



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

Enter an IP address:

Submit

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.045 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.044/0.046/0.050/0.000 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
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  7b1cdfd7c9f0
```

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

The best way to combat this would be to only allow numbers, in the format of an IP address. In other words, force input-validation so a user could not exploit the site in this way.

Web Application 2: A Brute Force to Be Reckoned With

Provide a screenshot confirming that you successfully completed this exploit:

The screenshot shows a web application security tool interface. At the top, there are tabs: Results, Positions, Payloads, Resource Pool, and Options. Below these is a filter bar that says "Filter: Showing all items".

Request	Payload 1	Payload 2	Status	Error	Timeout	Length ^	Comment
86	timtom	His Past. Our future	200			11801	
87	peterparker	His Past. Our future	200			11801	
88	clarkkent	His Past. Our future	200			11801	
89	micahaelsmith	His Past. Our future	200			11801	
90	henryhacker	His Past. Our future	200			11801	
91	superman	Change is coming	200			11801	
92	loislane	Change is coming	200			11801	
93	spiderman	Change is coming	200			11801	
94	jennyjones	Change is coming	200			11801	
95	tonystark	Change is coming	200			11801	
96	timtom	Change is coming	200			11801	
97	peterparker	Change is coming	200			11801	
98	clarkkent	Change is coming	200			11801	
99	micahaelsmith	Change is coming	200			11801	
100	henryhacker	Change is coming	200			11801	
75	tonystark	I am Iron Man	200			11827	

Below the table, there are tabs for "Request" and "Response". The "Response" tab is selected, showing a "Render" view. It displays a login form with a "Password:" label, a text input field, and a "Login" button. Below the form, a green message reads: "Successful login! You really are Iron Man :)".

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

If the data breach was indeed “years ago” update your password policies. Require users/admins to change passwords after a set amount of time, especially if a data breach is known about.

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

Provide a screenshot confirming that you successfully completed this exploit:

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Clear Guestbook

Facebook Session Timed Out

Your session has timed out due to inactivity.
Please re-enter your username and password to login.

Email: admin

Password:

Log in

Module Results History

id	date	label
0	2024-01-12 03:30	command 1
1	2024-01-12 03:32	command 2

Command results

1

data: answer=admin:password

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

The browser developer would need to include the "HttpOnly" attribute on the cookies. This way code, like JavaScript, would not be able to interact with users' sessions.