Assignment (b): Traffic Observation & Analysis

Login Request Observation (DVWA)

URL: http://localhost/dvwa/login.php

Method: POST

Parameters:

- username=admin

- password=password

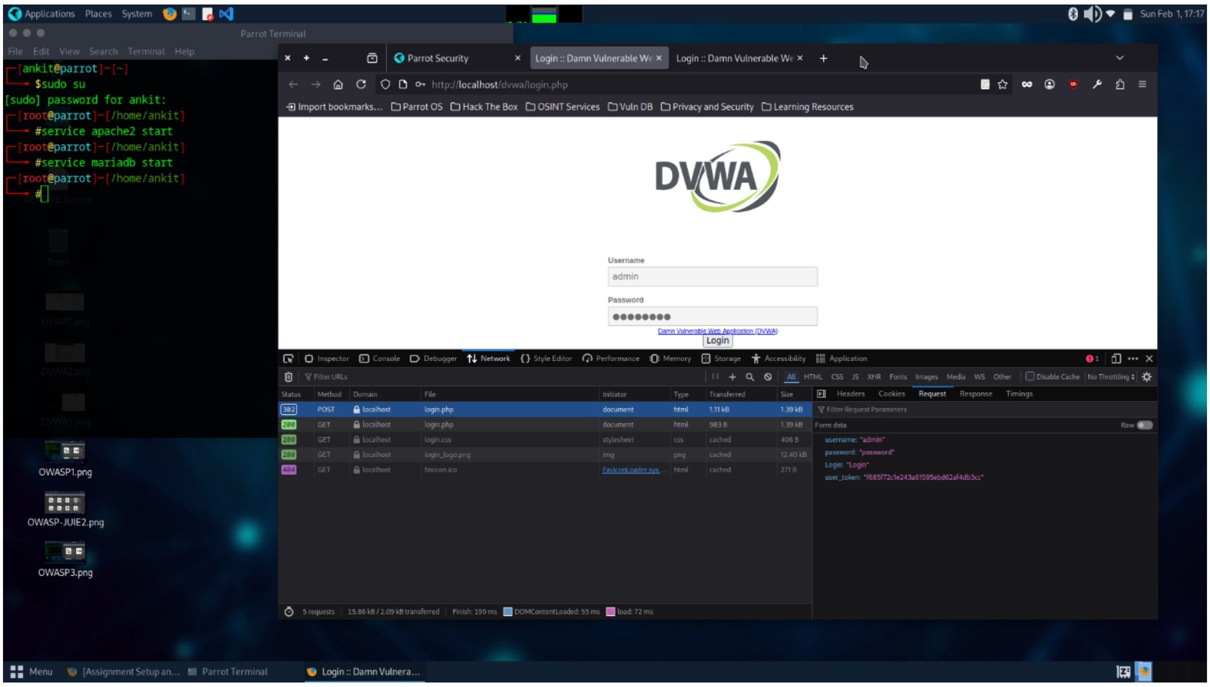
- Login=Login

Observation:

The login credentials are sent to the server using the POST method.

The username and password are visible in the request payload.

This shows how sensitive data travels from client to server.



```
┌─[ankit@parrot]─[~]
└──╼ $sudo su
[sudo] password for ankit:
┌─[root@parrot]─[/home/ankit]
└──╼ #service apache2 start
┌─[root@parrot]─[/home/ankit]
└──╼ #service mariadb start
┌─[root@parrot]─[/home/ankit]
└──╼ #
```

http://localhost/dvwa/login.php

Username: admin

Password: ●●●●●●●●

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	localhost	login.php	document	html	1.11 kB	1.39 kB
200	GET	localhost	login.php	document	html	983 B	1.39 kB
200	GET	localhost	login.css	stylesheet	css	cached	406 B
200	GET	localhost	login_logo.png	img	png	cached	12.40 kB
404	GET	localhost	favicon.ico	FaviconLoader.sys....	html	cached	271 B

Form data

```
username: "admin"
password: "password"
Login: "Login"
user_token: "f685f72c1e243a61595ebd62af4db3cc"
```

5 requests | 15.86 kB / 2.09 kB transferred | Finish: 199 ms | DOMContentLoaded: 55 ms | load: 72 ms

Form Request Observation (DVWA Command Injection)

URL: http://localhost/dvwa/vulnerabilities/exec/

Method: GET

Parameters:

- ip=127.0.0.1

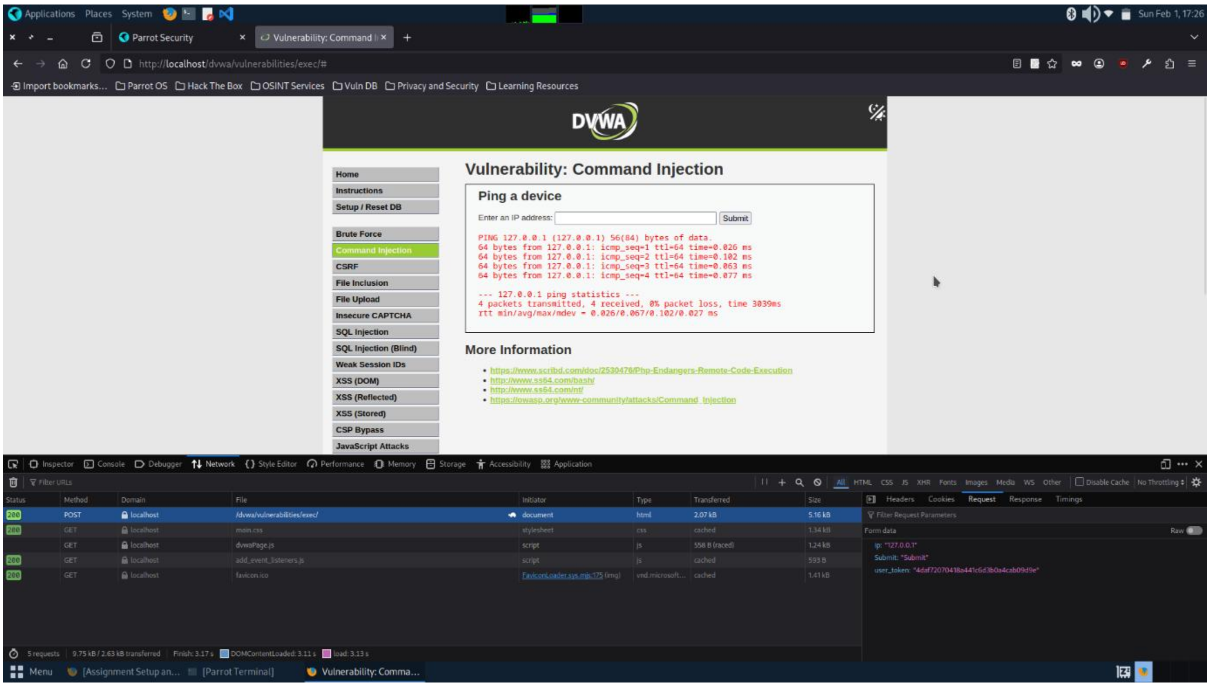
- Submit=Submit

Observation:

The input value is sent via GET method.

The parameters are visible directly in the URL.

This can be dangerous because attackers can manipulate input.



http://localhost/dvwa/vulnerabilities/exec/#

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.077 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3039ms
rtt min/avg/max/mdev = 0.026/0.067/0.102/0.027 ms
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	localhost	/dvwa/vulnerabilities/exec/	document	html	2.07 kB	5.16 kB
200	GET	localhost	main.css	stylesheet	css	cached	1.34 kB
	GET	localhost	dvwaPage.js	script	js	558 B (raced)	1.24 kB
200	GET	localhost	add_event_listeners.js	script	js	cached	593 B
200	GET	localhost	favicon.ico	FaviconLoader.sys.mjs:175 (img)	vnd.microsoft...	cached	1.41 kB

Form data

ip: "127.0.0.1"
Submit: "Submit"
user_token: "4daf72070418a441c6d3b0a4cab09d9e"

5 requests | 9.75 kB / 2.63 kB transferred | Finish: 3.17 s | DOMContentLoaded: 3.11 s | load: 3.13 s