TECHNICAL LAB REPORT

Student Name	Kareem Ibrahim Mahmoud Omar
Trainer Name	Amr Adel
National ID	30211122701897
Group Code	ONL3_ISS6_S2
Track	**Information Security Analyst**

1. Assessment Scope

Target IP / URL:
203.0.113.42____

Tools Used: [ ] Nmap   [ ] Nessus   [ ] Wireshark   [YES] Other

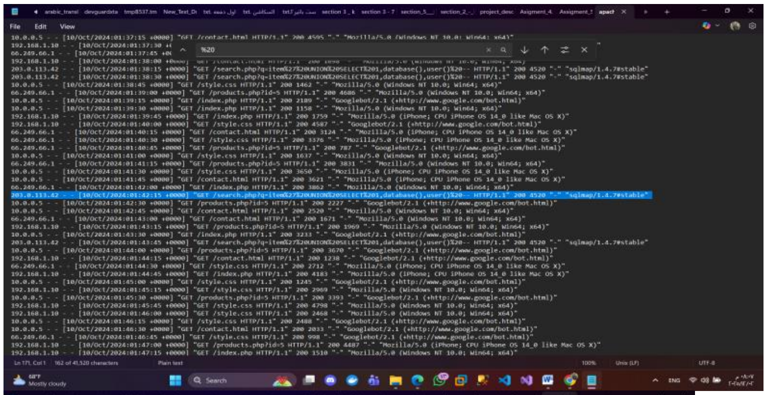
2. Findings Summary

Vulnerability Name	Severity	Status
SQL Injection Attempt	High	Confirmed
Malicious Automation (SQLMAP)	High	Confirmed
URL Encoding Injection (%27)	Medium	Confirmed

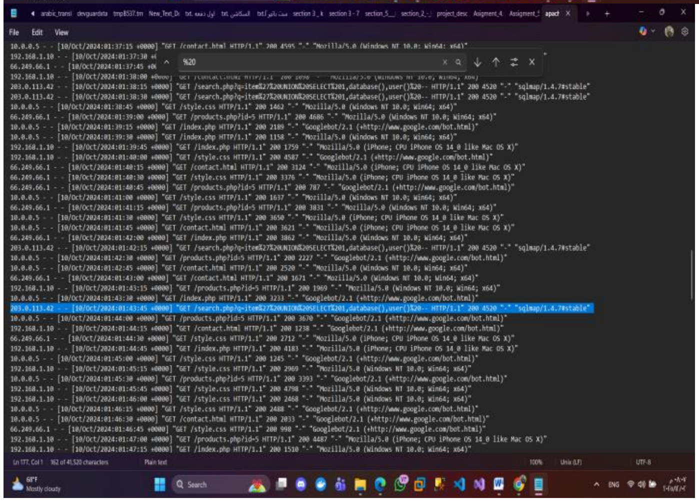
3. Technical Evidence

Paste screenshot verification below:

[PASTE SCREENSHOT HERE]



```
10.0.0.5 - - [10/Oct/2024:01:37:15 +0000] "GET /contact.html HTTP/1.1" 200 4595 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:37:30 +(                                                                    "
66.249.66.1 - - [10/Oct/2024:01:37:45 +0(
192.168.1.10 - - [10/Oct/2024:01:38:00 +0000] "GET /contact.html HTTP/1.1" 200 1090 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
203.0.113.42 - - [10/Oct/2024:01:38:15 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
203.0.113.42 - - [10/Oct/2024:01:38:30 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:38:45 +0000] "GET /style.css HTTP/1.1" 200 1462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:39:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 4686 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:39:15 +0000] "GET /index.php HTTP/1.1" 200 2189 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:39:30 +0000] "GET /index.php HTTP/1.1" 200 1158 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:39:45 +0000] "GET /index.php HTTP/1.1" 200 1759 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:40:00 +0000] "GET /style.css HTTP/1.1" 200 4587 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:40:15 +0000] "GET /contact.html HTTP/1.1" 200 3124 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:40:30 +0000] "GET /style.css HTTP/1.1" 200 3376 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:40:45 +0000] "GET /products.php?id=5 HTTP/1.1" 200 787 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:41:00 +0000] "GET /style.css HTTP/1.1" 200 1637 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:41:15 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3831 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:41:30 +0000] "GET /style.css HTTP/1.1" 200 3650 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
10.0.0.5 - - [10/Oct/2024:01:41:45 +0000] "GET /contact.html HTTP/1.1" 200 3621 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:42:00 +0000] "GET /index.php HTTP/1.1" 200 3862 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
203.0.113.42 - - [10/Oct/2024:01:42:15 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:42:30 +0000] "GET /products.php?id=5 HTTP/1.1" 200 2227 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:42:45 +0000] "GET /contact.html HTTP/1.1" 200 2520 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:43:00 +0000] "GET /contact.html HTTP/1.1" 200 1671 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:43:15 +0000] "GET /products.php?id=5 HTTP/1.1" 200 1969 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:43:30 +0000] "GET /index.php HTTP/1.1" 200 3233 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
203.0.113.42 - - [10/Oct/2024:01:43:45 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:44:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3670 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:44:15 +0000] "GET /contact.html HTTP/1.1" 200 1238 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:44:30 +0000] "GET /style.css HTTP/1.1" 200 2712 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:44:45 +0000] "GET /index.php HTTP/1.1" 200 4183 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
10.0.0.5 - - [10/Oct/2024:01:45:00 +0000] "GET /style.css HTTP/1.1" 200 1245 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:45:15 +0000] "GET /style.css HTTP/1.1" 200 2969 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:45:30 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3393 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:45:45 +0000] "GET /style.css HTTP/1.1" 200 4798 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:46:00 +0000] "GET /style.css HTTP/1.1" 200 2468 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:46:15 +0000] "GET /style.css HTTP/1.1" 200 2488 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:46:30 +0000] "GET /contact.html HTTP/1.1" 200 2033 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:46:45 +0000] "GET /style.css HTTP/1.1" 200 998 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:47:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 4487 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:47:15 +0000] "GET /index.php HTTP/1.1" 200 1510 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```



```
10.0.0.5 - - [10/Oct/2024:01:37:15 +0000] "GET /contact.html HTTP/1.1" 200 4595 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:37:30 +(                                                                    "
66.249.66.1 - - [10/Oct/2024:01:37:45 +0(
192.168.1.10 - - [10/Oct/2024:01:38:00 +0000] "GET /contact.html HTTP/1.1" 200 1090 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
203.0.113.42 - - [10/Oct/2024:01:38:15 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
203.0.113.42 - - [10/Oct/2024:01:38:30 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:38:45 +0000] "GET /style.css HTTP/1.1" 200 1462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:39:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 4686 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:39:15 +0000] "GET /index.php HTTP/1.1" 200 2189 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:39:30 +0000] "GET /index.php HTTP/1.1" 200 1158 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:39:45 +0000] "GET /index.php HTTP/1.1" 200 1759 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:40:00 +0000] "GET /style.css HTTP/1.1" 200 4587 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:40:15 +0000] "GET /contact.html HTTP/1.1" 200 3124 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:40:30 +0000] "GET /style.css HTTP/1.1" 200 3376 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:40:45 +0000] "GET /products.php?id=5 HTTP/1.1" 200 787 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:41:00 +0000] "GET /style.css HTTP/1.1" 200 1637 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:41:15 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3831 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:41:30 +0000] "GET /style.css HTTP/1.1" 200 3650 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
10.0.0.5 - - [10/Oct/2024:01:41:45 +0000] "GET /contact.html HTTP/1.1" 200 3621 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
66.249.66.1 - - [10/Oct/2024:01:42:00 +0000] "GET /index.php HTTP/1.1" 200 3862 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
203.0.113.42 - - [10/Oct/2024:01:42:15 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:42:30 +0000] "GET /products.php?id=5 HTTP/1.1" 200 2227 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:42:45 +0000] "GET /contact.html HTTP/1.1" 200 2520 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
66.249.66.1 - - [10/Oct/2024:01:43:00 +0000] "GET /contact.html HTTP/1.1" 200 1671 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:43:15 +0000] "GET /products.php?id=5 HTTP/1.1" 200 1969 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:43:30 +0000] "GET /index.php HTTP/1.1" 200 3233 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
203.0.113.42 - - [10/Oct/2024:01:43:45 +0000] "GET /search.php?q=item%27%20UNION%20SELECT%201,database(),user()%20-- HTTP/1.1" 200 4520 "-" "sqlmap/1.4.7#stable"
10.0.0.5 - - [10/Oct/2024:01:44:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3670 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:44:15 +0000] "GET /contact.html HTTP/1.1" 200 1238 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:44:30 +0000] "GET /style.css HTTP/1.1" 200 2712 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:44:45 +0000] "GET /index.php HTTP/1.1" 200 4183 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
10.0.0.5 - - [10/Oct/2024:01:45:00 +0000] "GET /style.css HTTP/1.1" 200 1245 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:45:15 +0000] "GET /style.css HTTP/1.1" 200 2969 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:45:30 +0000] "GET /products.php?id=5 HTTP/1.1" 200 3393 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:45:45 +0000] "GET /style.css HTTP/1.1" 200 4798 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.10 - - [10/Oct/2024:01:46:00 +0000] "GET /style.css HTTP/1.1" 200 2468 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
10.0.0.5 - - [10/Oct/2024:01:46:15 +0000] "GET /style.css HTTP/1.1" 200 2488 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
10.0.0.5 - - [10/Oct/2024:01:46:30 +0000] "GET /contact.html HTTP/1.1" 200 2033 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
66.249.66.1 - - [10/Oct/2024:01:46:45 +0000] "GET /style.css HTTP/1.1" 200 998 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
192.168.1.10 - - [10/Oct/2024:01:47:00 +0000] "GET /products.php?id=5 HTTP/1.1" 200 4487 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)"
192.168.1.10 - - [10/Oct/2024:01:47:15 +0000] "GET /index.php HTTP/1.1" 200 1510 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```

4. Recommendations

1. Implement Input Validation & Sanitization

Apply strict filtering to user input on the search page to prevent the entry of symbols such as ', UNION, and SELECT.
2. Use Prepared Statements / Parameterized Queries

Modify the code to use secure queries that prevent the execution of user-generated SQL commands.
3. Enable Web Application Firewall (WAF)

Enable WAF, such as ModSecurity, to automatically prevent SQL Injection attacks and block suspicious bots.
4. Block Attacker IP (203.0.113.42)

Add the attacker's IP to the server-level or firewall block list to prevent re-attacks.
5.Implement Rate Limiting on Search Endpoint

Limit the number of requests allowed per IP per minute to prevent automated attacks (bots/SQLMAPs).
6.Disable Detailed Error Messages

Disable detailed error messages that could help an attacker understand the database structure
7. Regular Log Monitoring

Monitor server logs daily for early detection of abnormal activity.

Financial

The total cost for performing the log analysis, confirming the attack vector, identifying the malicious IP, documenting all findings, and delivering the final technical report is

22 USD (one-time analysis fee).

This fee covers all work related to investigation, reporting, and recommendations.