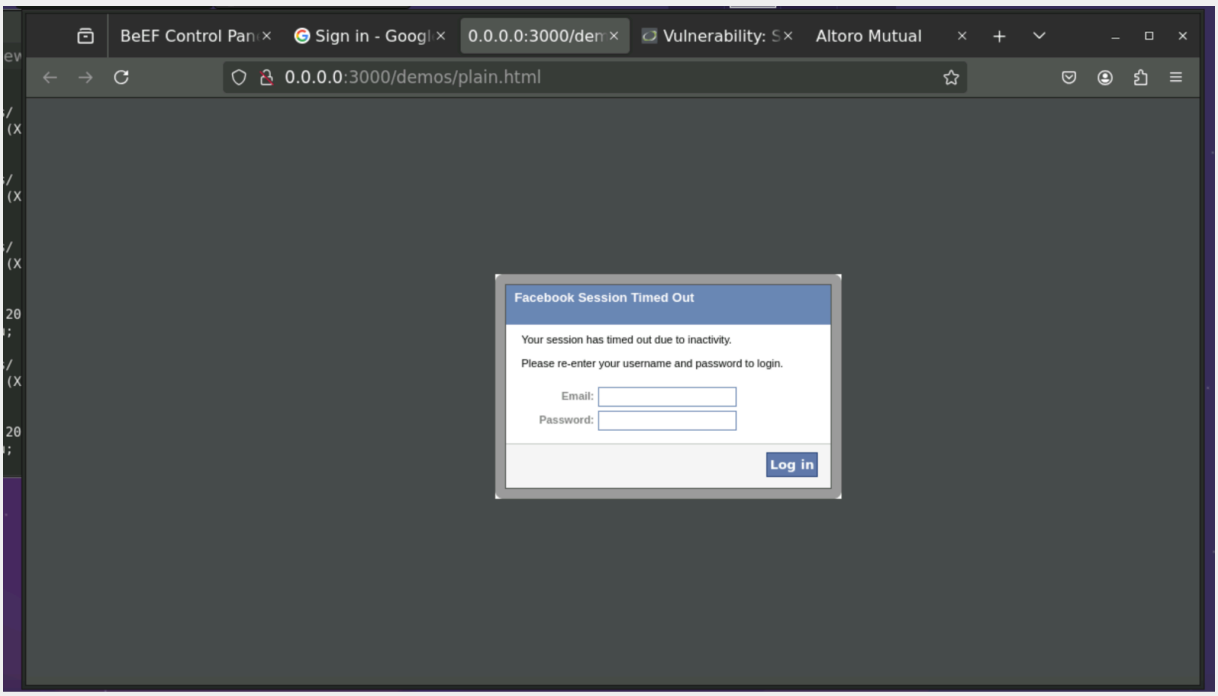
Web Application 3: *Where's the BeEF?*

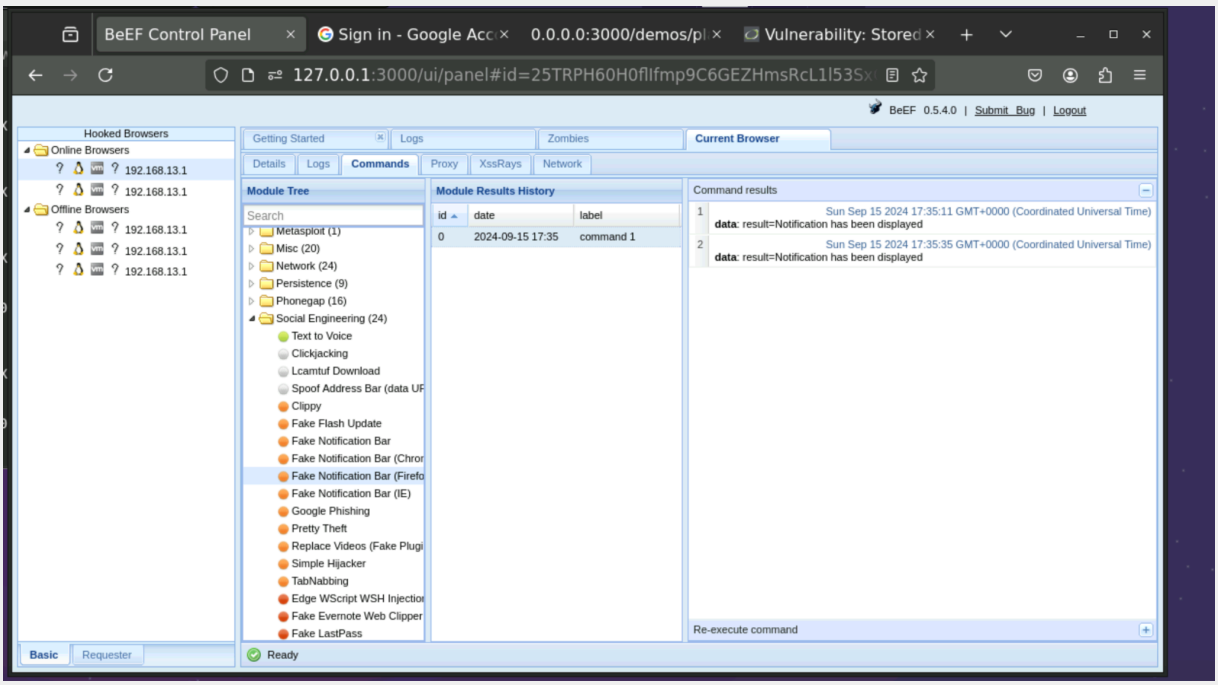
Provide a screenshot confirming that you successfully completed this exploit:

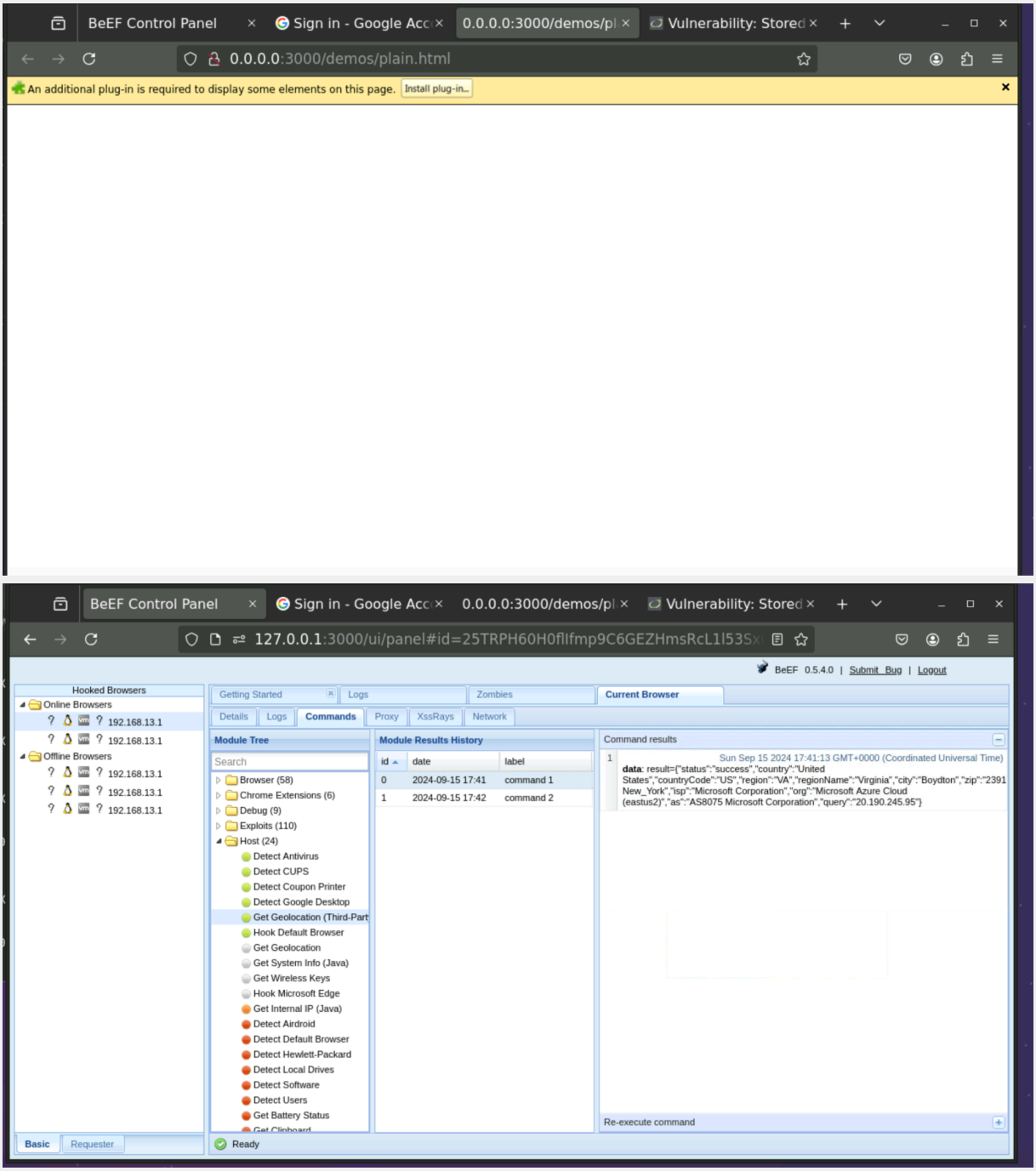
Firstly, I found that in the message box file, there only has maxlenght=50 and I fixed it as “100” and I could type the message.






BeEF Control Pan
Sign in - Googl
0.0.0.0:3000/den
Vulnerability: S
Altoro Mutual
0.0.0.0:3000/demos/plain.html
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


BeEF Control Panel
Sign in - Google Acc
0.0.0.0:3000/demos/pl
Vulnerability: Stored
127.0.0.1:3000/ui/panel#id=25TRPH60H0flIfmp9C6GEZHmsRcL1l53S
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
192.168.13.1
192.168.13.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Metasploit (1)
Misc (20)
Network (24)
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Lcamtuf Download
Spoof Address Bar (data UF
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Chro
Fake Notification Bar (Firefo
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Plugi
Simple Hijacker
TabNabbing
Edge WScript WSH Injectio
Fake Evernote Web Clipper
Fake LastPass
Module Results History
id
date
label
0
2024-09-15 17:35
command 1
Command results
1
Sun Sep 15 2024 17:35:11 GMT+0000 (Coordinated Universal Time)
data: result=Notification has been displayed
2
Sun Sep 15 2024 17:35:35 GMT+0000 (Coordinated Universal Time)
data: result=Notification has been displayed
Re-execute command
Basic
Requester
Ready



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

```
1.Input validation is a common method used to mitigate cross site-scripting.
2.Using extensions to block browser exploits.
```