DVWA – OWASP ZAP cheat-sheet

DVWA

Σε ένα debian based λειτουργικό όπως το KALI

Dependence:

apt install php-gd - (Μπορεί να μην είναι απαραίτητο)

Installation:

cd /var/www/html

sudo git clone https://github.com/digininja/DVWA.git

Configuration:

sudo chmod -R 777 DVWA

cd /DVWA/config/

sudo cp config.inc.php.dist config.inc.php

nano config.inc.php -(Προτείνω να αλλάξετε μόνο το password !)

DB configuration:

service mysql start or service mariadb start

mysql (Εάν είναι default το configuration δεν χρειάζεται password απλώς πατάτε enter)

```
mysql> create database dvwa;
Query OK, 1 row affected (0.00 sec)

mysql> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.01 sec)

mysql> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

Περίπτωση που θέλετε να ξαναχρησιμοποιήσετε την βάση που φτιάξατε πριν:

```
MariaDB [(none)]> use dvwa
Database changed
MariaDB [dvwa]> ^DBye
```

Apache configuration:

service apache2 start

cd /etc/php/8.1/apache2

nano php.ini

-- allow_url_include = On

service apache2 reload

Start of the service:

Ανοίγουμε browser και μπαίνουμε στο Localhost (127.0.0.1)

Αρχικά μπαίνουμε με τα εξής credentials [dvwa – p@ssw0rd]

Πατάμε create/reset database

Έπειτα ξανα-μπαίνουμε με τα εξής credentials [admin password]

OWASP ZAP

Το κατεβάζουμε και το κάνουμε εγκατάσταση στα windows όπως ένα οποιοδήποτε πρόγραμμα - https://www.zaproxy.org/download/

Manual explore configuration:

Στο μενού πηγαίνουμε Tools-options και κάνουμε τις παρακάτω ενέργειες.

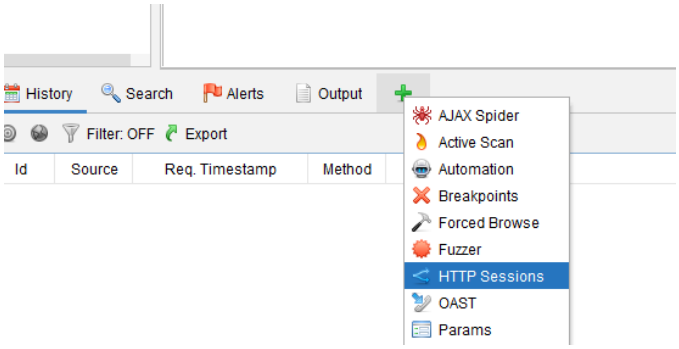
Έπειτα ενεργοποιούμε την proxy λειτουργία στον browser – Για τον firefox – options-general-more – enable proxy

Έπειτα γυρίζουμε στο zap και πάμε tools-options-dynamic ssl cert και το κατεβάζουμε.

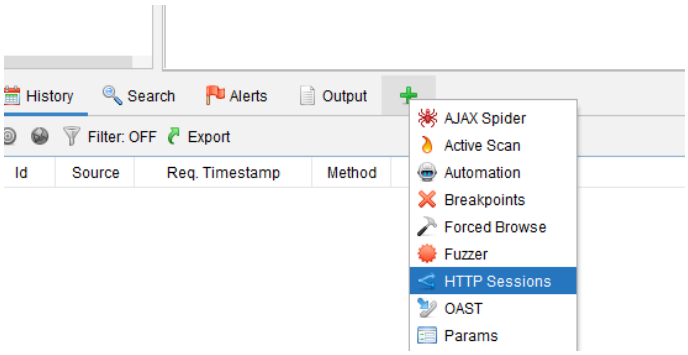
Κάνουμε import το cert στον firefox -properties – certificates-view-import- …

ZAP TIPS

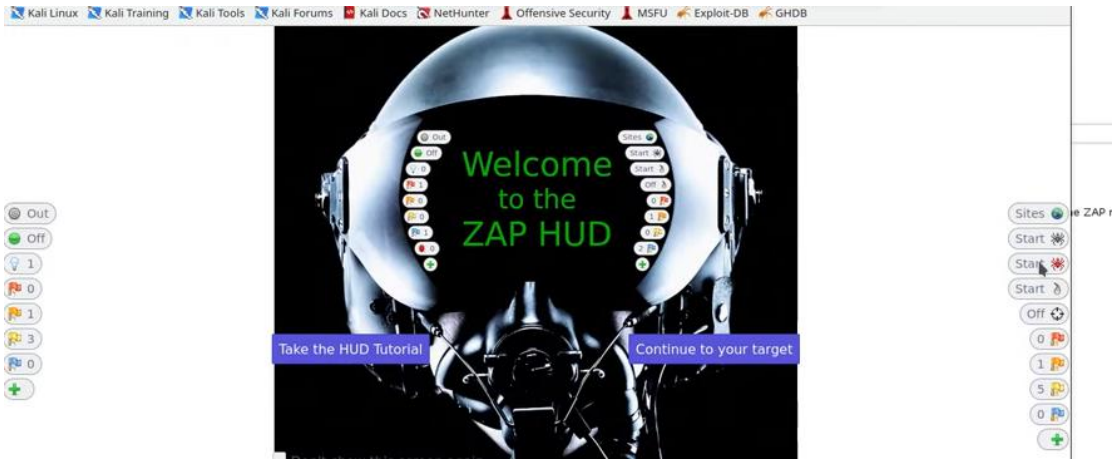
-Ενεργοποιούμε το button για τα http sessions



-Βάζουμε την IP του μηχανήματος dvwa και εκτελούμε το scan πατώντας -select – launch-browser



Έτσι εμφανίζεται μέσω του browser το DVWA μηχάνημα



DVWA experiments

Βάζουμε τα credentials (admin - password) στον DVWA

Πάμε στο inspect element και βρίσκουμε το PHPSESID

Έπειτα στο zap ανοίγουμε τα HTTP sessions και βρίσκουμε το αντίστοιχο ID , πατάμε δεξί κλικ -set as active

Έπειτα μέσω των βοηθητικών κουμπιών του zap στον browser πατάμε start active scan

Στα αριστερά φορτώνουν σιγά σιγά σε φακέλους όλες οι ευπάθειες του DVWA

Bruteforce

Για την εκτέλεση του bruteforce βρίσκουμε τον αντίστοιχο φάκελο

Έπειτα δεξί κλικ – fuzzer – και επιλέγουμε το περιεχόμενο των μεταβλητών username ή password. Με το που γίνει η επιλογή ενεργοποιείται το κουμπί add. Το πατάμε ακολουθούμε τα βήματα και εκτελούμε.

Στον ZAP θα εμφανιστεί ο σωστός κωδικός ανάμεσα στους πολλούς. Τον αναγνωρίζουμε από το διαφορετικό μέγεθος και το σύμβολο reflected.