



[SOAL 1][*Forgot My Pass*]

NAMA TIM : *Pejuang Ar-Rahman*

ZONA : [*2 Jawa & Madura*]

Hari/Tanggal : Selasa, 21 Maret 2017

Ketua Tim	
1.	Ravi Dharmawan
Member	
1.	
2.	

Table of Contents

Capture The Flag Report

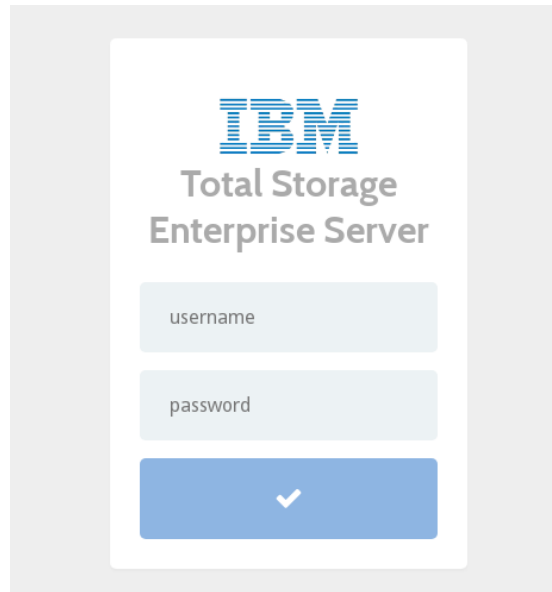
1. Executive Summary

Deskripsi Soal : *Bujang kehilangan user dan password salah satu [perangkatnya](#)
Bantu bujang untuk menemukan password tersebut dan dapatkan flagnya.*

Perangkat yang dimaksud berada di alamat <http://alianyang.screen6.id/>

2. Technical Report

Ketika URL <http://alianyang.screen6.id/> maka terdapat halaman login seperti ini :



<http://alianyang.screen6.id>

Dari halaman login diatas terdapat clue nama perangkat yang harus dicari tahu username dan passwordnya adalah IBM Total Storage Enterprise Sever.

Dengan modal googling, kami mendapatkan website yang memberi informasi username dan password default untuk login ke perangkat IBM Total Storage Enterprise Server. Username dan Password defaultnya adalah

Username : storwatch

Password : specialist

Gunakan password username dan password tersebut untuk login maka akan mendapatkan flag

3. Conclusion

Untuk menyelesaikan *challenge* ini, kita harus mencari username dan password default dari IBM Total Storage Server. Username dan password default tersebut didapatkan setelah googling. Login menggunakan username dan password default untuk mendapatkan flag.



Flag

SCREEN6{bubur_pedas}

OK

FLAG : **SCREEN6{bubur_pedas}**



[SOAL 2][QR Login]

Table of Contents

Capture The Flag Report

1. Executive Summary

Deskripsi Soal : *Demi menjaga keamanan websitenya[/web], bujang membuat sebuah sistem login dengan menggunakan QR Code. Ada yang bisa menembus sistem login tersebut?*

Dari soal diberikan URL <http://qrlogin.i-unteam.org> yang merupakan halaman login menggunakan QR Code.

TAMBAH QR CODE

LOGIN

2. Technical Report

Hal yang terpikirkan pertama kali oleh kami adalah SQL Injection untuk bypass halaman login. Tetapi yang membuat berbeda adalah halaman login ini menggunakan QR Code.

Untuk mencobanya kami mencoba membuat QR Code secara online di <https://www.the-qrcode-generator.com/> lalu untuk textnya kami isi dengan

' OR 1=1 LIMIT 1 #


Lalu didapatkan QR Code seperti ini



Setelah itu kami mencoba untuk mensubmit QR Code tersebut di halaman login yang disediakan.

TAMBAH QR CODE

test1.png



LOGIN

Setelah klik login maka akan mendapatkan flag



Login Sukses

Flagnya Adalah : `SCREEN6{enggang_gading_maskot_kalbar}`

OK

3. Conclusion

Untuk menembus halaman login tersebut, buatlah QR Code yang berisi 'OR 1=1 LIMIT 1 #. String tersebut berfungsi untuk menembus halaman login yang memiliki celah SQL Injection. Setelah membuat QR Code, submitlah QR Code tersebut untuk mendapatkan flag.

FLAG : `SCREEN6{enggang_gading_maskot_kalbar}`



SCREEN 6

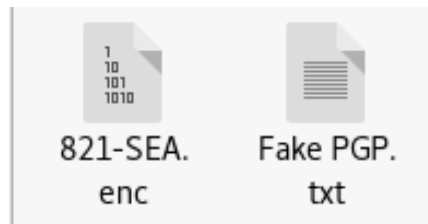
[SOAL 3][*Fake Fake*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah rar dan di dalamnya terdapat 2 buah file yang bernama Fake PGP.txt dan 821-SEA.enc



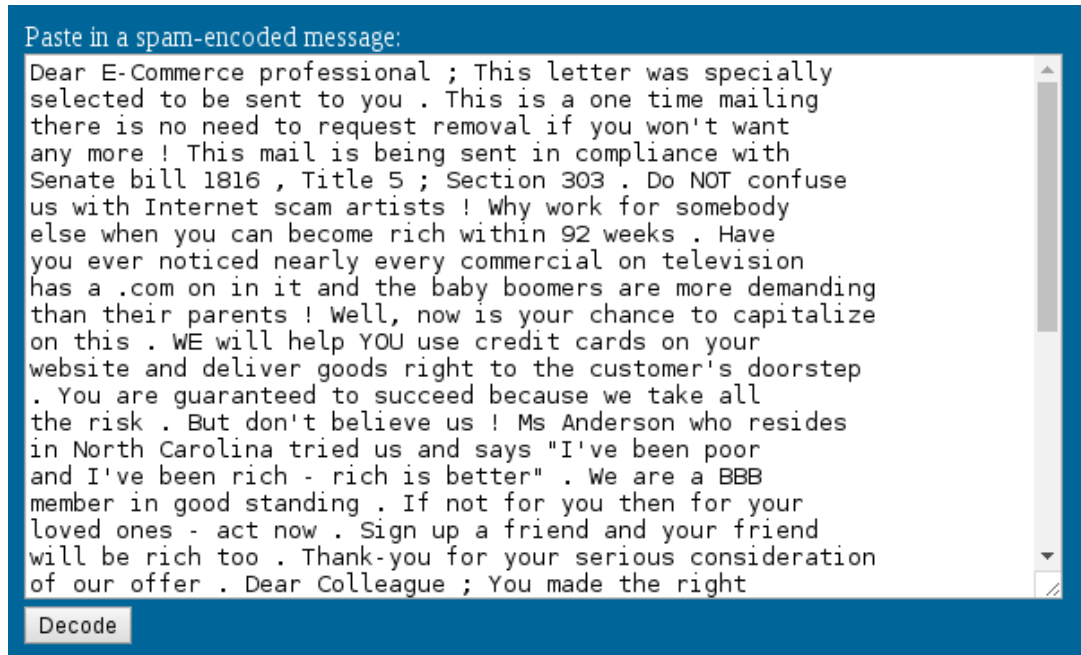
2. Technical Report

Ketika file Fake PGP.txt dibuka isinya seperti ini

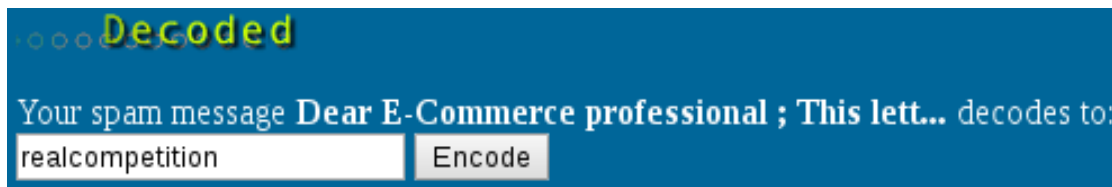
```
Dear E-Commerce professional ; This letter was specially  
selected to be sent to you . This is a one time mailing  
there is no need to request removal if you won't want  
any more ! This mail is being sent in compliance with  
Senate bill 1816 , Title 5 ; Section 303 . Do NOT confuse  
us with Internet scam artists ! Why work for somebody
```

Berdasarkan clue yang diberikan pada nama soal, kami mencari keyword di google yaitu Fake PGP Decode. Kami menemukan web untuk melakukan Fake PGP Decode di <http://www.spammimic.com> tapi pada saat melakukan PGP Decode tidak berhasil.

Lalu kami mencoba Spam Decode <http://www.spammimic.com>



Setelah disubmit hasil decodenya adalah **realcompetition**



Menurut dugaan kami, hasil decode diatas merupakan key untuk membuka enkripsi pada file 821-SEA.enc. Dan dari nama file 821-SEA.enc jika dibalik menjadi AES-128 berarti enkripsi yang digunakan pada file itu adalah AES-128 bit dengan key **realcompetition**.

Untuk mendecrypt pesan pada file 821-SEA.enc kami menggunakan perintah ini pada terminal

cat 821-SEA.enc | base64 | openssl enc -d -a -aes-128-cbc -p

Pada saat diminta password masukan passwordnya **realcompetiton**. Setelah itu akan menghasilkan seperti ini.

```
root@akhi:~/screen/fake# cat 821-SEA.enc | base64 | openssl enc -d -a -aes-128-cbc -p
enter aes-128-cbc decryption password:
salt=88A1478485542228
key=54203B0DDAEE377D9C65553630B54149
iv =53EC172A4C3B4AC48FECC265CD1D3CEA
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.2.5 (MingW32)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozdev.org

U0NSRUVONnt0aDFzX2lzX24wdF9mNGszX2ZsNGd9
-----END PGP MESSAGE-----
```

Dan kita mendapatkan hasil decryptnya setelah itu kami melakukan base64-decode pada string

U0NSRUVONnt0aDFzX2lzX24wdF9mNGszX2ZsNGd9

Hasilnya didapatkanlah flag yang kita cari

```
root@akhi:~/screen/fake# echo "U0NSRUVONnt0aDFzX2lzX24wdF9mNGszX2ZsNGd9" | base64 -d
SCREEN6{th1s_is_n0t_f4k3_fl4g}root@akhi:~/screen/fake#
```

3. Conclusion

Untuk menyelesaikan soal tersebut langkah pertamanya adalah mencari tahu key AES-128 pada file 821-SEA.enc. Untuk mencari key, lakukan spam decode. Spam encodednya berada di file Fake PGP.txt. Setelah mendapatkan key, decrypt file 821-SEA.enc menggunakan openssl pada terminal lalu hasil decrypt AES-128 di decode base64 untuk mendapatkan flag.

FLAG : **SCREEN6{th1s_is_n0t_f4k3_fl4g}**



[SOAL 4][*Nihil dan Unus*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan file nihil_unus.txt yang berisi banyak kata NIHIL! UNUS!

```
NIHIL! UNUS! NIHIL! UNUS! NIHIL!! UNUS!! NIHIL! UNUS! NIHIL!!!! UNUS!!! NIHIL! UNUS! NIHIL! UNUS! NIHIL!! UNUS! NIHIL!! UNUS! NIHIL!!! UNUS!  
NIHIL! UNUS! NIHIL! UNUS! NIHIL!!! UNUS! NIHIL! UNUS! NIHIL!! UNUS!!! NIHIL!!! UNUS!! NIHIL! UNUS!! NIHIL!! UNUS!!! NIHIL!  
UNUS!! NIHIL! UNUS!!! NIHIL! UNUS! NIHIL!!!! UNUS!! NIHIL! UNUS! NIHIL!! UNUS! NIHIL! UNUS! NIHIL! UNUS! NIHIL! UNUS!!!!  
NIHIL! UNUS!!! NIHIL!!!! UNUS!! NIHIL! UNUS!!!! NIHIL! UNUS!!! NIHIL! UNUS!!! NIHIL! UNUS!! NIHIL!! UNUS! NIHIL! UNUS! NIHIL! UNUS!!!!  
NIHIL!! UNUS! NIHIL!! UNUS! NIHIL! UNUS!!!! NIHIL! UNUS!! NIHIL! UNUS!!! NIHIL! UNUS!! NIHIL!! UNUS!! NIHIL!! UNUS! NIHIL! UNUS!!!!  
NIHIL! UNUS!! NIHIL! UNUS! NIHIL! UNUS!! NIHIL! UNUS!! NIHIL! UNUS! NIHIL! UNUS!! NIHIL!!!! UNUS!! NIHIL!! UNUS! NIHIL!  
UNUS! NIHIL! UNUS!!! NIHIL!!!! UNUS!! NIHIL!! UNUS! NIHIL! UNUS! NIHIL! UNUS!!! NIHIL! UNUS! NIHIL!!!! UNUS!!!! NIHIL! UNUS!
```

2. Technical Report

Menurut firasat kami, ini merupakan substitusi

NIHIL! = 0

UNUS! = 1

Bagaimana jika tanda serunya lebih dari satu seperti UNUS!! maka hasil substitusinya adalah 11. Substitusikan kata-kata tersebut sehingga didapatkan hasil seperti ini

010100110100001101010010010001010100010101001110001101100
111101101110100011010000110010101011111011100000110111101
110111011001010111001001011111011011110110011001011111011
010110110010101110000011001010111000001100101011101000111
1101

Setelah didapatkan hasil seperti diatas, konversikan bilangan biner tersebut ke string. Bisa menggunakan <http://string-functions.com/binary-string.aspx>. Hasilnya adalah

Binary to string converter

Enter the binary text to decode, and then click "Convert!":

```
0101001101000011010100100100010101000101010011100011011001111011  
0111010001101000011001010101111101110000011011110111011100101  
0111001001011111011011110110011001011111011010110110010101110000  
0110010101110000011001010111010001111101
```

Convert!

The decoded string:

```
SCREEN6{the_power_of_kepepet}
```

3. Conclusion

Substitusikan kata NIHIL! Menjadi 0 dan UNUS! Menjadi 1. Jika tanda seru lebih dari 1 maka sesuaikan berdasarkan jumlah tanda seru. Setelah nilai biner didapatkan, convert nilai biner tersebut ke string untuk mendapatkan flag

FLAG : **SCREEN6{the_power_of_kepepet}**



[SOAL 5][Find My TXT]

Table of Contents

Capture The Flag Report

1. Executive Summary

Deskripsi Soal :

Perkenalkan nama saya Bujang, CTF Lord event kali ini. Sebagai perkenalan, saya memberikan sebuah flag pada suatu TXT pada DNS domain ini.

Selamat mencari ^_^

2. Technical Report

Dari soal diatas dikatakan bahwa flag tersimpan pada TXT pada DNS domain scoreboard. Maka untuk mendapatkan TXT pada DNS domain dapat menggunakan perintah

dig TXT ctf.screen6.id

Setelah perintah tersebut dijalankan, maka tampilan terminal akan seperti ini

```
root@akhi:~# dig TXT ctf.screen6.id

; <<>> DiG 9.10.3-P4-Debian <<>> TXT ctf.screen6.id
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25515
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;ctf.screen6.id.                IN      TXT

;; ANSWER SECTION:
ctf.screen6.id.                14400   IN      TXT      "SCREEN6{pontianak_bukan_kuntila
nak}"

;; AUTHORITY SECTION:
screen6.id.                    14400   IN      NS       ns1.eazysmart.co.id.
screen6.id.                    14400   IN      NS       ns2.eazysmart.co.id.

;; Query time: 16 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Mar 21 14:34:51 WIB 2017
;; MSG SIZE  rcvd: 129
```

3. Conclusion

Gunakan perintah dig ctf.screen6.id pada terminal linux untuk mendapatkan flag.

FLAG : **SCREEN6{pontianak_bukan_kuntilanak}**