

Write-up
Asgama-CTF



Sumat3ra
Gayu Gumelar

Forensic

Weird Channel (30)

Diberikan sebuah file image, ketika kita zoom image tersebut maka muncul sebuah flag. Namun flag tersebut masih samar-samar dan tidak jelas. Kemudian saya coba buka di Photoshop dan saya atur kecerahan dan muncul flag.



Flag : `CTF{w3lc0m3_to_w4t3rmark1ng_st3g4n0}`

Kriptografi

base64 (5)

QVNHYW1he2phbGFuX2hla2Vsa3VfbXVsYWlfZGFyaV9iZWxhamFyX2VuY29kaW5nfQ==

Diberikan soal base64 yang sudah di enkripsi, menurut saya nama soal tersebut adalah clue jadi saya langsung decode ke base64 dengan python

```
File Edit View Search Terminal Help
root@Hexa:~# python
Python 2.7.3 (default, Mar 14 2014, 11:57:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> "QVNHYW1he2phbGFuX2hla2Vsa3VfbXVsYWlfZGFyaV9iZWxhamFyX2VuY29kaW5nfQ==".decode('base64')
'ASGama{jalan_hekelku_mulai_dari_belajar_encoding}'
>>> |
```

Flag : ASGama{jalan_hekelku_mulai_dari_belajar_encoding}

Caesar (10)

BvhvXOA{xvzzn5vm_nj_zut}

Diberikan soal dengan nama caesar, untuk menyelesaikan soal tersebut saya masuk ke <http://rumkin.com/tools/cipher/caesar.php> dan ternyata itu merupakan rot5

ASGama CTF x Caesarian Shift x

rumkin.com/tools/cipher/caesar.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Caesarian Shift

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

This is a standard Caesarian Shift cipher encoder, also known as a rot-N encoder and is also a style of substituting 25 to your string and see how it changes. This is an offshoot of the [rot13](#) encoder on this web site. To perform the paper. Line them up so the top strip's A matches the bottom strip's D (or something) and then you can encode. , [alphabet](#) into the encoder and then change the values of N.

This sort of cipher can also be known as a wheel cipher. This is where an inner wheel has the alphabet around it and the alphabet going around it. You can rotate the wheels so that ABC lines up with ABC, or ABC may line up with QRS.

To encode something, just pick an N and type in your message. To decode something, subtract the encryption N.

N: 5

BvhvXOA{xvzzn5vm_nj_zut}

This is your encoded or decoded text:

GamaCTF{caees5ar_so_ezy}

Flag : GamaCTF{caees5ar_so_ezy}

Hash (10)

742929dcb631403d7c1c1efad2ca2700

karena perintah nya hash maka saya masuk ke terminal kemudian mengetikan hash-identifikasi

```
File Edit View Search Terminal Help  
root@Hexa:~# hash-identifier  
#####  
#                                     #  
#           \ / \ / \ / \ / \ / \   \ / \ / \ / \ / \   v1.1 #  
#          / \ / \ / \ / \ / \ / \   / \ / \ / \ / \   By Zion3R #  
#         _/_/_/_/_/_/_/_/_/_/_/__/_/_/_/_/_/_/_/_/_/_/_ #  
#        www.Blackexploit.com #  
#      Root@Blackexploit.com #  
#####  
-----  
HASH: 742929dcb631403d7c1c1efad2ca2700
```

Possible Hashs:

- [+] MD5
- [+] Domain Cached Credentials - MD4(MD4((\$pass)).(strtolower(\$username)))

dan itu merupakan hasil dari hash MD5, kemudian saya ketikkan lagi
findmyhash MD5 -h 742929dcb631403d7c1c1efad2ca2700

```
File Edit View Search Terminal Help
root@Hexa:~# findmyhash MD5 -h 742929dcb631403d7c1c1efad2ca2700
Cracking hash: 742929dcb631403d7c1c1efad2ca2700
Analyzing with my-addr (http://md5.my-addr.com)...
***** HASH CRACKED!! *****
The original string is: chicken

The following hashes were cracked:
-----

742929dcb631403d7c1c1efad2ca2700 -> chicken
```

Flag : GamaCTF{chicken}

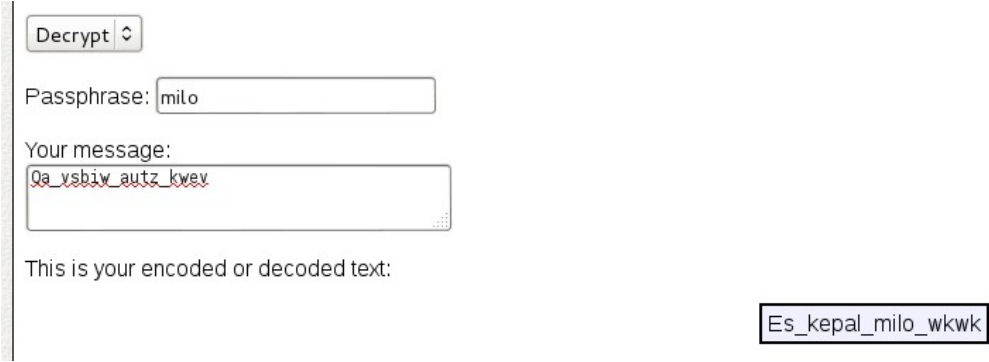
Vinnegar (35)

Diberikan soal dengan

key: milo

Cipher : Qa_vsbiw_autz_kwev

kemudian saya masuk ke <http://rumkin.com/tools/cipher/vigenere.php> dan saya masukan key, cipher tadi, kemudian saya decode.



Decrypt ↕

Passphrase:

Your message:

This is your encoded or decoded text:

Flag : GamaCTF{Es_kepal_milo_wkww}

1byte ROXy ? (45)

Diberikan soal

e7c1cdc1e3f4e6dbcfcec5ffc2d9d4c5ffd8cfd2d29f9fdd

kemudian saya buat script python seperti di bawah ini

```
1byteROXy.py x
import sys
import base64
a="e7c1cdc1e3f4e6dbcfcec5ffc2d9d4c5ffd8cfd2d29f9fdd"
b1=a.decode("hex")
for a in range(1, 256):
    for b in b1:
        c = ord(b)
        d = c^a
        sys.stdout.write(chr(d))
    print " Kunci"+str(a)+"\n"
```

flag berada pada line 160

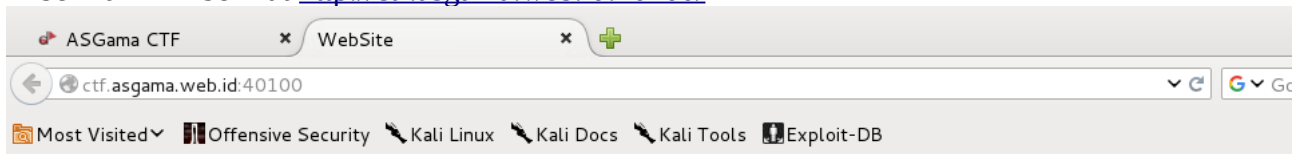
```
File Edit View Search Terminal Help
y_S_}jxEQP[a\GJ[aFQLL[0000] Kunci158
x^R^|kyDPQZ`]FKZ`GPM MB Kunci159
GamaCTF{one_byte_xorr??} Kunci160
F`l`BUGznod^cxud^ynss>>| Kunci161
EcocAVDymlg]`{vg]zmp==[00]Kunci162
```

Flag : GamaCTF{one_byte_xorr??}

Web

Sauce (5)

Diberikan link berikut <http://ctf.asgama.web.id:40100/>



WebSite

[Home](#) [About](#) [Contact](#)

-->

Tidak ada apa-apa disini.

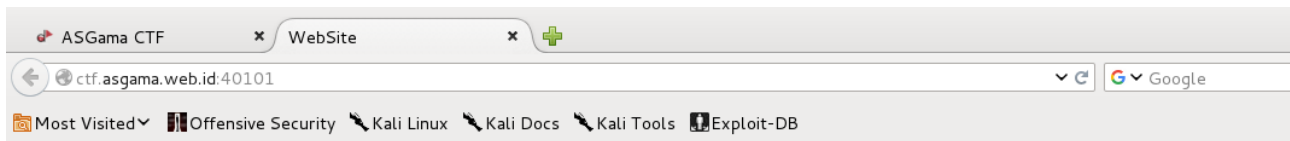
kemudian saya cek inspect element

```
Source of: http://ctf.asgama.web.id:40100/ - Iceweasel
File Edit View Help
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <meta http-equiv="X-UA-Compatible" content="ie=edge">
7   <title>WebSite</title>
8 </head>
9 <body>
10   <center>
11     <h1>WebSite</h1>
12     <hr>
13     <a href="#">Home</a> <a href="#">About</a> <a href="#">Contact</a><br><br>
14 |
15
16     --><p>Tidak ada apa-apa disini.</p>
17     <!-- FLAG: GamaCTF{S0urc3_c0d3} -->
18   </center>
19 </body>
20 </html>
21
```

Flag : **GamaCTF{S0urc3_c0d3}**

Secret Dir (10)

Diberikan link berikut <http://ctf.asgama.web.id:40101> dengan Hint : Flag ada di sebuah directory



WebSite

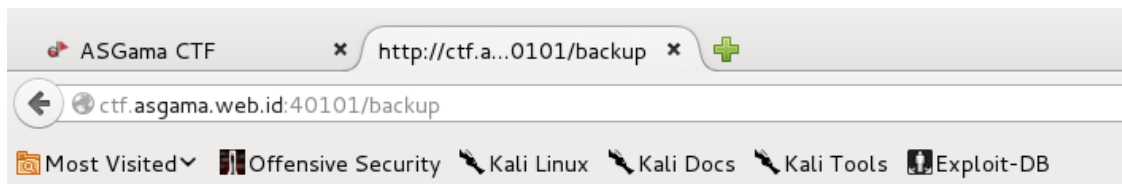
UNDER MAINTENANCE

Maaf kk webnya sedang maintenance

Jangan sedih, untungnya semua data sudah kami backup di directory tertentu

kemudian saya inspect element lagi, dan benar muncul clue /backup

```
Source of: http://ctf.asgama.web.id:40101/ - Iceweasel
File Edit View Help
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <meta http-equiv="X-UA-Compatible" content="ie=edge">
7   <title>WebSite</title>
8 </head>
9 <body>
10   <center>
11     <h1>WebSite</h1>
12     <hr>
13     <h3>UNDER MAINTENANCE</h3>
14     <p>Maaf kk webnya sedang maintenance</p>
15     <p>Jangan sedih, untungnya semua data sudah kami backup di directory tertentu</p>
16   </center>
17 </body>
18 </html>
19 <!-- Backup: /backup -->
20
```

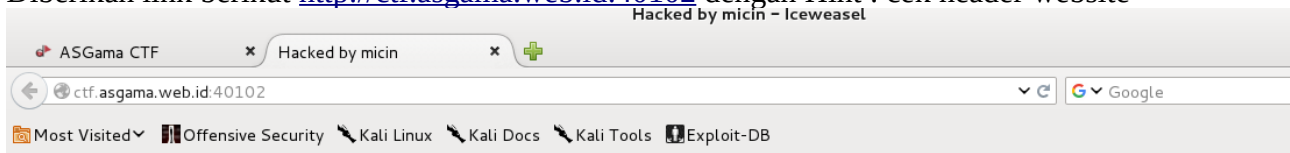


GamaCTF{b4ckUP}

Flag : **GamaCTF{b4ckUP}**

Ndasmu (15)

Diberikan link berikut <http://ctf.asgama.web.id:40102> dengan Hint : cek header website



HACKED BY C4h_M1c1N

Webnya ane hack ea, klo mau balik cari aja sendiri flagnya

Karena ane hekel baik, coba aja pke curl

kemudian saya masuk terminal dan mengetikan curl -i http://ctf.asgama.web.id:40102

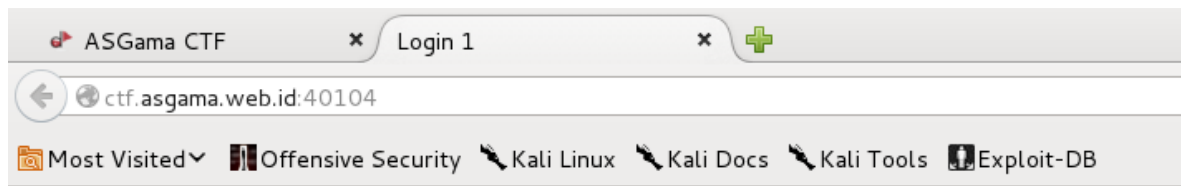
```
File Edit View Search Terminal Help
root@Hexa:~# curl -i http://ctf.asgama.web.id:40102
HTTP/1.1 200 OK
Host: ctf.asgama.web.id:40102
Date: Sun, 25 Nov 2018 01:13:19 +0000
Connection: close
X-Powered-By: PHP/7.2.6
BENDERA: GamaCTF{check_your_head}
Content-type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <title>Hacked by micin</title>
</head>
<body>
  <center>
    <marquee><h1>HACKED BY C4h_M1c1N</h1></marquee>
    <hr>
    <p>Webnya ane hack ea, klo mau balik cari aja sendiri flagnya</p>
    <p>Karena ane hekel baik, coba aja pke curl</p>
  </center>
</body>
</html>
```

Flag : **GamaCTF{check_your_head}**

Login 1 (25)

Diberikan link berikut <http://ctf.asgama.web.id:40104/> dengan Hint : strcmp vulnerability

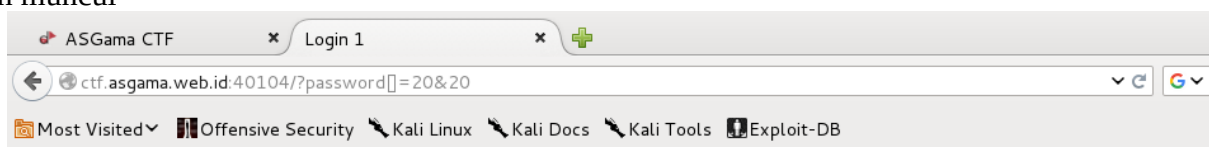


Login 1

Password:

Login

kemudian saya ketikkan [http://ctf.asgama.web.id:40104/?password\[\]=20&20](http://ctf.asgama.web.id:40104/?password[]=20&20) dan muncul



Login 1

Password:

Login

Warning: strcmp() expects parameter 1 to be string, array given in /home/web/index.php on line 19
GamaCTF{aw4s_strcmp}

Flag : **GamaCTF{aw4s_strcmp}**