Cybersecurity

Module 15 Challenge Submission File

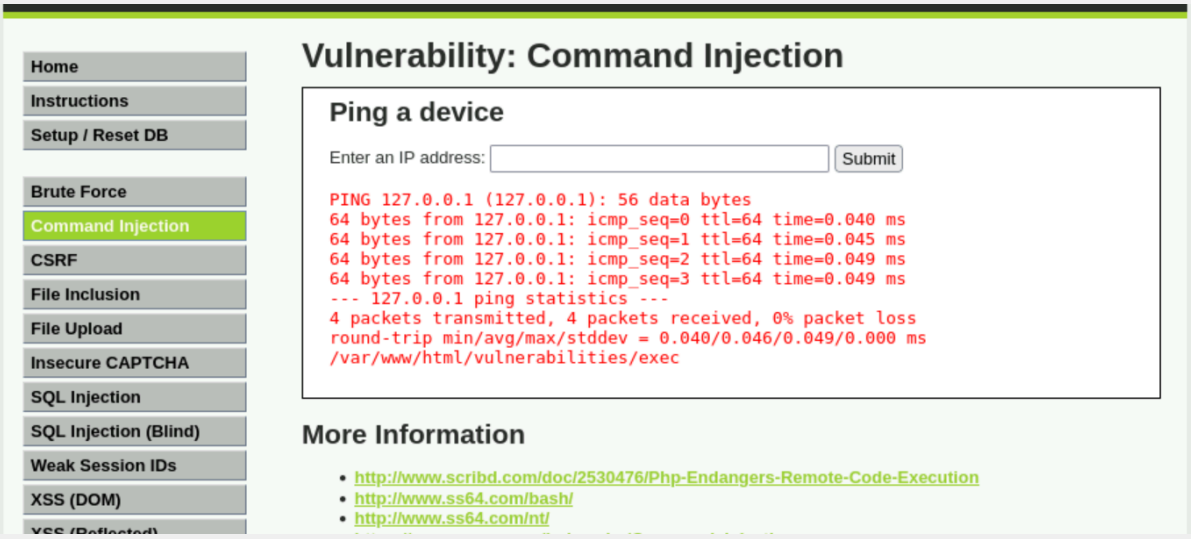
Testing Web Applications for Vulnerabilities

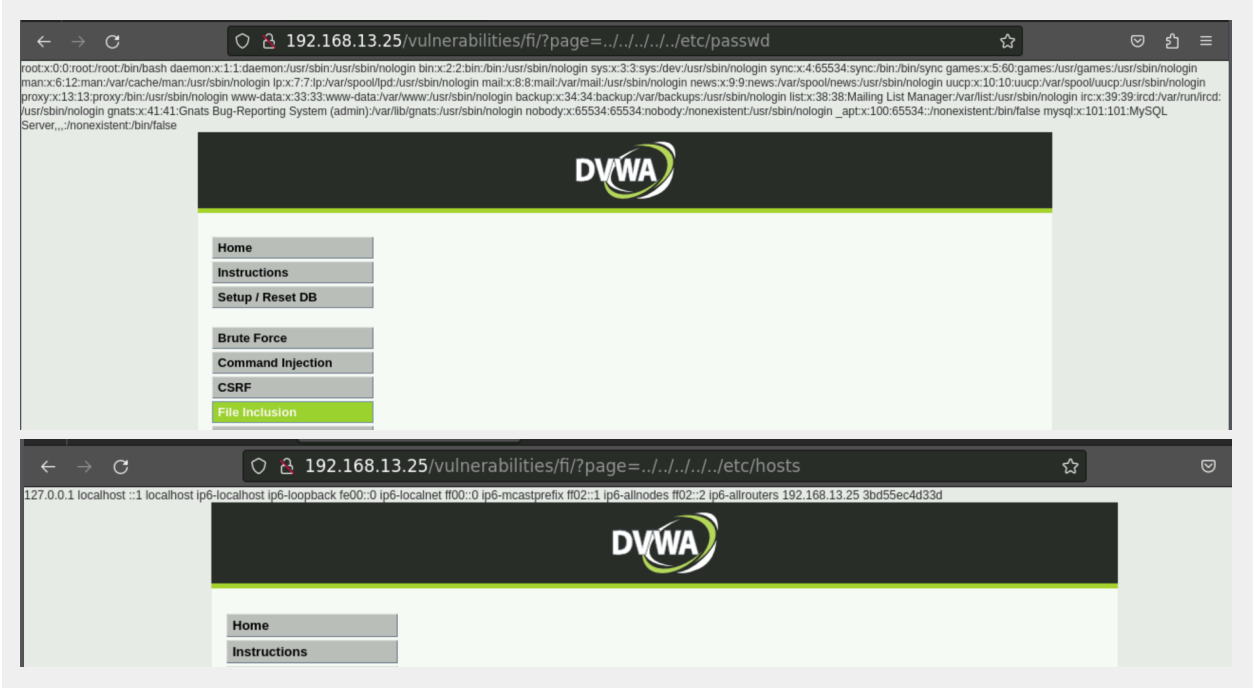
Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

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

Provide a screenshot confirming that you successfully completed this exploit:


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)
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=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.052 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.044/0.050/0.055/0.000 ms
More Information
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/


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)
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=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.049 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.040/0.046/0.049/0.000 ms
/var/www/html/vulnerabilities/exec
More Information
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

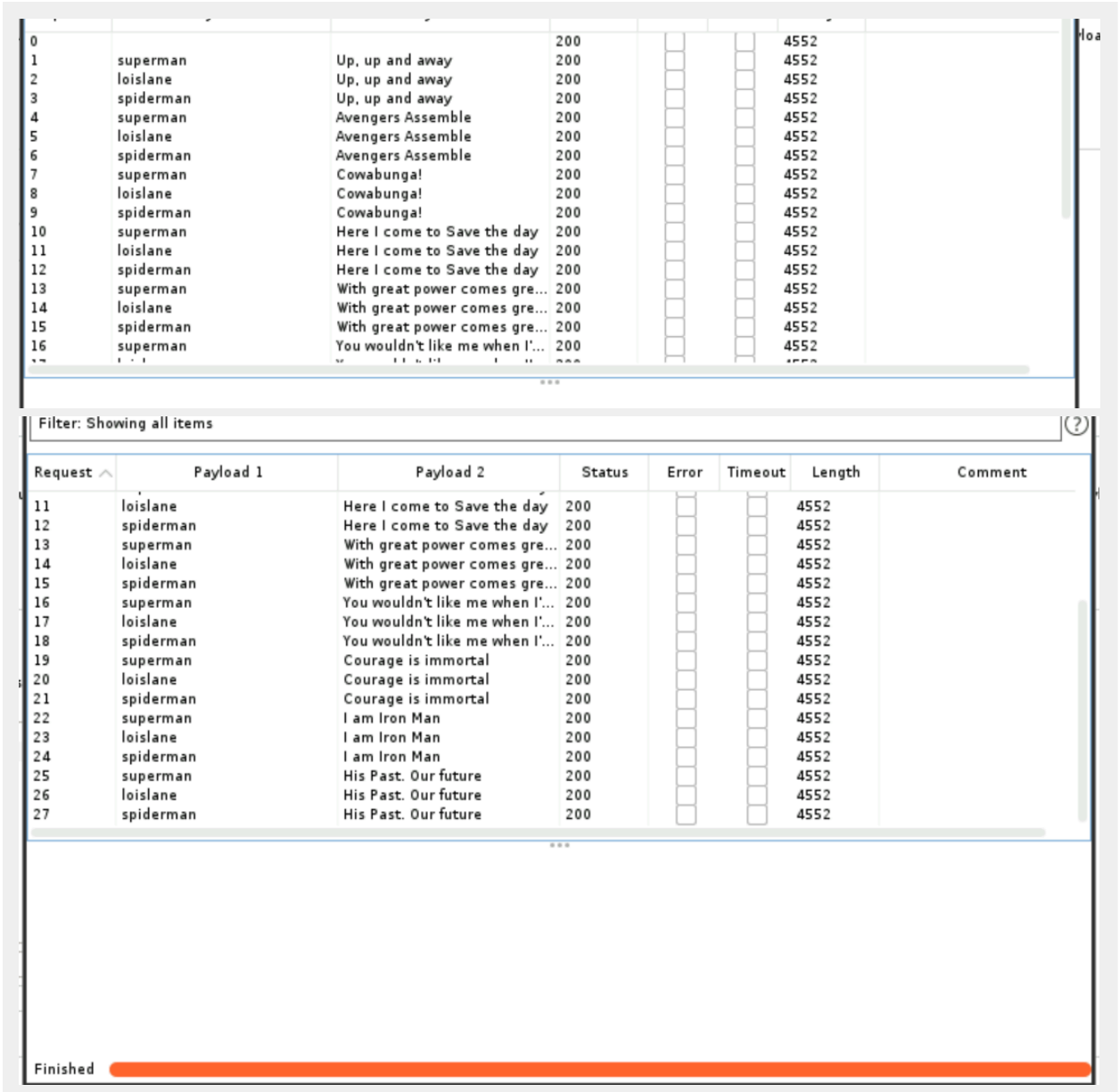


Write two or three sentences outlining mitigation strategies for this vulnerability:

To prevent this kind of attack we can make sure that our web server software is updated, sanitizing users' inputs so nobody can take their information, and using input validation to limit the users ability to modify any file.

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

Provide a screenshot confirming that you successfully completed this exploit:

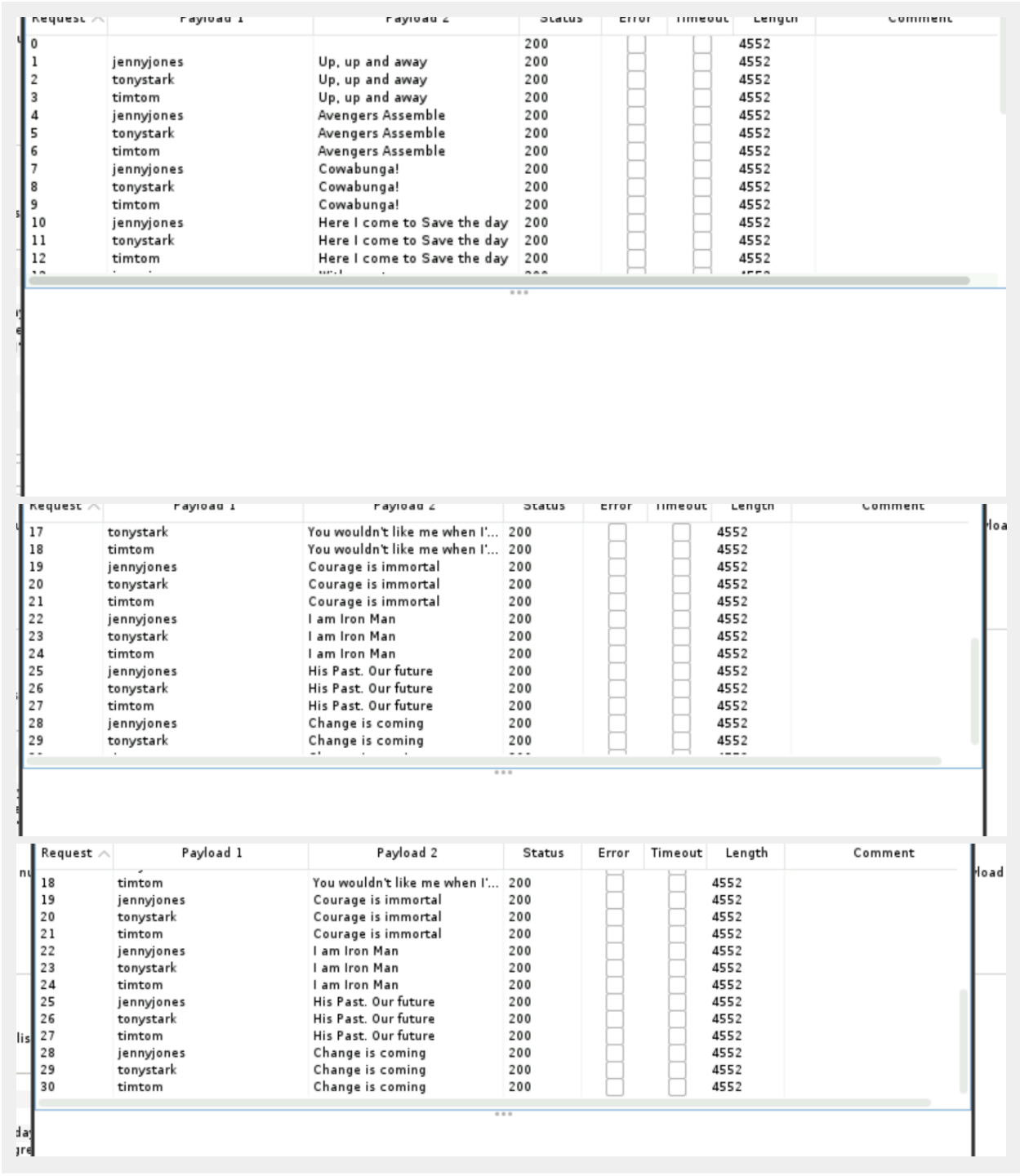


0			200			4552	
1	superman	Up, up and away	200			4552	
2	loislane	Up, up and away	200			4552	
3	spiderman	Up, up and away	200			4552	
4	superman	Avengers Assemble	200			4552	
5	loislane	Avengers Assemble	200			4552	
6	spiderman	Avengers Assemble	200			4552	
7	superman	Cowabunga!	200			4552	
8	loislane	Cowabunga!	200			4552	
9	spiderman	Cowabunga!	200			4552	
10	superman	Here I come to Save the day	200			4552	
11	loislane	Here I come to Save the day	200			4552	
12	spiderman	Here I come to Save the day	200			4552	
13	superman	With great power comes gre...	200			4552	
14	loislane	With great power comes gre...	200			4552	
15	spiderman	With great power comes gre...	200			4552	
16	superman	You wouldn't like me when I'...	200			4552	

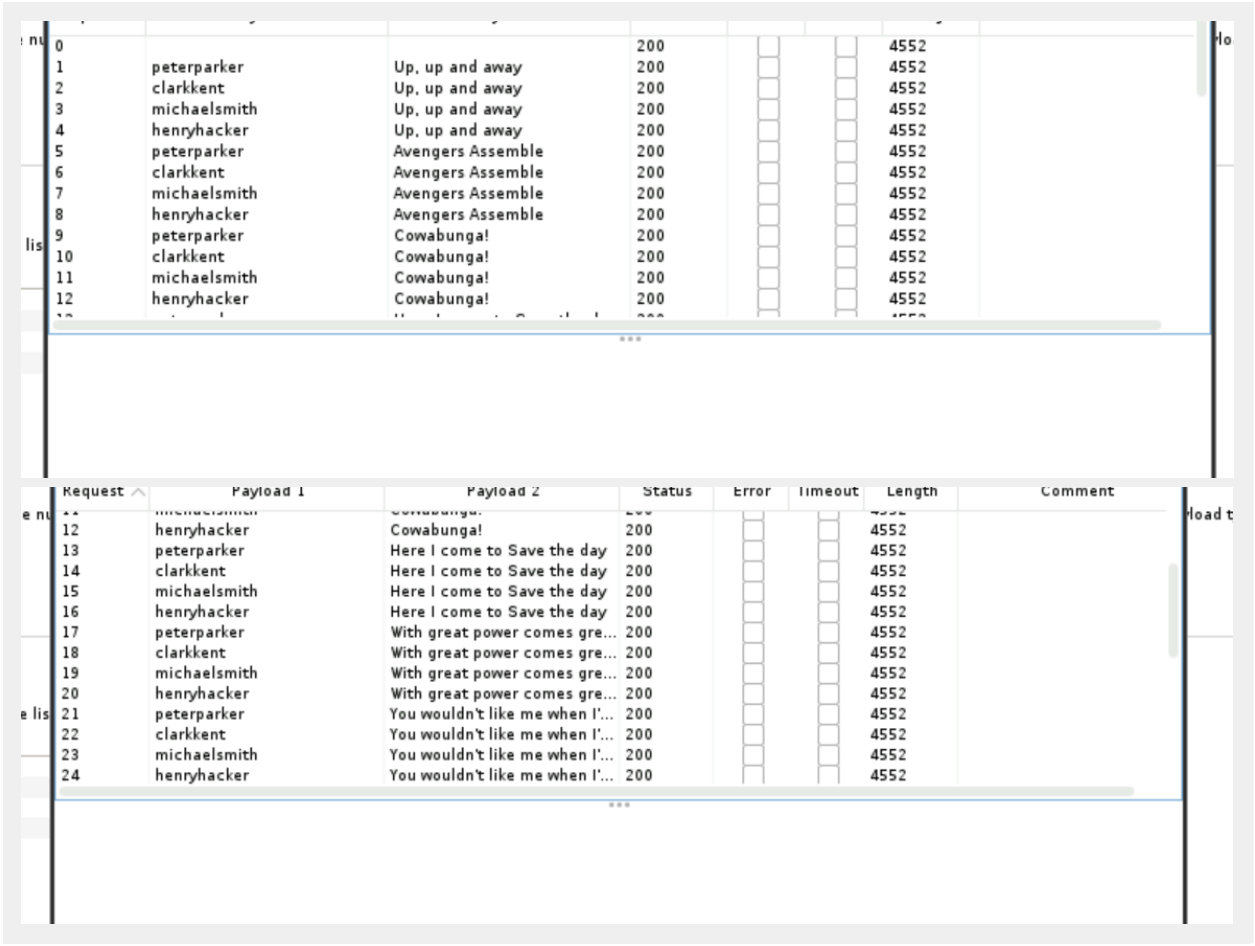
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
11	loislane	Here I come to Save the day	200			4552	
12	spiderman	Here I come to Save the day	200			4552	
13	superman	With great power comes gre...	200			4552	
14	loislane	With great power comes gre...	200			4552	
15	spiderman	With great power comes gre...	200			4552	
16	superman	You wouldn't like me when I'...	200			4552	
17	loislane	You wouldn't like me when I'...	200			4552	
18	spiderman	You wouldn't like me when I'...	200			4552	
19	superman	Courage is immortal	200			4552	
20	loislane	Courage is immortal	200			4552	
21	spiderman	Courage is immortal	200			4552	
22	superman	I am Iron Man	200			4552	
23	loislane	I am Iron Man	200			4552	
24	spiderman	I am Iron Man	200			4552	
25	superman	His Past. Our future	200			4552	
26	loislane	His Past. Our future	200			4552	
27	spiderman	His Past. Our future	200			4552	

Finished

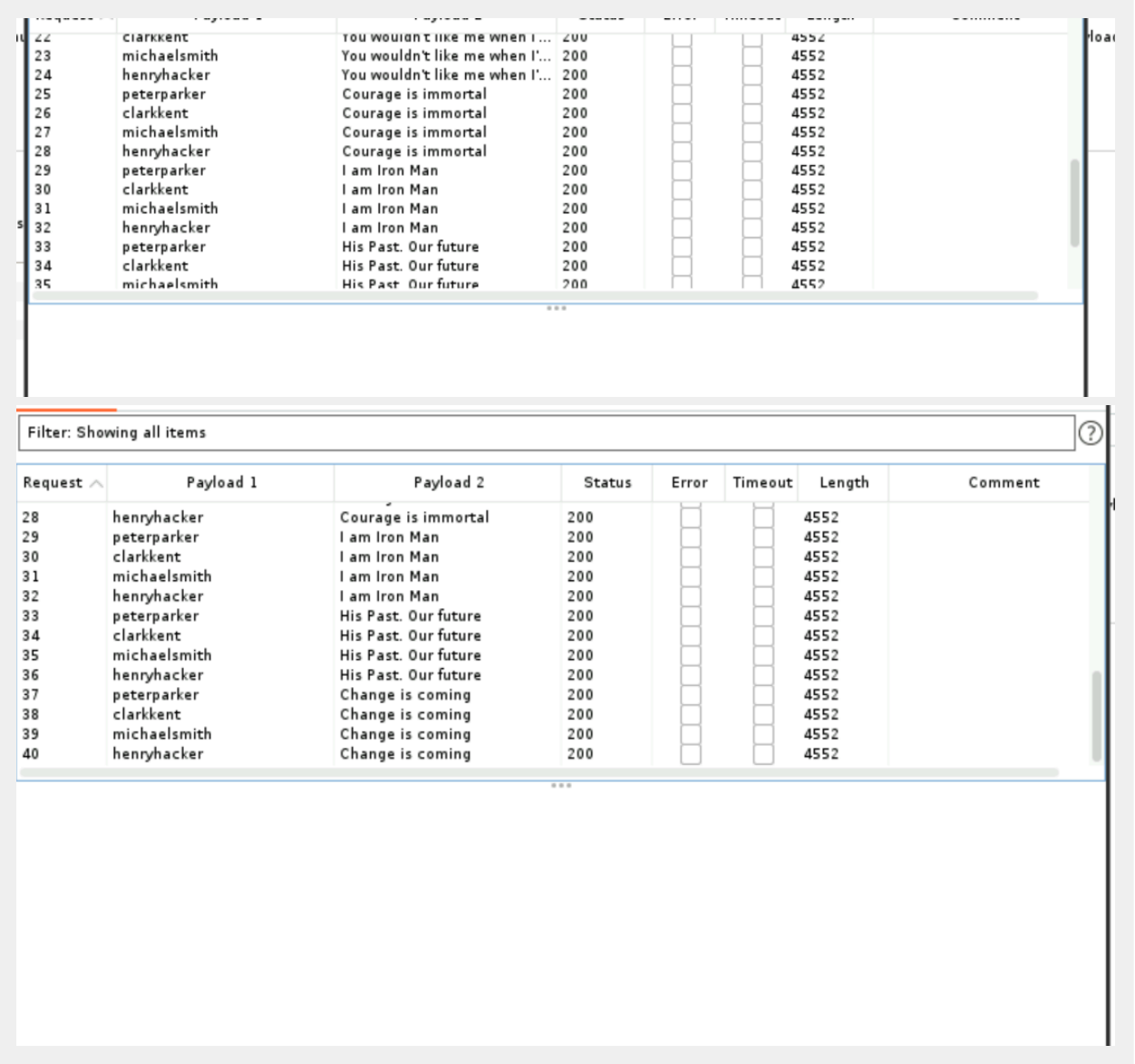


Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200			4552	
1	jennyjones	Up, up and away	200			4552	
2	tonystark	Up, up and away	200			4552	
3	timtom	Up, up and away	200			4552	
4	jennyjones	Avengers Assemble	200			4552	
5	tonystark	Avengers Assemble	200			4552	
6	timtom	Avengers Assemble	200			4552	
7	jennyjones	Cowabunga!	200			4552	
8	tonystark	Cowabunga!	200			4552	
9	timtom	Cowabunga!	200			4552	
10	jennyjones	Here I come to Save the day	200			4552	
11	tonystark	Here I come to Save the day	200			4552	
12	timtom	Here I come to Save the day	200			4552	
17	tonystark	You wouldn't like me when I'...	200			4552	
18	timtom	You wouldn't like me when I'...	200			4552	
19	jennyjones	Courage is immortal	200			4552	
20	tonystark	Courage is immortal	200			4552	
21	timtom	Courage is immortal	200			4552	
22	jennyjones	I am Iron Man	200			4552	
23	tonystark	I am Iron Man	200			4552	
24	timtom	I am Iron Man	200			4552	
25	jennyjones	His Past. Our future	200			4552	
26	tonystark	His Past. Our future	200			4552	
27	timtom	His Past. Our future	200			4552	
28	jennyjones	Change is coming	200			4552	
29	tonystark	Change is coming	200			4552	
30	timtom	Change is coming	200			4552	



Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200			4552	
1	peterparker	Up, up and away	200			4552	
2	clarkkent	Up, up and away	200			4552	
3	michaelsmith	Up, up and away	200			4552	
4	henryhacker	Up, up and away	200			4552	
5	peterparker	Avengers Assemble	200			4552	
6	clarkkent	Avengers Assemble	200			4552	
7	michaelsmith	Avengers Assemble	200			4552	
8	henryhacker	Avengers Assemble	200			4552	
9	peterparker	Cowabunga!	200			4552	
10	clarkkent	Cowabunga!	200			4552	
11	michaelsmith	Cowabunga!	200			4552	
12	henryhacker	Cowabunga!	200			4552	

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
12	henryhacker	Cowabunga!	200			4552	
13	peterparker	Here I come to Save the day	200			4552	
14	clarkkent	Here I come to Save the day	200			4552	
15	michaelsmith	Here I come to Save the day	200			4552	
16	henryhacker	Here I come to Save the day	200			4552	
17	peterparker	With great power comes gre...	200			4552	
18	clarkkent	With great power comes gre...	200			4552	
19	michaelsmith	With great power comes gre...	200			4552	
20	henryhacker	With great power comes gre...	200			4552	
21	peterparker	You wouldn't like me when I'...	200			4552	
22	clarkkent	You wouldn't like me when I'...	200			4552	
23	michaelsmith	You wouldn't like me when I'...	200			4552	
24	henryhacker	You wouldn't like me when I'...	200			4552	

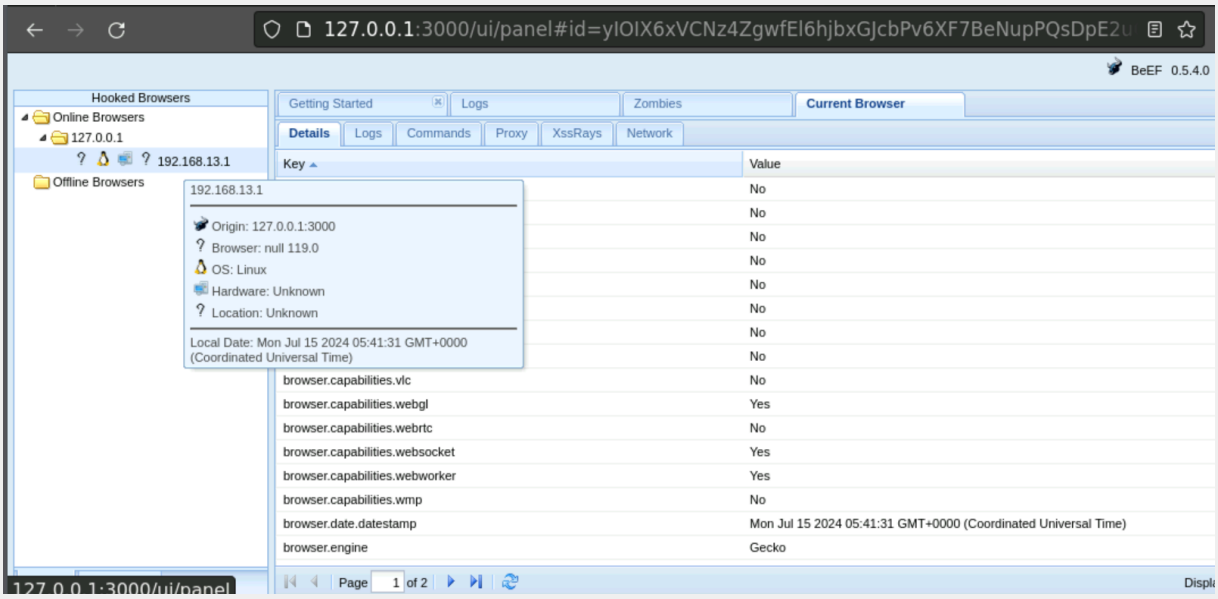


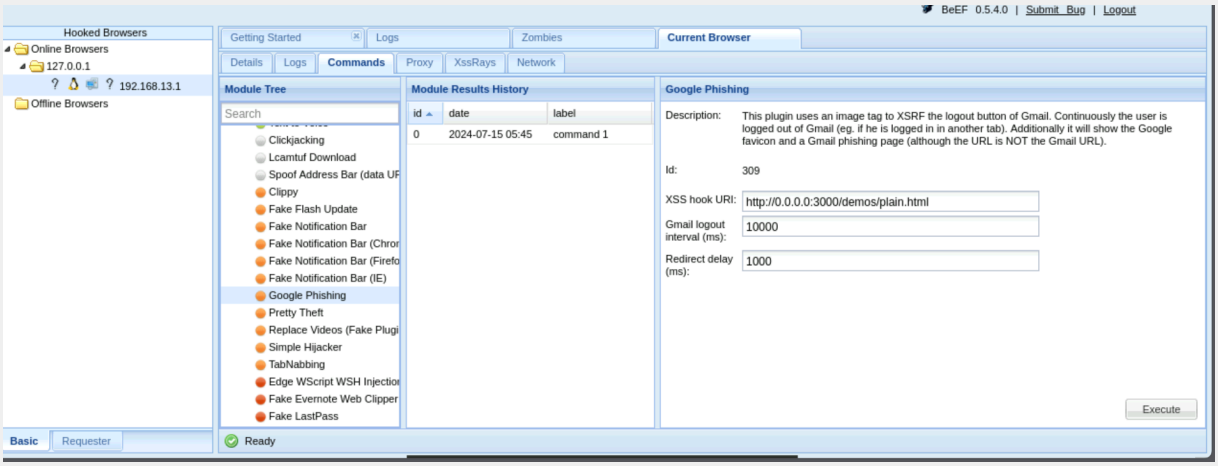
Write two or three sentences outlining mitigation strategies for this vulnerability:

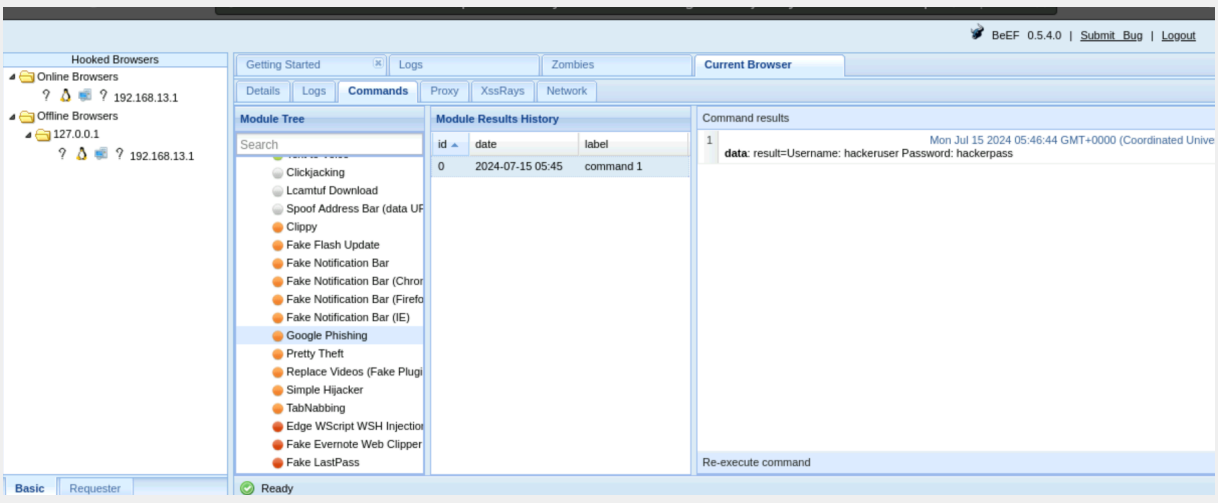
```
Make sure we use strong passwords and nothing related to us, also we can use
the multi-factor authenticator, also a strong username, enforce password
policies: minimum and maximum length and complexity requirements.
```

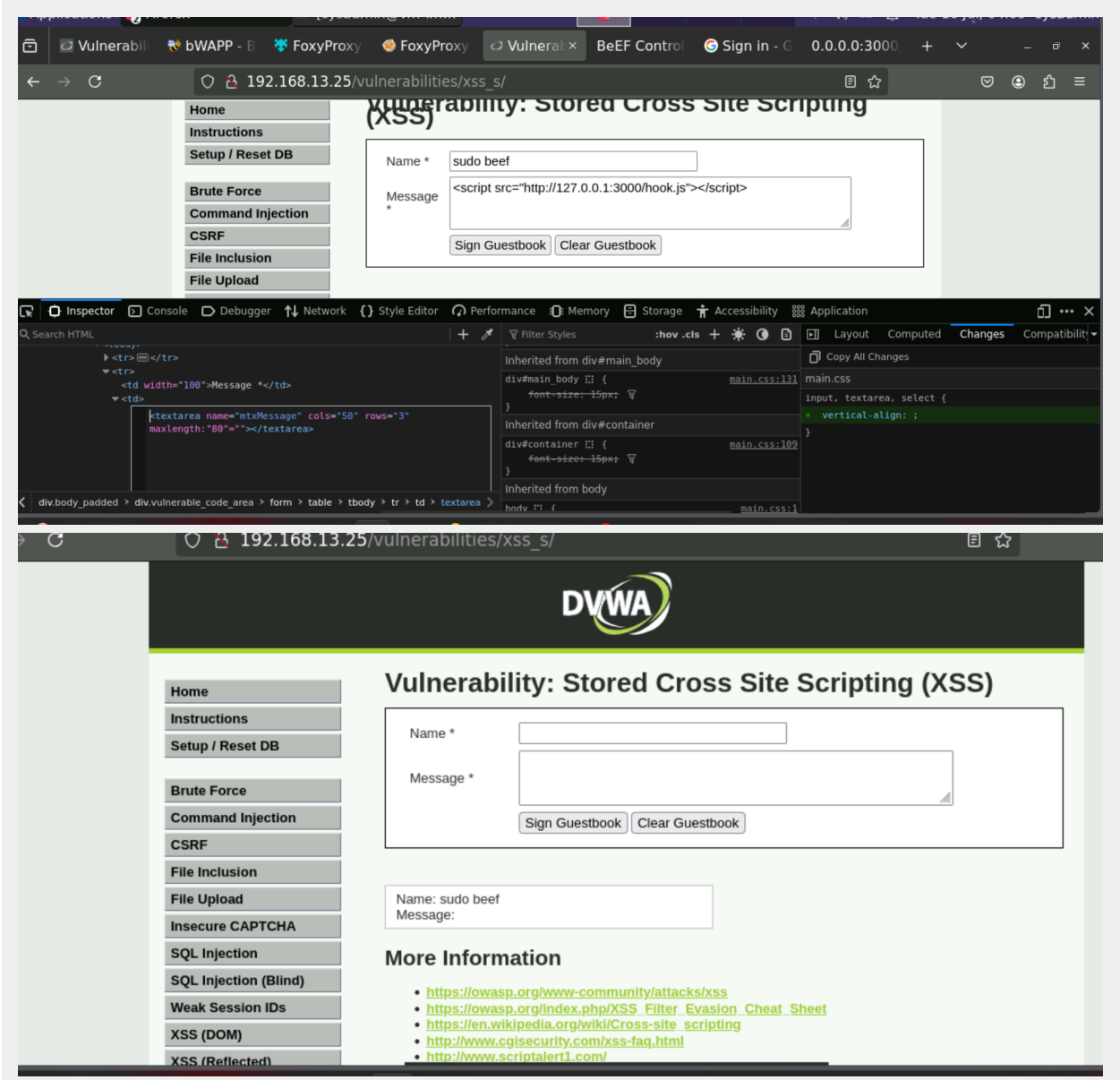
Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:


127.0.0.1:3000/ui/panel#id=yIOIX6xVCNz4ZgwfEl6hjbxGJcbPv6XF7BeNupPQsDpE2u
BeEF 0.5.4.0
Hooked Browsers
Online Browsers
127.0.0.1
192.168.13.1
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Key
Value
192.168.13.1
Origin: 127.0.0.1:3000
Browser: null 119.0
OS: Linux
Hardware: Unknown
Location: Unknown
Local Date: Mon Jul 15 2024 05:41:31 GMT+0000 (Coordinated Universal Time)
browser.capabilities.vlc No
browser.capabilities.webgl Yes
browser.capabilities.webrtc No
browser.capabilities.websocket Yes
browser.capabilities.webworker Yes
browser.capabilities.wmp No
browser.date.datestamp Mon Jul 15 2024 05:41:31 GMT+0000 (Coordinated Universal Time)
browser.engine Gecko
Page 1 of 2


BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
127.0.0.1
192.168.13.1
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Clickjacking
Lcamtuf Download
Spoof Address Bar (data UF
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Chror
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
2024-07-15 05:45
command 1
Google Phishing
Description:
This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will show the Google favicon and a Gmail phishing page (although the URL is NOT the Gmail URL).
Id:
309
XSS hook URI:
http://0.0.0.0:3000/demos/plain.html
Gmail logout interval (ms):
10000
Redirect delay (ms):
1000
Execute
Basic
Requester
Ready


BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.13.1
Offline Browsers
127.0.0.1
192.168.13.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Clickjacking
Lcamtuf Download
Spoof Address Bar (data UF
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Chror
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
2024-07-15 05:45
command 1
Command results
1
Mon Jul 15 2024 05:46:44 GMT+0000 (Coordinated Unive
data: result=Username: hackeruser Password: hackerpass
Re-execute command
Basic
Requester
Ready



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

We can keep our browser and endpoints updated, also enforce strong passwords and use the multi-factor authenticator, monitor any strange network traffic, use modern frameworks to prevent an attack, and also intrusion prevention and detection systems.