Cybersecurity

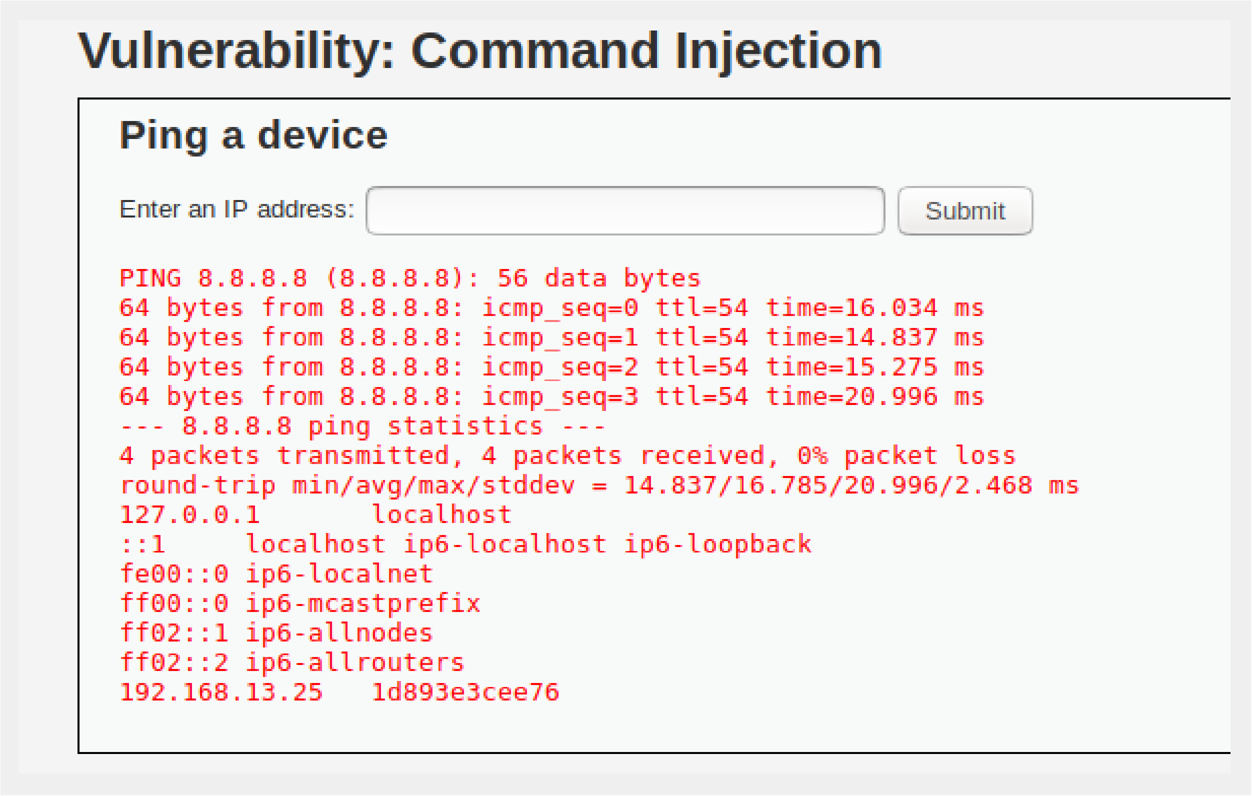
Module 15 Challenge Submission File

# 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*

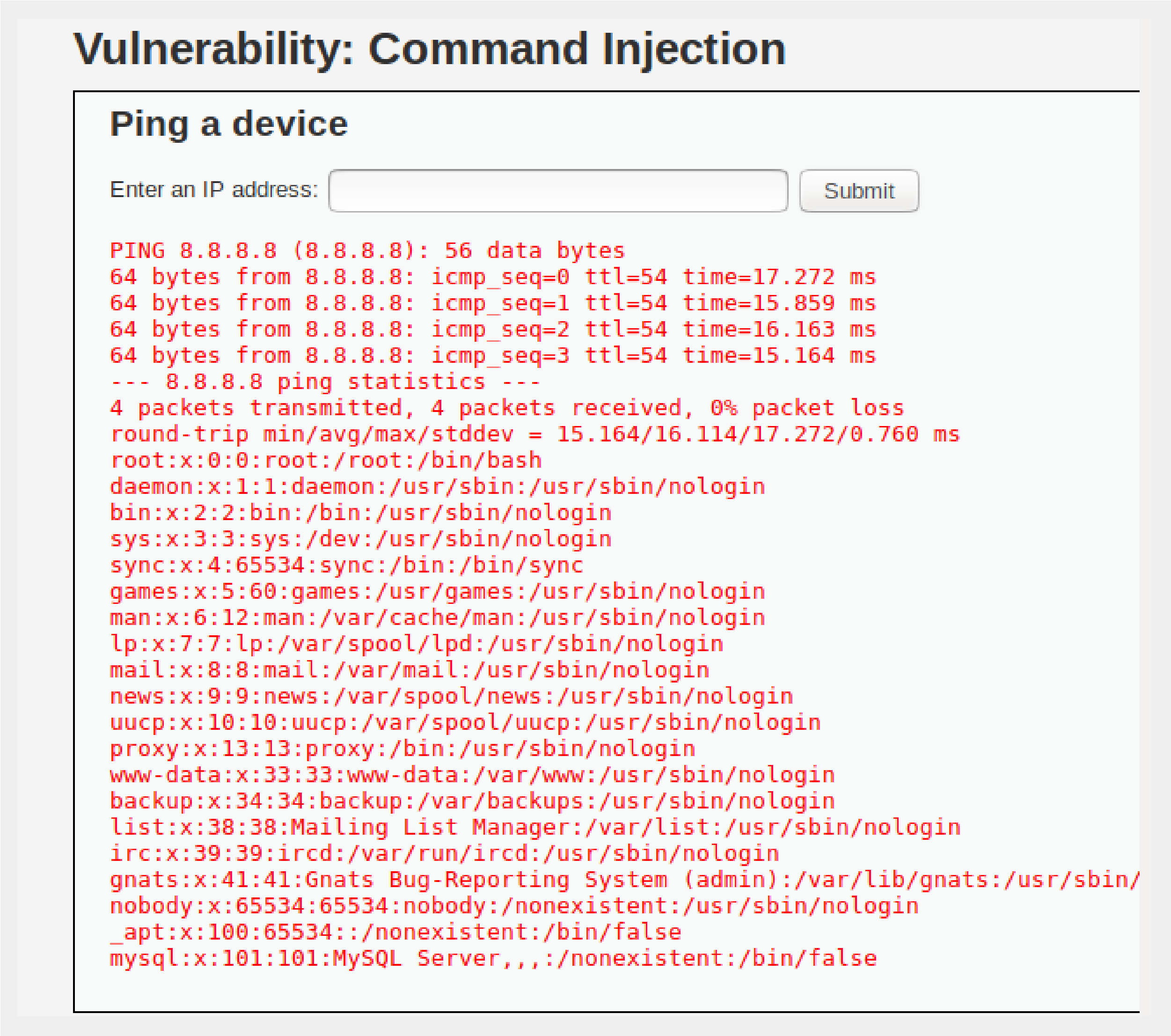
Provide a screenshot confirming that you successfully completed this exploit:



# 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=54 time=16.034 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=14.837 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=15.275 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=20.996 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.837/16.785/20.996/2.468 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   1d893e3cee76
```



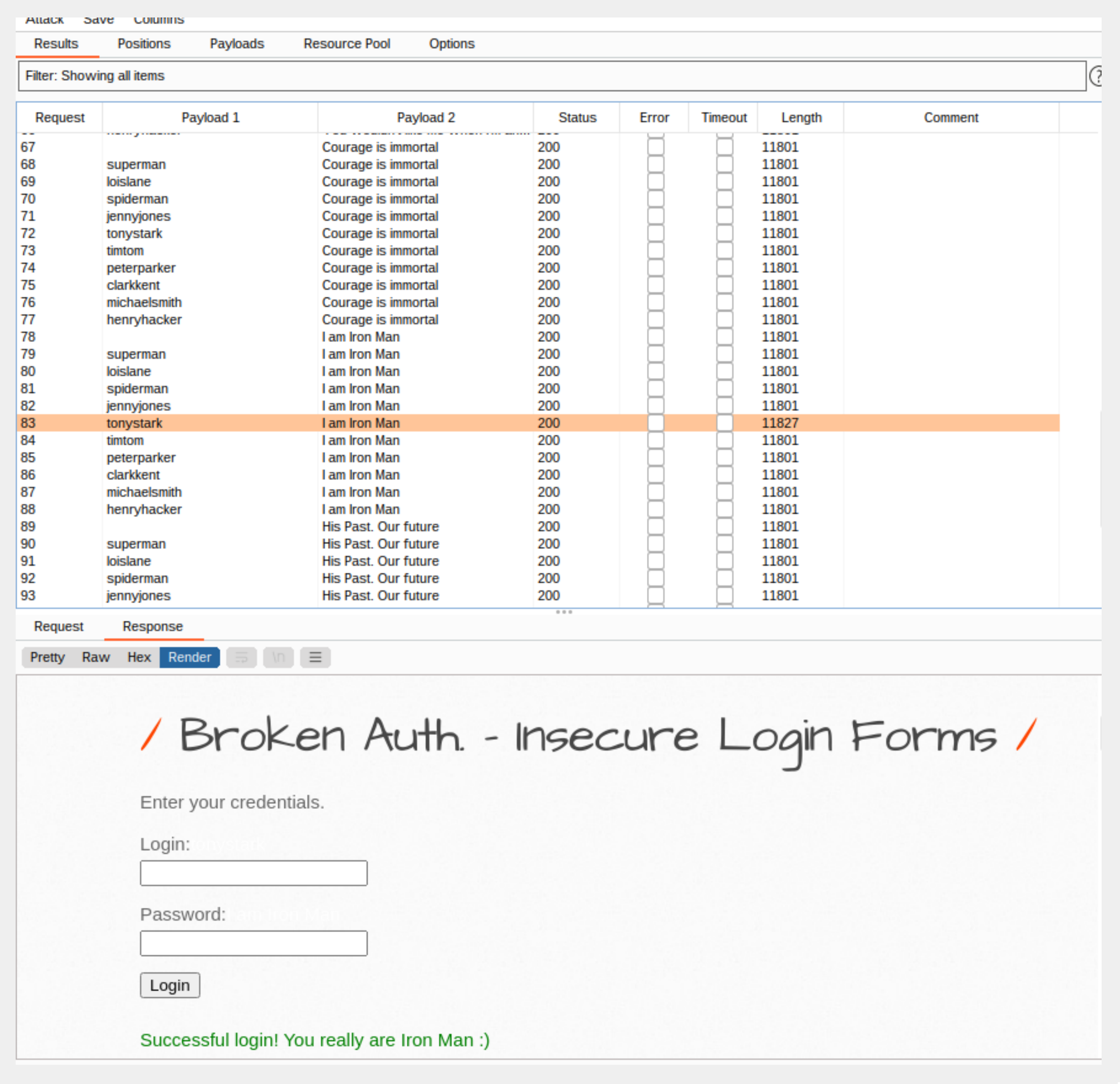
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=54 time=17.272 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=15.859 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=16.163 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=15.164 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 15.164/16.114/17.272/0.760 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
```

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

```
Limiting character input is one way to mitigate this attack. By only
allowing letters, numbers, and certain special characters (!,$,etc)
injecting scripts and commands would be more difficult.
```

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

Provide a screenshot confirming that you successfully completed this exploit:



Filter: Showing all items

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 67 | | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 68 | superman | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 69 | loislane | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 70 | spiderman | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 71 | jennyjones | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 72 | tonystark | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 73 | timtom | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 74 | peterparker | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 75 | clarkkent | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 76 | michaelsmith | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 77 | henryhacker | Courage is immortal | 200 | ☐ | ☐ | 11801 | |
| 78 | | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 79 | superman | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 80 | loislane | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 81 | spiderman | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 82 | jennyjones | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 83 | tonystark | I am Iron Man | 200 | ☐ | ☐ | 11827 | |
| 84 | timtom | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 85 | peterparker | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 86 | clarkkent | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 87 | michaelsmith | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 88 | henryhacker | I am Iron Man | 200 | ☐ | ☐ | 11801 | |
| 89 | | His Past. Our future | 200 | ☐ | ☐ | 11801 | |
| 90 | superman | His Past. Our future | 200 | ☐ | ☐ | 11801 | |
| 91 | loislane | His Past. Our future | 200 | ☐ | ☐ | 11801 | |
| 92 | spiderman | His Past. Our future | 200 | ☐ | ☐ | 11801 | |
| 93 | jennyjones | His Past. Our future | 200 | ☐ | ☐ | 11801 | |

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login: tonystark

Password: I am Iron Man

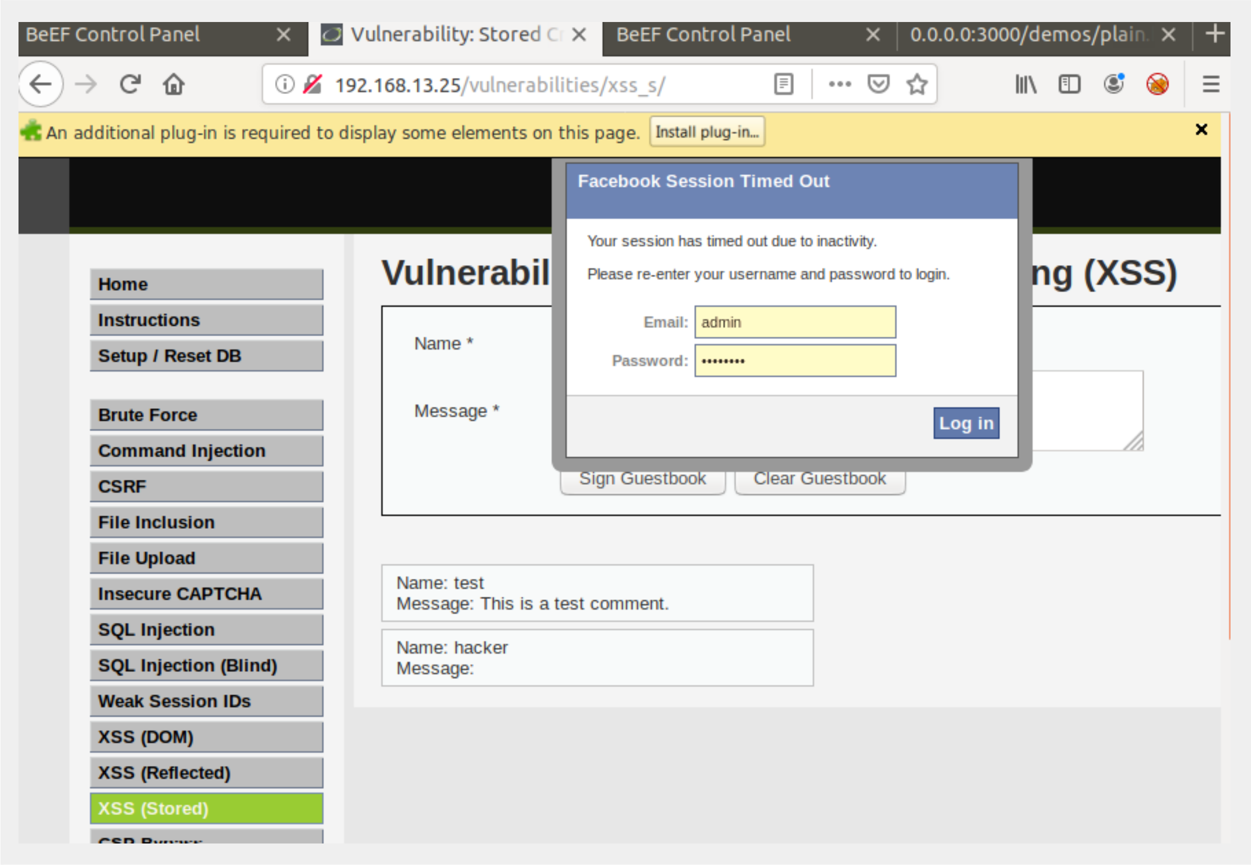
Successful login! You really are Iron Man :)

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

```
Strong username and password rules is one way to mitigate a brute force
attack. The shorter the password, the easier it is to crack. We should also
limit login attempts, make users change password periodically, or use a 2
factor authentication system.
```

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

Provide a screenshot confirming that you successfully completed this exploit:



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

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email: admin
Password: ••••••••

Name *

Message *

Name: test
Message: This is a test comment.

Name: hacker
Message:

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

```
You should always make sure your systems are up to date. Beef XSS can also
be mitigated by not allowing script to be inserted in any fields on the
page.
```