Cybersecurity

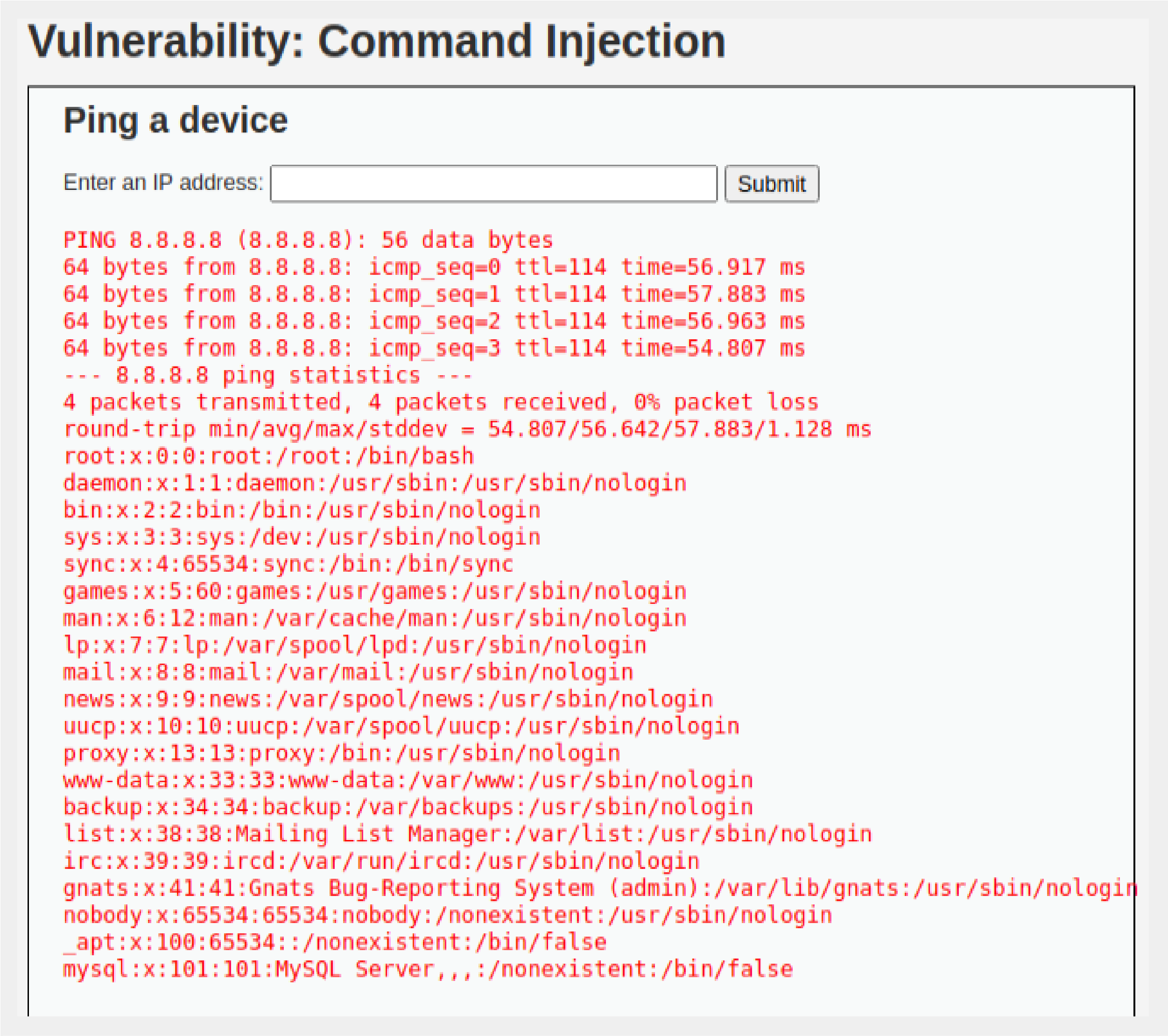
Module 15 Challenge Submission File

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*

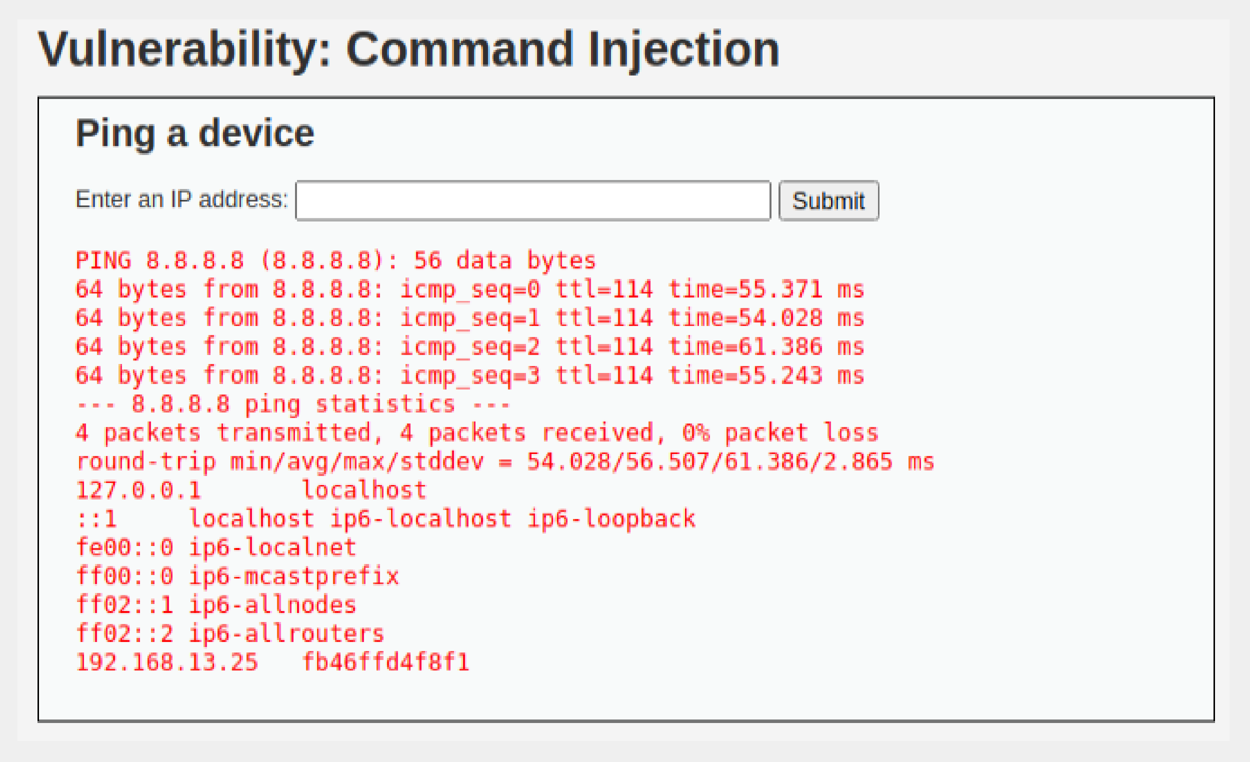
Provide a screenshot confirming that you successfully completed this exploit:



Vulnerability: Command Injection

Ping a device

```
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=56.917 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=57.883 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=56.963 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=54.807 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 54.807/56.642/57.883/1.128 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
```



Vulnerability: Command Injection

Ping a device

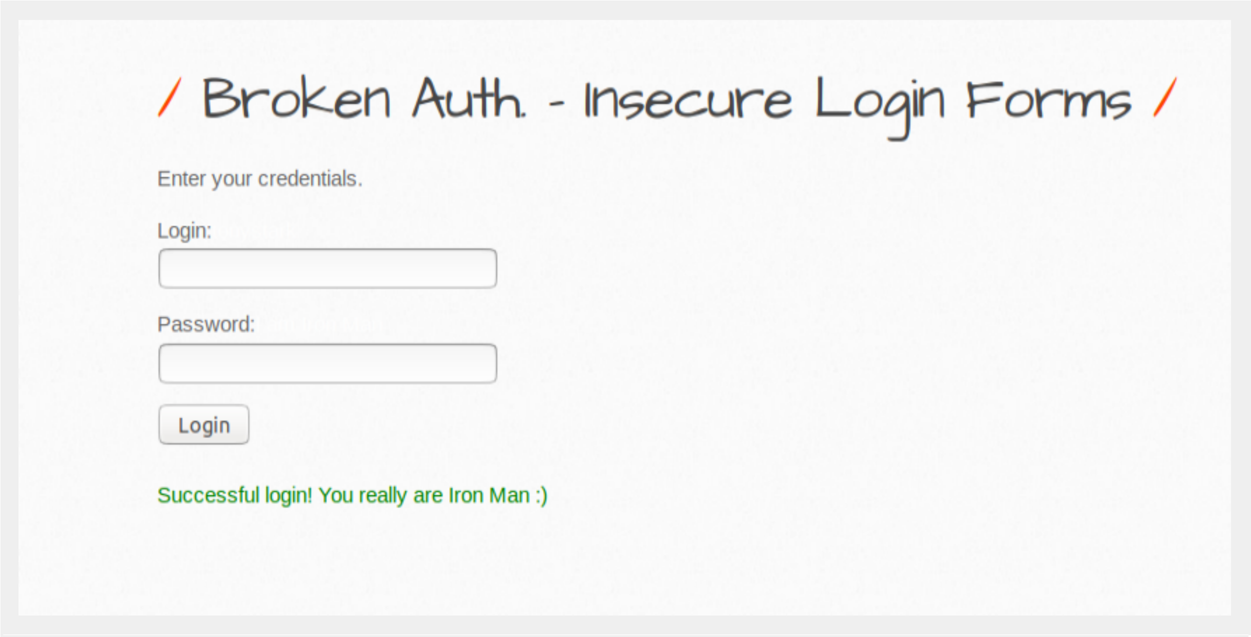
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=55.371 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=54.028 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=61.386 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=55.243 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 54.028/56.507/61.386/2.865 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   fb46ffd4f8f1
```

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

```
Command injection is a web vulnerability that leads to lack of input
validation. An approach called whitelisting can help with validation.
```

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: tonystark

Password: I am Iron Man

Successful login! You really are Iron Man :)

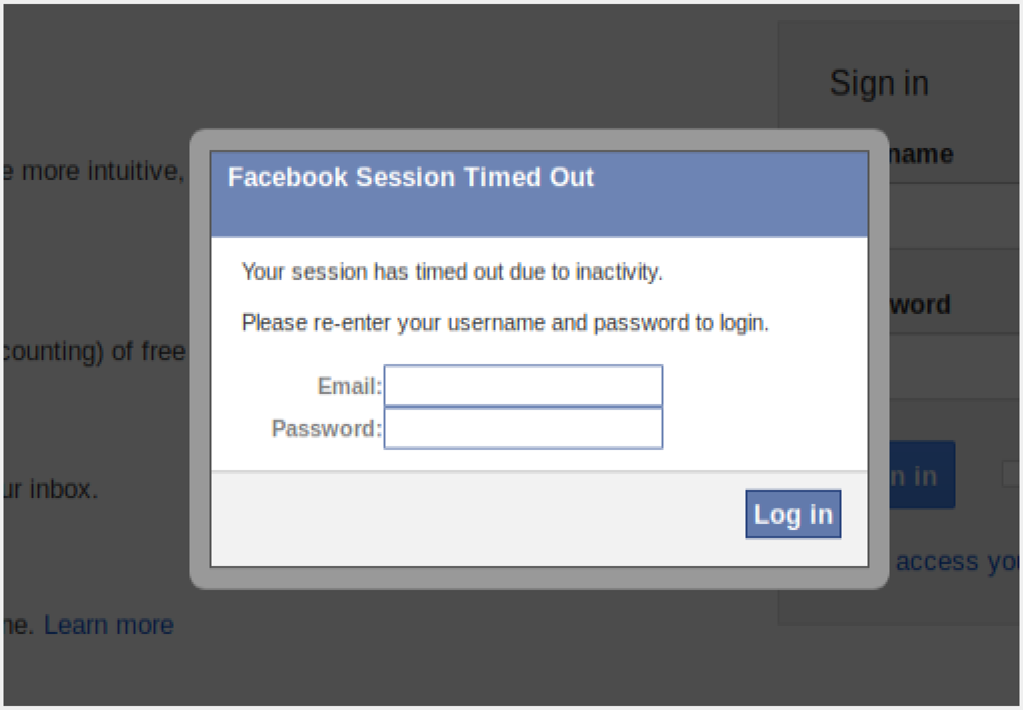
Write two or three sentences outlining mitigation strategies for this vulnerability:

```
A simple way to work around brute force is to lock out accounts with sign in
or brute force attempts. Setting an amount of sign in attempts and a
significant lock out time can prevent future attempts on that account.
```

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

Provide a screenshot confirming that you successfully completed this exploit:

```
Pretty Theft
```



Facebook Session Timed Out

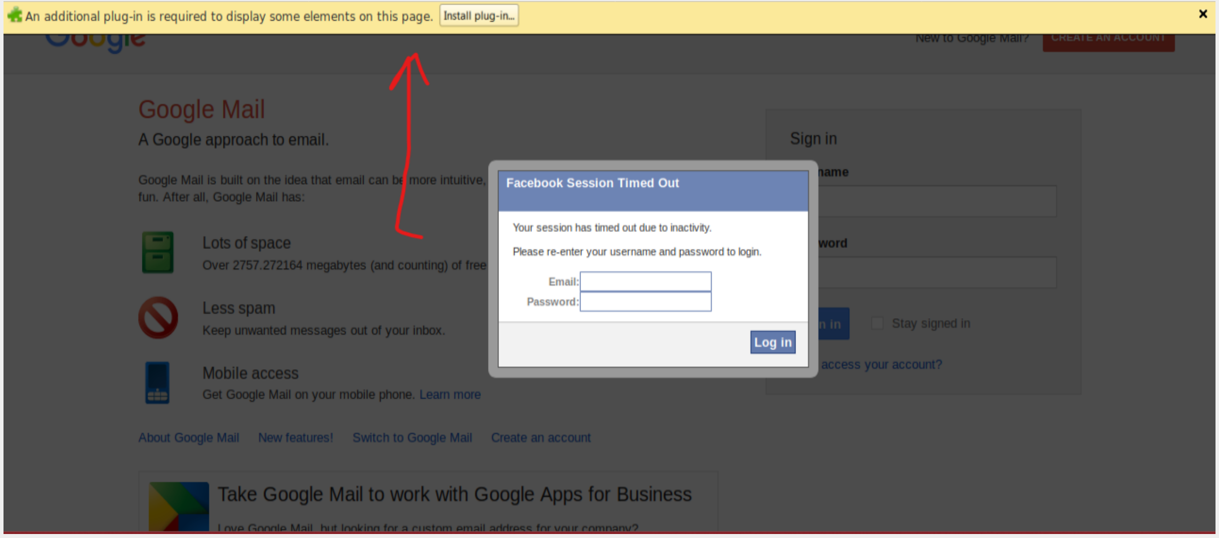
Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email:

Password:

Fake Notification Bar



An additional plug-in is required to display some elements on this page. Install plug-in...

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, fun. After all, Google Mail has:

Lots of space

Over 2757.272164 megabytes (and counting) of free

Less spam

Keep unwanted messages out of your inbox.

Mobile access

Get Google Mail on your mobile phone. Learn more

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

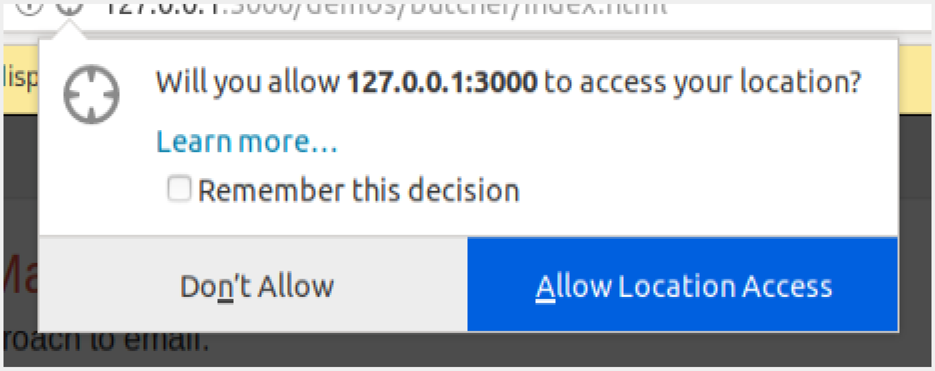
Email:

Password:

Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?

Get Geolocation



Will you allow **127.0.0.1:3000** to access your location?

Learn more...

□ Remember this decision

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

Setting up security settings to avoid Java. Using proxies to detect XSS attacks when it happens.