

EJERCICIOS INTRODUCCIÓN WEB

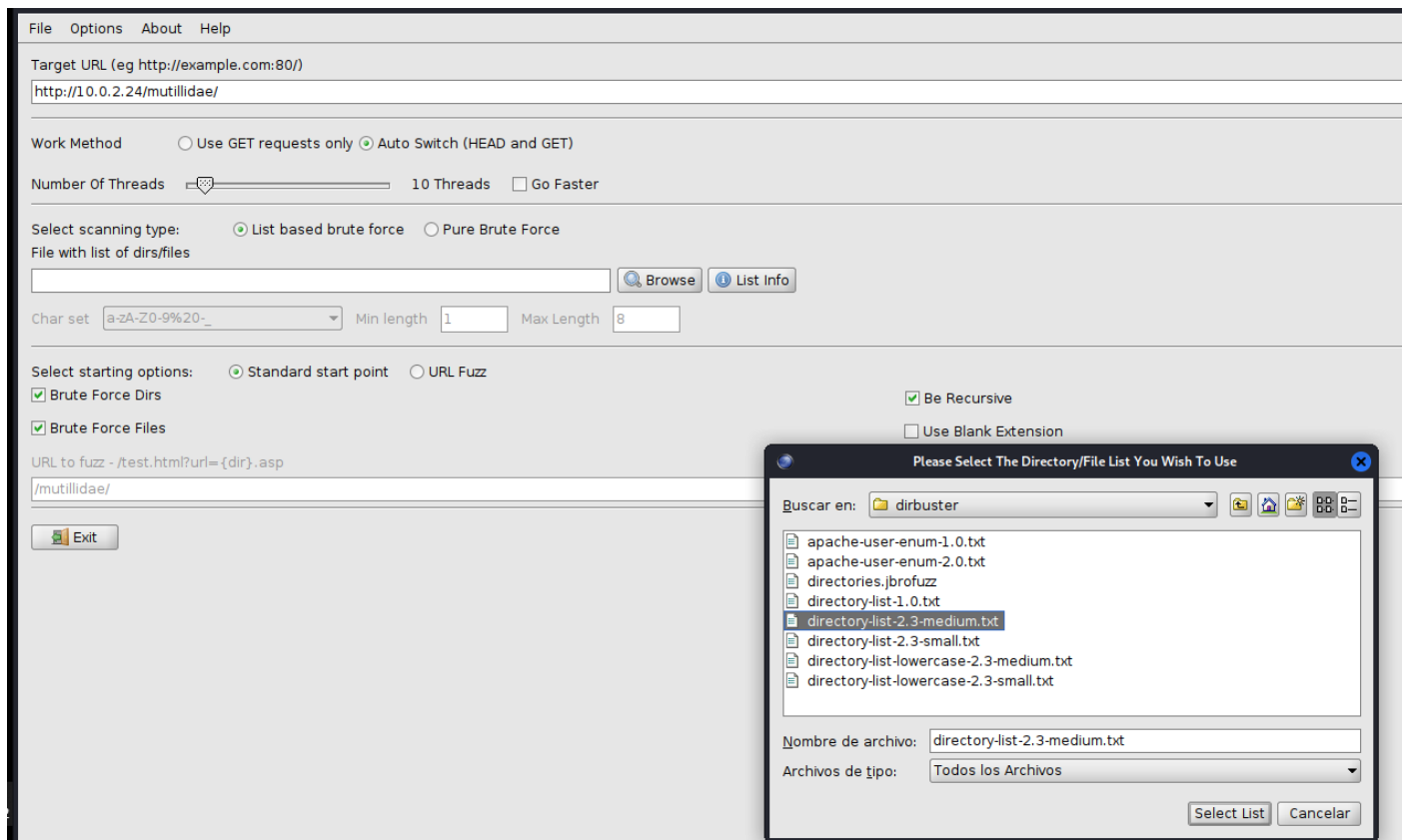
Prerrequisitos

- Kali Linux
- OWASP BWA

Ejercicio 1 - Dirbuster

- Realizar un mapa de la aplicación web Mutillidae II utilizando Dirbuster y un diccionario de nombres de tamaño medio.

Paso 1: ingresamos a la maquina OWASP BWA y abrimos el url en Kali y abrir dirbuster y completar los campos



Paso 2: se realiza el mapeo de Mutillidae II utilizando diccionario de nombres de tamaño medio. Este mapeo no ha culminado se hace a efectos de notar que el mapeo se realizo correctamente.

http://10.0.2.24:80/mutillidae/					
Scan Information Results - List View: Dirs: 127 Files: 52 Results - Tree View Errors: 2					
Type	Found	Response	Size		
Dir	/mutillidae/images/	200	10736		
Dir	/mutillidae/index/	200	46978		
File	/mutillidae/index.php	200	46978		
Dir	/mutillidae/home/	500	572		
Dir	/mutillidae/	200	47059		
File	/mutillidae/home.php	500	572		
Dir	/mutillidae/login/	500	1629		
Dir	/mutillidae/register/	500	416		
File	/mutillidae/login.php	500	1629		
File	/mutillidae/register.php	500	416		
Dir	/	200	29003		
File	/mutillidae/images/hints.html	200	17583		
Dir	/images/	200	1836		
Dir	/mutillidae/images/hints_files/	200	1283		
Dir	/2006/	501	551		
Dir	/mutillidae/images/gritter/	200	2305		
Dir	/icons/	200	73405		
Dir	/12/	503	525		
Dir	/11/	503	525		
Dir	/10/	503	525		
Dir	/cgi-bin/	200	1442		
Dir	/2005/	503	525		
Dir	/1/	503	525		
Dir	/09/	503	525		
Dir	/01/	503	525		
Dir	/08/	503	525		
Dir	/06/	503	525		
Dir	/2/	503	525		
Dir	/07/	503	525		
File	/mutillidae/set-up-database.php	200	5477		
Dir	/mutillidae/webservices/soap/	200	2124		
Dir	/mutillidae/webservices/	200	1625		
File	/mutillidae/webservices/soap/ws-user-account.php	200	9775		
Dir	/mutillidae/webservices/rest/	200	1484		
Dir	/05/	503	525		
File	/mutillidae/webservices/rest/ws-user-account.php	200	3841		
Dir	/04/	503	525		
Dir	/03/	503	525		
File	/mutillidae/webservices/soap/ws-lookup-dns-record.php	200	5343		
Dir	/02/	503	525		
File	/mutillidae/framer.html	200	1916		
File	/mutillidae/webservices/soap/ws-hello-world.php	200	5251		
Dir	/mutillidae/documentation/	200	2489		
File	/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf	200	1538682		
Dir	/mutillidae/includes/	200	5508		
File	/mutillidae/includes/pop-up-help-context-generator.php	200	640		
Dir	/mutillidae/javascript/	200	2292		

http://10.0.2.24:80/mutillidae/

Scan Information | Results - List View: Dirs: 147 Files: 54 | Results - Tree View | Errors: 2 |

Directory Structure		Response Code	Response Size
mutillidae	200	47059	
webservices	200	1625	
images	200	1836	
2006	501	551	
icons	200	73405	
12	503	525	
11	503	525	
10	503	525	
cgi-bin	200	1442	
2005	503	525	
1	503	525	
09	503	525	
01	503	525	
08	503	525	
06	503	525	
2	503	525	
07	503	525	
mutillidae	???	???	
05	503	525	
04	503	525	
03	503	525	
02	503	525	
3	503	525	
13	503	525	
4	503	525	
14	503	525	
15	503	525	
16	503	525	
2004	503	525	
18	503	525	
20	503	525	
21	503	525	
5	503	525	
22	503	525	
6	503	525	
19	503	525	
24	503	525	

Ejercicio 2 - Nikto

- Realizar un análisis de vulnerabilidades a la aplicación web Mutillidae II utilizando Nikto.

Paso 1: se abre nikto en la terminal de Kali y se ejecuta nikto -host <http://10.0.2.24/mutillidae/>

```
(root@kali)~# nikto -host http://10.0.2.24/mutillidae/
- Nikto v2.1.6

+ Target IP: 10.0.2.24
+ Target Hostname: 10.0.2.24
+ Target Port: 80
+ Start Time: 2022-12-19 23:44:11 (GMT1)

OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Not Logged In

+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 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
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ PHP/5.3.2-lubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 7913 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2022-12-19 23:44:24 (GMT1) (13 seconds)

+ 1 host(s) tested
```

Paso 2: análisis de resultados.

En el primero punto el tipo de servidor esta expuesto. Apache, Ubuntu y la versión, lo cual es una sobreexposición de información.

El anticlickjacking no está presente, esta es una vulnerabilidad ya que al clicar cualquier usuario que esta navegando puede ser un link de descarga de malwares, etc.

Si el servidor no está configurado para devolver un encabezado 'X-XSS-Protection', significa que cualquier página de este sitio web podría correr el riesgo de sufrir un ataque Cross-Site Scripting (XSS).

Si el encabezado http "X-Content-Type-Options" está configurado cuando el navegador obtiene una respuesta del servidor web y no lo reconoce intenta averiguar el contenido de esta petición y como manejarlo, si esto no está configurado puede llevar a problemas de seguridad. Por ejemplo, si una página permite adjuntar imágenes jpg y un atacante adjunta una imagen como extensión de jpg siendo este un html, puede descargarlo.

Si el directorio CGI no existe o no ha sido encontrado, es muy fácil para un atacante explotar esta vulnerabilidad ya que este directorio analiza y filtra la entrada de un usuario y se pueden emitir varios parámetros o comandos a través de URL y así el atacante puede ingresar y explotar cualquier vulnerabilidad.

Se puede notar también que hay varios paquetes desactualizados, y esto supone un problema siempre ya que cada vez aparecen vulnerabilidades y tipos de ataques nuevos y si los paquetes están desactualizados evidentemente son vulnerables ya que no están preparados para afrontar ataques.

La herramienta menciona justamente que los paquetes mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 y versiones anteriores son vulnerables a un desbordamiento de búfer remoto que puede permitir un shell remoto.

El http trace method esta activo, lo que hace ver que el host es vulnerable al XST, cross-site tracing que implica el uso de cross-site scripting, el XST puede usarse como método para robar cookies del usuario a través de XSS.

Ejercicio 3 - Burp Suite

- Utilizando Burp Suite como proxy, y Firefox, cargar la web de Mutillidae II, sección "Login/Register"

10.0.2.24/mutillidae/index.php?page=login.php

Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecNessus Essentials / Fo...

 **OWASP Mutillidae II: Web Pwn in Mass Production**

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

HomeLogin/RegisterToggle HintsShow Popup HintsToggle SecurityEnforce SSLReset DBView LogView Captured Data

Login

 Back

 Help Me!

 Hints

Please sign-in

Username

Password

Login

Dont have an account? [Please register here](#)

- Interceptar la petición de login con las credenciales:
Username: admin Password: admin
- Continuar y acceder

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' section shows a request to http://10.0.2.24:80. The 'Raw' view displays the following request details:

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 10.0.2.24
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 59
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; PHPSESSID=4m2tuvr5us9ah5b4oobo0lasr6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 username=admin&password=admin&login-php-submit-button=Login
```

- Listar las peticiones HTTP que hemos hecho en Burp

Burp	Project	Intruder	Repeater	Window	Help												
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extensions	Learn							
Intercept	HTTP history	WebSockets history		Options													
Filter: Hiding CSS, image and general binary content																	
# ^	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener	
1	http://10.0.2.24	GET	/			200	28533	HTML		owaspbwa OWASP Brok...			10.0.2.24		01:01:07 20 di...	8080	
2	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=4m2tu...	01:01:11 20 di...	8080	
3	http://10.0.2.24	GET	/mutillidae/index.php?page=login.php	✓		200	50726	HTML	php				10.0.2.24		01:01:24 20 di...	8080	
7	http://10.0.2.24	POST	/mutillidae/index.php?page=login.php	✓				HTML	php				10.0.2.24		01:03:16 20 di...	8080	
8	http://10.0.2.24	GET	/mutillidae/index.php?page=login.php	✓				HTML	php				10.0.2.24		01:04:48 20 d...	8080	
9	http://10.0.2.24	GET	/dvwa										10.0.2.24		01:07:33 20 di...	8080	
10	http://10.0.2.24	GET	/dvwa/										10.0.2.24		01:07:33 20 di...	8080	
11	http://10.0.2.24	GET	/WebGoat/attack										10.0.2.24		01:07:41 20 di...	8080	
12	http://10.0.2.24	GET	/dvwa/										10.0.2.24		01:08:33 20 di...	8080	
13	http://10.0.2.24	GET	/mutillidae/										10.0.2.24		01:08:51 20 di...	8080	
14	http://ocsp.digicert.com	POST	/	✓									192.16.58.8		01:10:04 20 di...	8080	
17	http://10.0.2.24	GET	/dvwa/										10.0.2.24	01:10:10 20 di...	8080		
18	http://10.0.2.24	GET	/mutillidae/										10.0.2.24	01:13:06 20 di...	8080		
19	http://10.0.2.24	GET	/mutillidae/										10.0.2.24	01:13:07 20 di...	8080		

- Filtrar y listar únicamente las de Mutillidae II

Burp	Project	Intruder	Repeater	Window	Help											
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extensions	Learn						
Intercept	HTTP history	WebSockets history	Options													
Filter: Hiding out of scope items; hiding CSS, image and general binary content																
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=4m2tu...	01:01:11 20 di...	8080
3	http://10.0.2.24	GET	/mutillidae/index.php?page=login.php	✓		200	50726	HTML	php				10.0.2.24		01:01:24 20 di...	8080
7	http://10.0.2.24	POST	/mutillidae/index.php?page=login.php	✓		302	50892	HTML	php				10.0.2.24	username=admin; ...	01:03:16 20 di...	8080
8	http://10.0.2.24	GET	/mutillidae/index.php?page=login.php	✓		200	50796	HTML	php				10.0.2.24		01:04:48 20 d...	8080
13	http://10.0.2.24	GET	/mutillidae/			200	46085	HTML					10.0.2.24		01:08:51 20 di...	8080
18	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=g0rslu...	01:13:06 20 di...	8080
19	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=67123...	01:13:07 20 di...	8080
20	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=auum...	01:13:07 20 di...	8080
21	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=9jea5...	01:13:08 20 di...	8080
22	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=rftn3bj...	01:13:08 20 di...	8080
23	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=3a6q1...	01:13:08 20 di...	8080
24	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=kjkr2l4...	01:13:21 20 di...	8080
25	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=2741v...	01:13:23 20 di...	8080
27	http://10.0.2.24	GET	/mutillidae/			200	46126	HTML					10.0.2.24	PHPSESSID=s19ee...	01:13:41 20 di...	8080