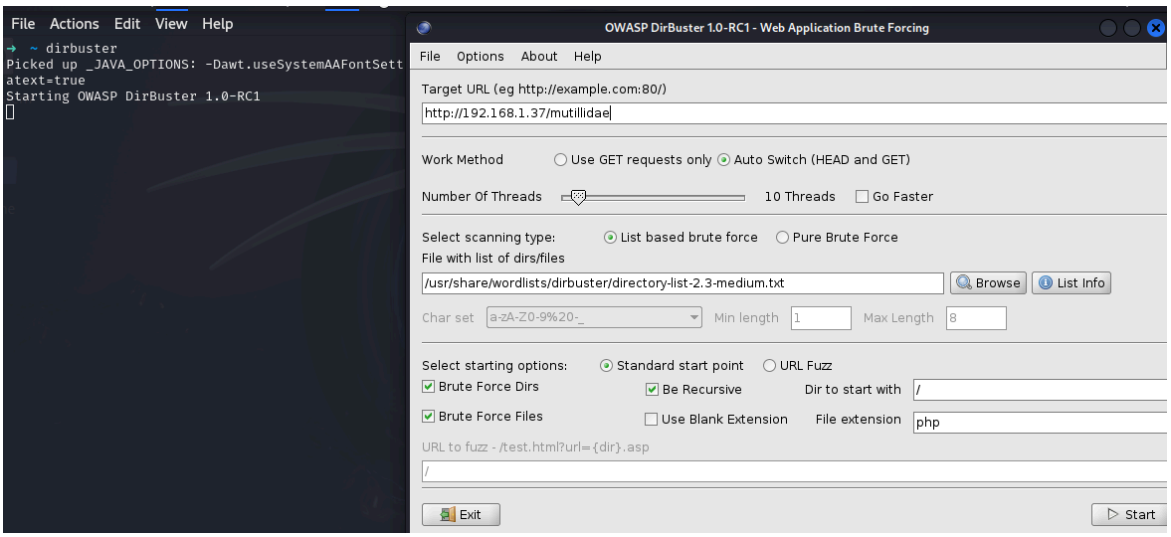
EJERCICIOS INTRODUCCIÓN WEB

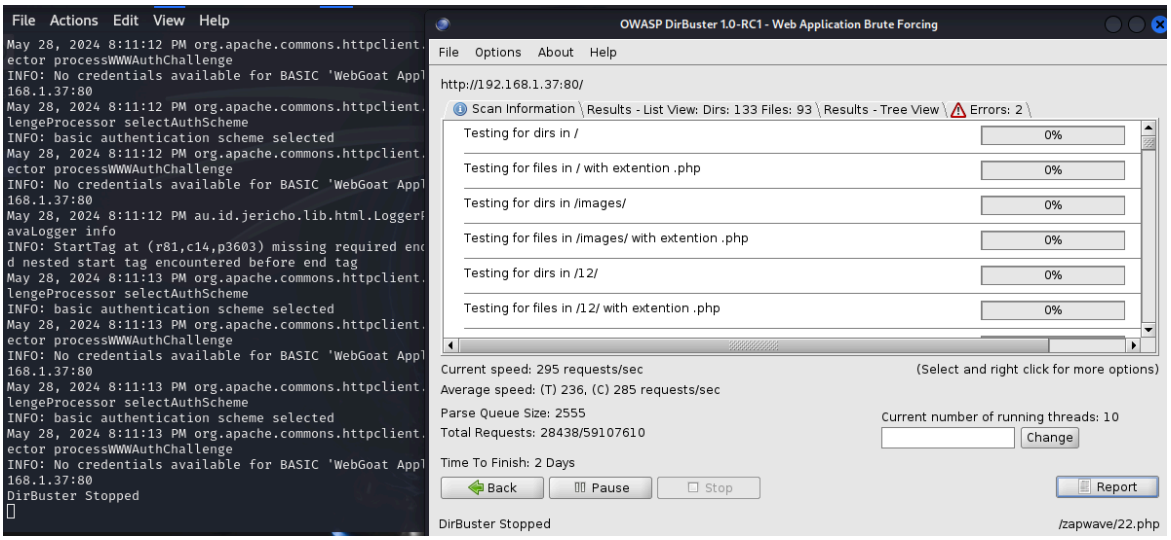
Prerrequisitos

Kali Linux
OWASP BWA

Ejercicio 1 - Dirbuster

Realizar enumeración de la aplicación web Mutillidae II utilizando Dirbuster y un diccionario de directorios de tamaño medio

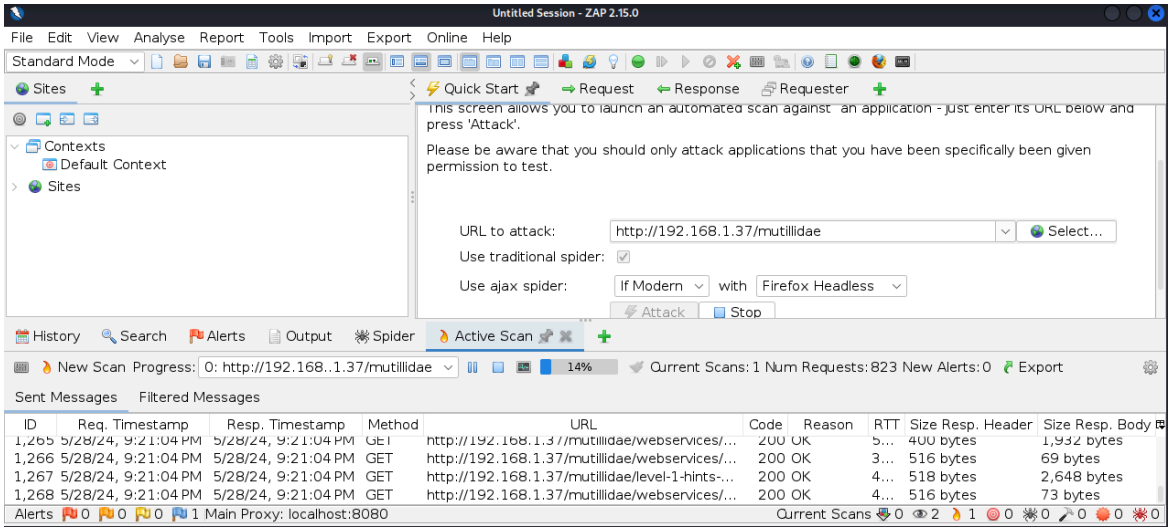




Ejercicio 2 - Nikto, Nessus y OWASP Zap

Realizar un análisis de vulnerabilidades con Nikto a la aplicación web Mutillidae II volcando los resultados en un documento ".txt"
(Opcional) Realizar un análisis de vulnerabilidades con Nessus al servidor web OWASP BWA
Realizar un análisis de vulnerabilidades con OWASP Zap a la aplicación web Mutillidae II

```
→  ~ nikto -h http://192.168.1.37/mutillidae/ -output results.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
---------
+ Target IP:          192.168.1.37
+ Target Hostname:    192.168.1.37
+ Target Port:        80
+ Start Time:         2024-05-28 20:18:00 (GMT2)
---------------------------------------------------------------------------
---------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.
30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.
5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2
.0.4 Perl/v5.10.1
+ /mutillidae/: Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.3
0.
```


Untitled Session - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://192.168.1.37/mutillidae
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox Headless
Attack
Stop
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress:
0: http://192.168..1.37/mutillidae
14%
Current Scans: 1 Num Requests: 823 New Alerts: 0
Export
Sent Messages
Filtered Messages
ID
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
1,266 5/28/24, 9:21:04 PM 5/28/24, 9:21:04 PM GET http://192.168.1.37/mutillidae/webservices/... 200 OK 3... 516 bytes 69 bytes
1,267 5/28/24, 9:21:04 PM 5/28/24, 9:21:04 PM GET http://192.168.1.37/mutillidae/level-1-hints-... 200 OK 4... 518 bytes 2,648 bytes
1,268 5/28/24, 9:21:04 PM 5/28/24, 9:21:04 PM GET http://192.168.1.37/mutillidae/webservices/... 200 OK 4... 516 bytes 73 bytes
Alerts 0 0 0 1 Main Proxy: localhost:8080
Current Scans 0 2 1 0 0 0 0 0

Ejercicio 3 - Nikto y OWASP Zap

Evaluar los resultados del escaneo con Nikto y explicar en detalle alguna de las vulnerabilidades encontradas Evaluar los resultados del escaneo con OWASP Zap y explicar en detalle la vulnerabilidad que mas alertas haya suscitado

nikto: CVE-2003-1418 - CVE-2000-0649

CVE-2003-1418 Detalle

MODIFICADO

Esta vulnerabilidad ha sido modificada desde la última vez que fue analizada por el NVD. Está a la espera de un nuevo análisis que puede dar lugar a nuevos cambios en la información proporcionada.

Descripción

Apache HTTP Server v1.3.22 a 1.3.27 en OpenBSD permite a atacantes remotos obtener información confidencial a través de (1) el encabezado ETag, que revela el número de inodo, o (2) el límite MIME multiparte, que revela los ID de procesos secundarios (PID).

INFORMACIÓN RÁPIDA

Entrada del diccionario CVE:
CVE-2003-1418
NVD Fecha de publicación:
31/12/2003
Última modificación de NVD:
19/10/2017
Fuente:
MITRE

Gravedad CVSS versión 4.0 | CVSS versión 3.x | CVSS versión 2.0

Severidad y métricas de CVSS 4.0:

NVD **NIST:** NVD N/A La evaluación NVD aún no se ha proporcionado.

CVE-2000-0649 Detalle

Descripción

IIS 4.0 permite a atacantes remotos obtener la dirección IP interna del servidor a través de una solicitud HTTP 1.0 para una página web que está protegida por autenticación básica y no tiene ningún dominio definido.

Gravedad

CVSS versión 4.0 | CVSS versión 3.x | CVSS versión 2.0

Severidad y métricas de CVSS 4.0:

NIST: NVD N/A La evaluación NVD aún no se ha proporcionado.

INFORMACIÓN RÁPIDA

Entrada del diccionario CVE:
CVE-2000-0649
NVD Fecha de publicación:
13/07/2000
NVD Última modificación:
23/11/2020
Fuente:
MITRE

zap: Top_10_2013-A1 - Top_10_2013-A10

OWASP Top 10 2013: actualización de los riesgos más extendidos asociados a las aplicaciones web

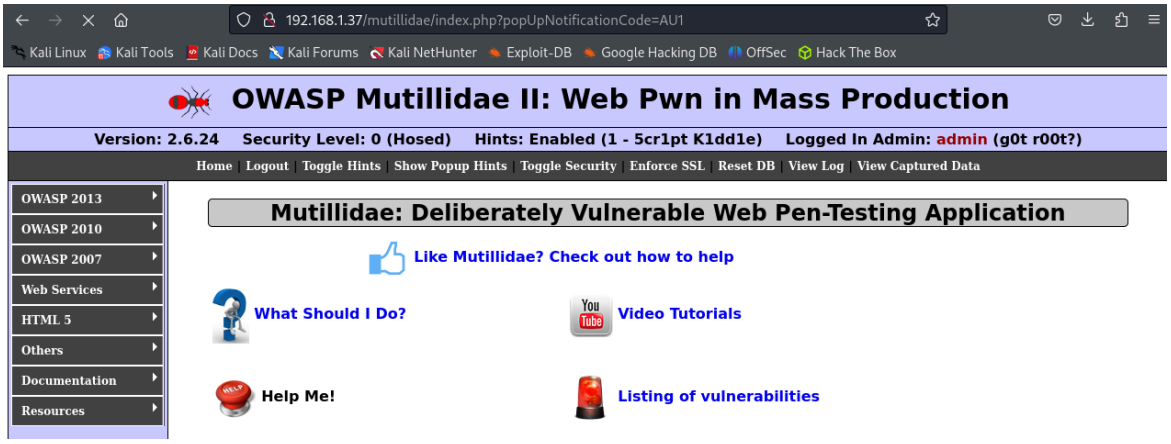
El proyecto OWASP Top 10, referente y uno de los más emblemáticos de esta organización, ha visto recientemente una nueva actualización. Con una mentalidad de divulgación y con el claro objetivo de educar, tanto a las organizaciones como a todas aquellas personas que, de una u otra manera, están implicadas en el ciclo de vida de las aplicaciones, este Top 10 enumera y describe los diez riesgos más críticos y extendidos que sufren las aplicaciones web en la actualidad. Respecto a su anterior versión, la de 2010, cabe destacar la incorporación de una nueva categoría para considerar el riesgo asociado al uso de componentes vulnerables conocidos.

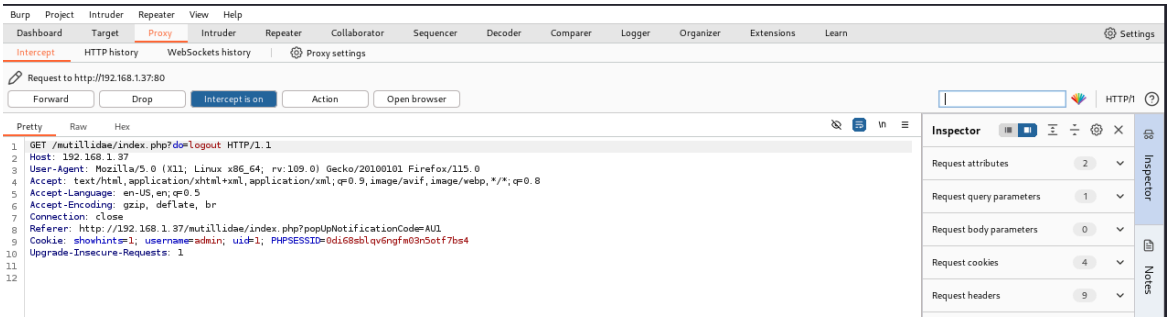
Vicente Aguilera Díaz

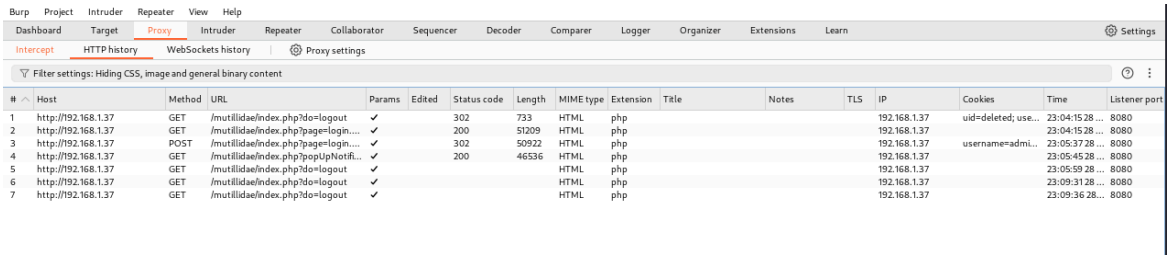
OWASP Top 10 2010 (versión anterior)	OWASP Top 10 2013 (versión actual)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cyrptographic Storage (combinado con 2010-A9)	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access (ampliado en 2013-A7)	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
Incluído en la categoría 2010-A6	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Combinado con 2010-A7 en la nueva categoría 2013-A6

Ejercicio 4 - Burp Suite

Utilizando Burp Suite y Firefox, cargar la web de Mutillidae II sección "Login/Register"
Añadir Mutillidae II en el alcance
Interceptar la petición de login con las credenciales admin - admin
Dejar de capturar peticiones para poder continuar y acceder
Listar las peticiones HTTP que hemos hecho
Filtrar y listar únicamente las peticiones de Mutillidae II






Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP Cookies Time Listener port
1 http://192.168.1.37 GET /mutillidae/index.php?do=logout ✔ 302 733 HTML php 192.168.1.37 uid=deleted; use... 23:04:15 28 ... 8080
2 http://192.168.1.37 GET /mutillidae/index.php?page=login.... ✔ 200 51209 HTML php 192.168.1.37 23:04:15 28 ... 8080
3 http://192.168.1.37 POST /mutillidae/index.php?page=login.... ✔ 302 50922 HTML php 192.168.1.37 username=admi... 23:05:37 28 ... 8080
4 http://192.168.1.37 GET /mutillidae/index.php?popUpNotifi... ✔ 200 46536 HTML php 192.168.1.37 23:05:45 28 ... 8080
5 http://192.168.1.37 GET /mutillidae/index.php?do=logout ✔ HTML php 192.168.1.37 23:05:59 28 ... 8080
6 http://192.168.1.37 GET /mutillidae/index.php?do=logout ✔ HTML php 192.168.1.37 23:09:31 28 ... 8080
7 http://192.168.1.37 GET /mutillidae/index.php?do=logout ✔ HTML php 192.168.1.37 23:09:36 28... 8080