



Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Lab #12

Instructor:

Ubaid Ullah

Fahad Waheed

You are a cyber security specialist who has been called upon to investigate a major cyber security breach. The company's web server has been compromised, and the attacker has attempted to exploit multiple vulnerabilities. You've been given the task of piecing together the attacker's intentions and uncovering the extent of the damage. With that in mind, your challenge is to answer the following questions:

1. What IP address does the attack seem to be originating from?

192.168.0.106

[illegible]

2. Which vulnerabilities do you think are being exploited, and what evidence do you have to support your findings?

- Path Traversal
- Remote File Inclusion
- SQL Injection
- Command Injection

```
192.168.0.106 - [16/Feb/2023:01:36:15 +0500] "GET /users.php HTTP/1.1" 200 1153 "-" Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - [16/Feb/2023:01:36:19 +0500] "POST /users.php HTTP/1.1" 200 1115 "http://192.168.0.101:9090/users.php" Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - [16/Feb/2023:01:36:25 +0500] "POST /users.php HTTP/1.1" 200 1116 "http://192.168.0.101:9090/users.php" Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - [16/Feb/2023:01:36:31 +0500] "POST /users.php HTTP/1.1" 200 1087 "http://192.168.0.101:9090/users.php" Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.0.106 - [16/Feb/2023:01:36:55 +0500] "GET /users.php HTTP/1.1" 200 1117 "sqlmap/1.6.11stable (https://sqlmap.org)"
192.168.0.106 - [16/Feb/2023:01:36:56 +0500] "GET /users.php HTTP/1.1" 200 1117 "sqlmap/1.6.11stable (https://sqlmap.org)"
192.168.0.106 - [16/Feb/2023:01:37:01 +0500] "POST /users.php HTTP/1.1" 200 1050 "sqlmap/1.6.11stable (https://sqlmap.org)"
```

3. How can we determine what web browser the attacker is using?

Firefox 102

[illegible]

4. Did the attacker use any automated tools during the attack? If so, can you identify the name of the tool and its purpose?

Attacker used sqlmap for sql injection

5. Which file was the attacker trying to access but couldn't due to limited server access?

```
--ad14d463-F--
HTTP/1.1 404 Not Found
Content-Length: 277
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

--ad14d463-E--
<!DOCTYPE HTML PUBLIC "-//IETF/DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr/>
<address>Apache/2.4.52 (Ubuntu) Server at 192.168.0.101 Port 9090</address>
</body></html>

--ad14d463-H--
Message: Warning. Pattern match "^(?:\s+):$" at REQUEST_HEADERS:Host [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735" [id "920500"] [tag "Host header is a numeric IP address"] [data "192.168.0.101:9090"] [severity "WARNING"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level-1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"] [tag "PCI/6.5.10"]
ModSecurity: [error] [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735" [id "920500"] [msg "Host header is a numeric IP address"] [data "192.168.0.101:9090"] [severity "WARNING"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level-1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname "192.168.0.101"] [uri "/database.php"] [unique_id "Y-1CNU0L0J151W0Yv0QGAaaaa"]
ModSecurity: [error] [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735" [id "920500"] [msg "Host header is a numeric IP address"] [data "192.168.0.101:9090"] [severity "WARNING"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level-1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname "192.168.0.101"] [uri "/database.php"] [unique_id "Y-1CNU0L0J151W0Yv0QGAaaaa"]
Apache-Handler: application/x-httpd-php
Stopwatch: 1676493367883282 1862 (- -)
Stopwatch: 1676493367883282 1862; combined=1138, p1=358, p2=339, p3=24, p4=116, p5=181, sr=77, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.5 (http://www.modsecurity.org/). OWASP_CRS/3.3.2.
Server: Apache/2.4.52 (Ubuntu)
Engine-Mode: "DETECTION_ONLY"

--ad14d463-Z--
```

- ```
192.168.0.106 - [16/Feb/2023:01:35:07 +0500] "GET /view.php?image=/etc/passwd HTTP/1.1" 200 202 "http://192.168.0.101:9090/images.php" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
```

An important secret was compromised. Can you figure it out? Hint: The secret you're looking for is not in a .sql or a .php file.

The attacker left a message for the server administrator. Find out what the message said, and also mention how you were able to find it.

[illegible]

```

192.168.0.106 - - [16/Feb/2023:01:35:00 +0500] "GET /images.php?file=red_vineyards.jpg HTTP/1.1" 302 2427 "ht
192.168.0.106 - - [16/Feb/2023:01:35:00 +0500] "GET /view.php?image=red_vineyards.jpg HTTP/1.1" 200 796956 "h
192.168.0.106 - - [16/Feb/2023:01:35:07 +0500] "GET /images.php?file=%2Fetc%2Fpasswd HTTP/1.1" 302 2422 "http
192.168.0.106 - - [16/Feb/2023:01:35:07 +0500] "GET /view.php?image=/etc/passwd HTTP/1.1" 200 202 "http://192
192.168.0.106 - - [16/Feb/2023:01:35:13 +0500] "GET /view.php?image=../etc/passwd HTTP/1.1" 200 203 "-" "Mozil
192.168.0.106 - - [16/Feb/2023:01:35:17 +0500] "GET /view.php?image=../../etc/passwd HTTP/1.1" 200 202 "-" "M
192.168.0.106 - - [16/Feb/2023:01:35:23 +0500] "GET /view.php?image=../../etc/passwd HTTP/1.1" 200 203 "-"
192.168.0.106 - - [16/Feb/2023:01:35:27 +0500] "GET /view.php?image=../../etc/passwd HTTP/1.1" 200 650
192.168.0.106 - - [16/Feb/2023:01:35:30 +0500] "GET /view.php?image=../../etc/shadow HTTP/1.1" 200 202
192.168.0.106 - - [16/Feb/2023:01:35:34 +0500] "GET / HTTP/1.1" 200 966 "-" "Mozilla/5.0 (X11; Linux x86_64;
192.168.0.106 - - [16/Feb/2023:01:35:36 +0500] "GET /command.php HTTP/1.1" 200 1019 "http://192.168.0.101:909

```

10. Based on this attack, what indicators of compromise can be used to detect future attacks?

- logs and alert are to be used to detect future attacks.
- Monitor logs and alerts
- Use IDS and IPS