

# WRITEUPS OLIMPIADE HACKING

Ardhi Putra Pradana - SMK N 7 Semarang



vinzel Today at 11:42 AM

turu turu



.melodicsoul Today at 11:42 AM

angel ws

WEEK 1

# Daftar Isi

---

<b>Daftar Isi</b> .....	<b>2</b>
<b>Cryptography</b> .....	<b>4</b>
Vlodkndq whnv vrdo gdsdw glwxolv gl ohpedu lql.....	4
Flag: flag{cangkul}.....	5
EASY-PEASY.....	6
Flag: flag{md5_sudah_tidak_direK0mendaskan}.....	7
No comment.....	8
Flag: flag{Shh_Its_S3cret!!}.....	9
<b>Database Attack</b> .....	<b>10</b>
Login Web.....	10
Flag: flag{sql_injection}.....	11
DVWA.....	12
Flag: flag{2}.....	12
DVWA DVWA.....	13
Flag: flag{5.7.25-28}.....	13
<b>BONUS</b> .....	<b>14</b>
EASY.....	14
Flag: flag{BENAR}.....	14
undangan_pernikahan.apk.....	15
Flag: flag{4444}.....	15
cookie[s].....	16
Flag: flag{disini_letak_nilai_cookie}.....	16
<b>Bruteforce</b> .....	<b>17</b>
Ini Aplikasi Apa?.....	17
Flag: {TIDAK}.....	18
<b>Digital Signature</b> .....	<b>19</b>
GnuPG.....	19
Flag: flag{dekripsi-gnupg-ctf@itts.ac.id}.....	19
Surat dari Pak Lurah.....	20
Flag: flag{31}.....	20
PROKLAMASI'45.....	21
Flag: flag{GOOD}.....	21
<b>Credential Leak</b> .....	<b>22</b>
Rahasia Dian.....	22
Pablo Picasso.....	23
Flag: flag{letmein}.....	23
<b>Data Leak</b> .....	<b>24</b>
MyWEB.....	24
k0De-SuM13eR.....	25
<b>Reconnaissance</b> .....	<b>26</b>

Scan Me!.....	26
Flag: flag{8010}.....	26
NM4P.....	27
Flag: flag{21 22 23 25 53 80 110 143 993 995 3306}.....	27
<b>Steganography.....</b>	<b>28</b>
Ctrl + A.....	28
Flag: flag{SmkBisaHebatSiapKerjaSantunMandiriKreatif}.....	28

# Cryptography

---

Vlodkndq whnv vrdo gdsdw glwxolv gl ohpedu lql



Diberikan sebuah soal dengan deskripsi dan juga attachment file nya dalam bentuk zip yang dipassword. Di dalam soal sudah dijelaskan bahwa passwordnya **nqzvavfgengbe**, namun harus didecode terlebih dahulu. Ketika melihat password yang terenkripsi tersebut langsung terpikirkan menggunakan algoritma *ROT13*, kemudian saya langsung melakukan decode password yang terenkripsi tersebut

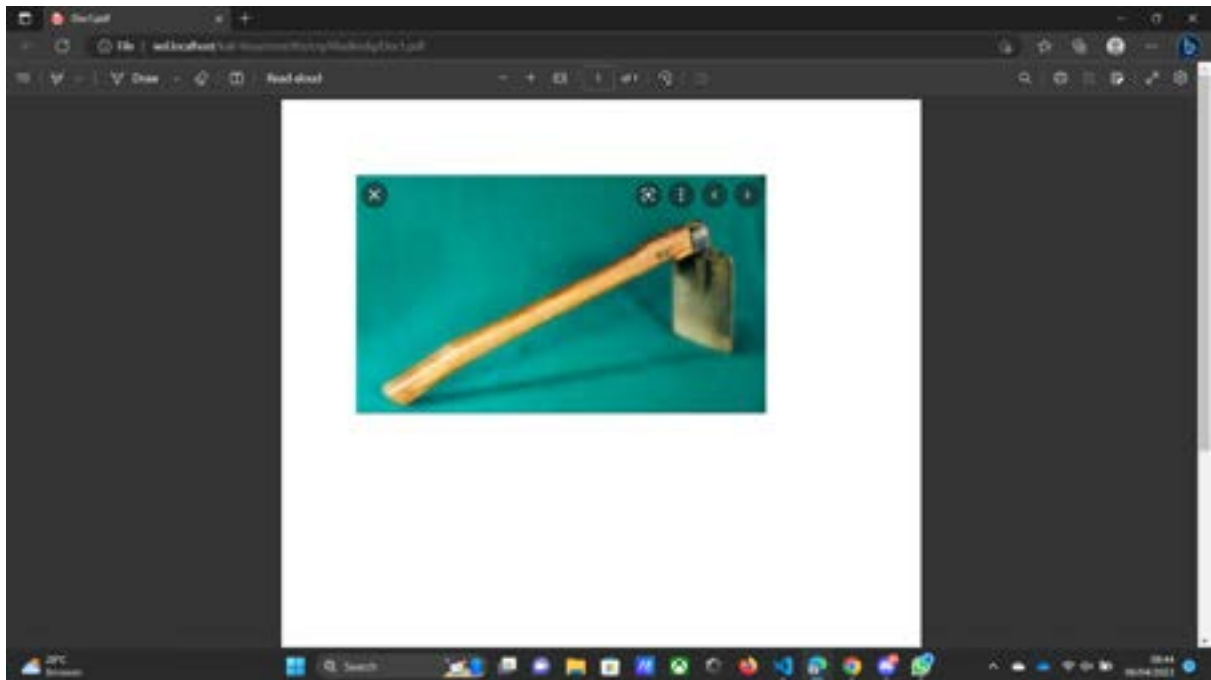
```
(root@sijastemba2202) - [~]  
# echo nqzvavfgengbe | tr 'A-Za-z' 'N-ZA-Mn-za-m'  
administrator
```

Dan benar ternyata passwordnya adalah **administrator**, kemudian saya melakukan ekstrak file zip tersebut

```
(root@sijastemba2202) - [~/itts/cry/Vlodkndq]
# unzip doc1.zip
Archive:  doc1.zip
[doc1.zip] Doc1.pdf password:
inflating: Doc1.pdf

(root@sijastemba2202) - [~/itts/cry/Vlodkndq]
# ls
Doc1.pdf  doc1.zip
```

Setelah diekstrak ada file pdf, kemudian saya buka file tersebut, dan hasilnya adalah gambar cangkul, dan sesuai dengan deskripsi soal kita disuruh untuk menebak gambarnya



Jadi, setelah itu saya wrap nama gambar nya dengan format flag yang valid

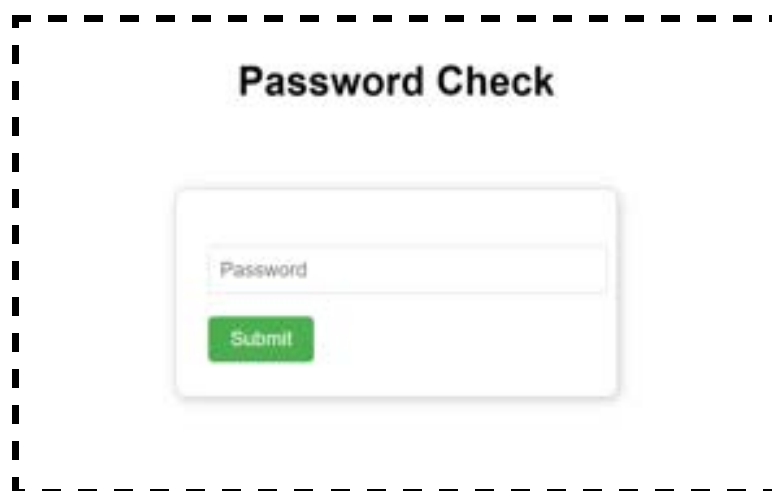
**Flag: flag{cangkul}**

## EASY-PEASY



The screenshot shows a challenge window with a title bar containing 'Challenge' and '33 Solves'. The main title is 'EASY-PEASY 100'. Below the title, the instruction reads: 'Temukan flag dalam halaman web yang diberi password di bawah ini'. A URL is provided: 'http://180.214.246.108:8084/access'. At the bottom, there is a text input field labeled 'Flag' and a 'Submit' button.

Diberikan sebuah soal dan deskripsinya, dan kita diharuskan menemukan sebuah flag dari web service yang dicantumkan tersebut. Ketika dibuka akan menampilkan tampilan seperti dibawah, dan kita harus memasukkan password untuk mendapatkan flagnya.



The screenshot shows a 'Password Check' form. It features a text input field labeled 'Password' and a green 'Submit' button.

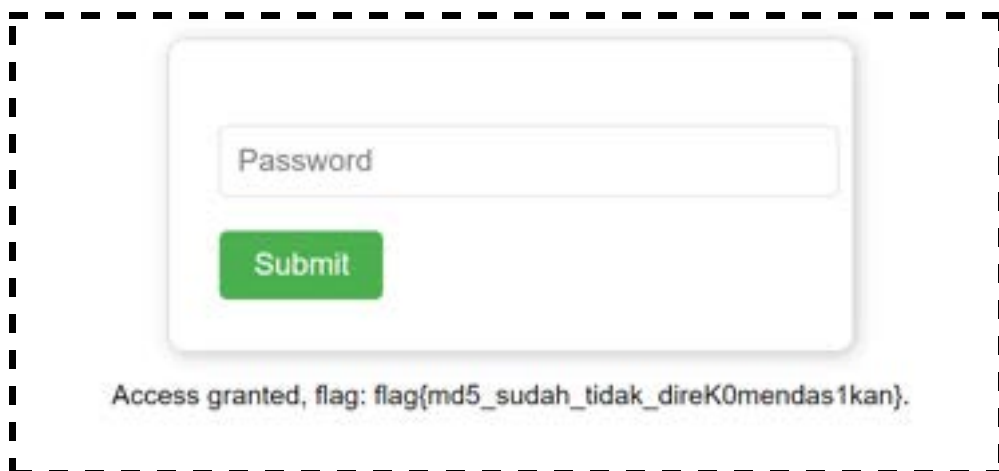
Saya langsung mengecek bagian page source dari web ini, dan hasilnya saya menemukan sebuah text yang mencurigakan, saya rasa ini adalah password yang terenkripsi

```
47 <body>
48   <h1>Password Check</h1>
49   <form method="post">
50     <input type="password" name="password" placeholder="Password">
51     <input type="submit" value="Submit">
52   </form>
53   <!--0192023a7bbd73250516f069df18b500--></body>
54 </html>
```

Dan jika dilihat dari text tersebut, saya langsung berasumsi bahwa text tersebut adalah hash dari MD5, lalu saya mencoba untuk melakukan decode hash tersebut melalui layanan compare hash MD5 online

```
Found : admin123
(hash = 0192023a7bbd73250516f069df18b500)
```

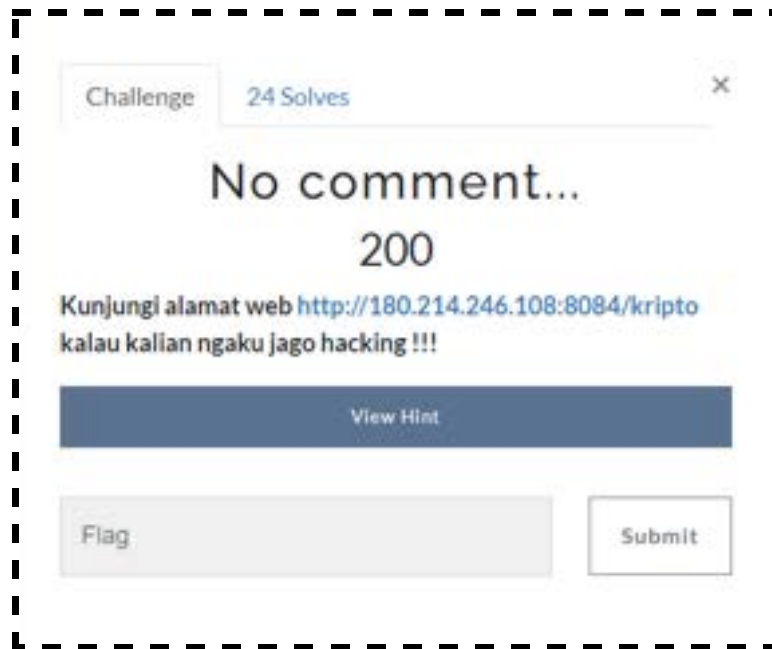
Dan benar saja saya mendapatkan hasil dari hash MD5 tersebut, kemudian saya langsung masukkan password **admin123** kedalam web nya, dan berhasil mendapatkan flagnya



Access granted, flag: flag{md5\_sudah\_tidak\_direkomendasikan}.

Flag: flag{md5\_sudah\_tidak\_direkomendasikan}

No comment...



Challenge 24 Solves

No comment...

200

Kunjungi alamat web <http://180.214.246.108:8084/kripto>  
kalau kalian ngaku jago hacking !!!

View Hint

Flag Submit

Diberikan soal dan deskripsi, terdapat sebuah web service yang bisa diakses, ketika di cek hasilnya sebagai berikut



Bahasa buatan dalam *Fantasi Terakhir X*

Vmykhoy ytymyr : vmyk{Crr\_Edc\_C3lnad!!}

Flag:  Check

Dan ternyata terdapat sebuah flag, namun flag tersebut masih terenkripsi, namun disitu terdapat tulisan **“Bahasa buatan dalam *Fantasi Terakhir X*”** sepertinya ini adalah hint bahwa enkripsi tersebut menggunakan bahasa buatan dari *Final Fantasy X*, kemudian saya mencari bahasa tersebut dan mendapatkan hasilnya di wikipedia





Ternyata bahasa yang digunakan adalah **Bahasa Al Bhed**, dan cara kerja dari bahasa tersebut menggunakan salah satu teknik enkripsi yaitu **substitution cipher**, yaitu dengan menggunakan schema seperti ini

Bahasa Inggris	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Al Bhed	Y	P	L	T	A	V	K	R	E	Z	G	M	S	H	U	B	X	N	C	D	I	J	F	Q	O	W

Kemudian saya mencoba melakukan decrypt dengan schema tersebut menggunakan teknik **substitution cipher**, dan berikut adalah hasilnya



Dan terlihat langsung flagnya dari hasil **substitution cipher** dengan menggunakan schema dari **Bahasa Al Bhed**

**Flag: flag{Shh\_Its\_S3cret!!}**

# Database Attack

---

## Login Web



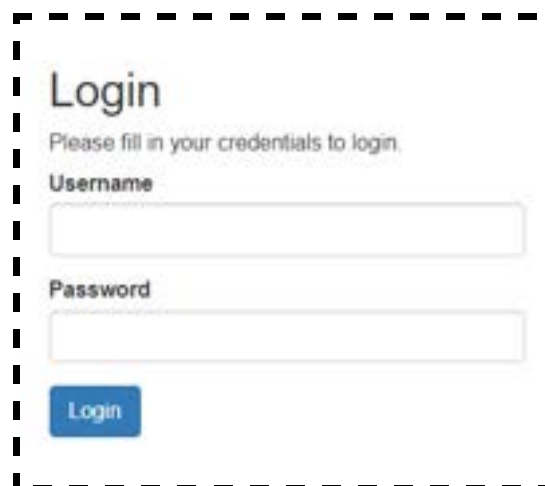
Challenge 26 Solves

### Login Web 100

Salah satu website yang beralamat di <http://180.214.246.108:9081/login-web/login.php> mempunyai form login username dan password. Temukan flag yang tersimpan di website tersebut

Flag

Diberikan sebuah soal dan deskripsinya, sesuai deskripsi ketika web tersebut dibuka langsung diberikan form login dengan field username dan juga password



### Login

Please fill in your credentials to login.

Username

Password

Kemudian saya langsung mencoba melakukan SQL Injection dengan payload yang simple, berikut payload yang saya gunakan untuk melakukan SQL Injection

username: ' OR '1'='1' #  
password: 123 \*nilai sembarang

Setelah menekan tombol login saya berhasil masuk dan mendapatkan flagnya



Flag: flag{sql\_injection}

## DVWA



Diberikan sebuah soal dan deskripsinya beserta dengan file hasil dari sqlmap. Kita diharuskan untuk menganalisa hasil dari sqlmap tersebut dan menghitung total tabel yang ada. Setelah dilakukan analisa ada bagian yang memberikan informasi mengenai total tabel yang ada dalam database

```
sqlmap -u 'http://192.168.0.80/DVWA-1.0.0/vulnerabilities/sqli/?id=1&Submit=Submit#'
--cookie="security=low; PHPSESSID=0dim4l9ngdppog70gdihpc141" -O dvwa --tables

[07:08:39] [INFO] fetching tables for database: 'dvwa'
[07:08:39] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
```

Sesuai dengan informasi tersebut, berarti ada 2 tabel dalam databasenya, kemudian langsung diwrap menggunakan format flag yang valid

**Flag: flag{2}**

## DVWA DVWA

Challenge

36 Solves

×

DVWA DVWA

100

SQL Injection di DVWA dilakukan dengan perintah,

`%' or 0=0 union select null, version() #`

Hasilnya adalah sebagai berikut,

ID: `%' or 0=0 union select null, version() #` First name: admin  
Surname: admin

ID: `%' or 0=0 union select null, version() #` First name: Gordon  
Surname: Brown

ID: `%' or 0=0 union select null, version() #` First name: Hack  
Surname: Me

ID: `%' or 0=0 union select null, version() #` First name: Pablo  
Surname: Picasso

ID: `%' or 0=0 union select null, version() #` First name: Bob  
Surname: Smith

ID: `%' or 0=0 union select null, version() #` First name:  
Surname: 5.7.25-28

Tulis nomor versi database yang digunakan?

Flag

Submit

Diberikan sebuah soal dan deskripsinya, di dalam deskripsi terdapat hasil dari SQL Injection, dan diharuskan untuk menjawab nomor versi dari database yang digunakan, dengan hanya membaca beberapa payload SQL Injection pada bagian `ID: %' or 0=0 union select null, version()` hasilnya adalah versi dari database, berarti versi databasenya adalah **5.7.25-28**. Langkah selanjutnya wrap dengan format flag yang valid

**Flag: flag{5.7.25-28}**

## BONUS

---

### EASY

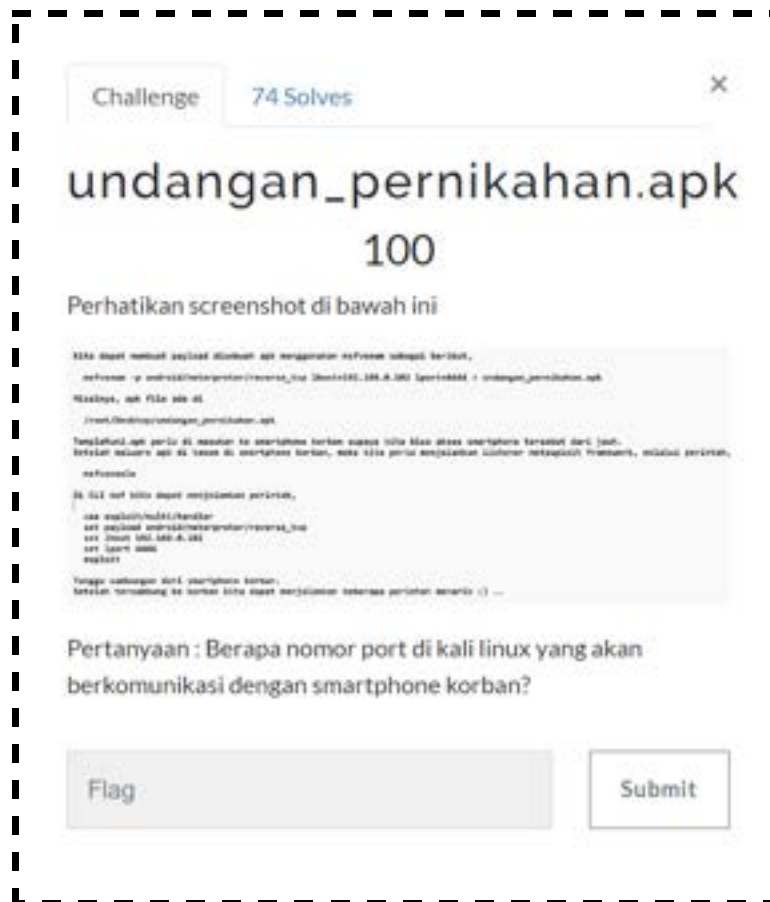


The screenshot shows a challenge interface with a dashed border. At the top left, there is a 'Challenge' tab and a '54 Solves' count. The title 'EASY' is prominently displayed above the number '100'. The main text describes ransomware as a type of destructive device designed to block access to computer systems or data until a ransom is paid, often by encrypting the user's data and promising its return upon payment. Below this text, a question asks whether the statement is 'BENAR' (True) or 'SALAH' (False). At the bottom, there is a 'Flag' input field and a 'Submit' button.

Diberikan sebuah soal dan deskripsi yang berupa pernyataan mengenai **ransomware**, dimana disini harus menentukan apakah pernyataan tersebut BENAR atau SALAH. Jika dilihat dari pernyataannya mengenai ransomware yaitu mengenai menghalangi akses sistem dan harus membayar untuk bisa mengembalikannya kembali maka pernyataan tersebut bernilai **BENAR**.

**Flag: flag{BENAR}**

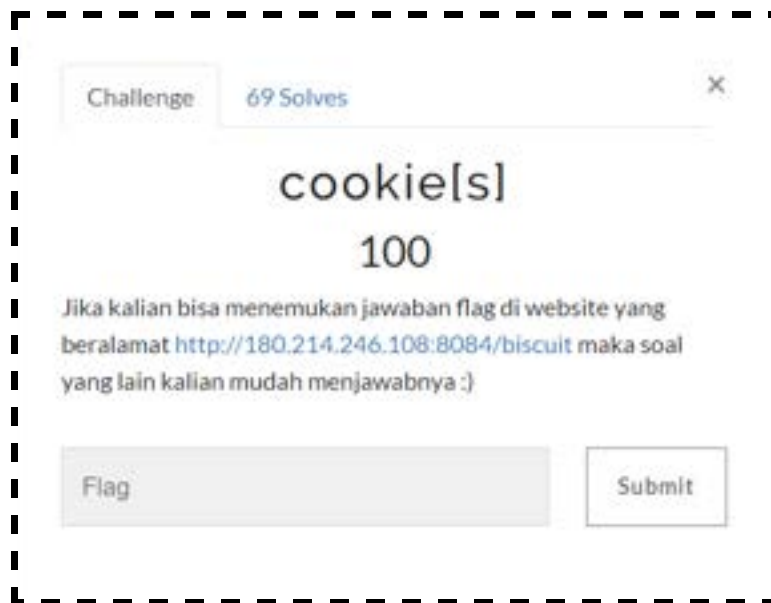
undangan\_pernikahan.apk



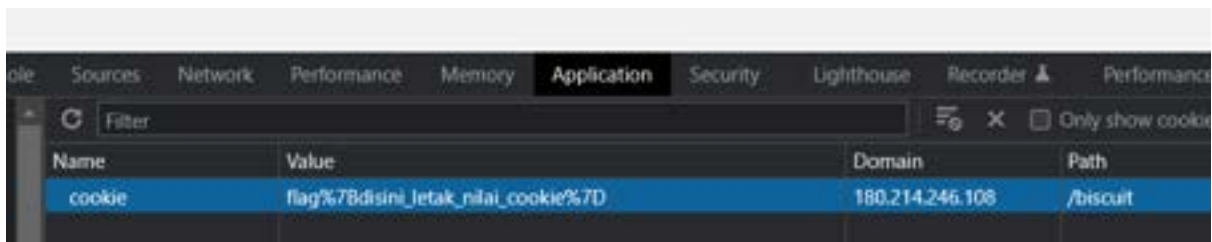
Diberikan sebuah soal dan deskripsinya, pada soal ini diharuskan untuk menentukan kira - kira port berapa yang akan digunakan untuk berkomunikasi dengan smartphone dari sebuah gambar yang juga disertakan pada soal ini. Jika dilihat di dalam gambarnya sudah tertera untuk **lport** diset nilainya ke **4444**, artinya ini adalah listening port yang digunakan.

Flag: flag{4444}

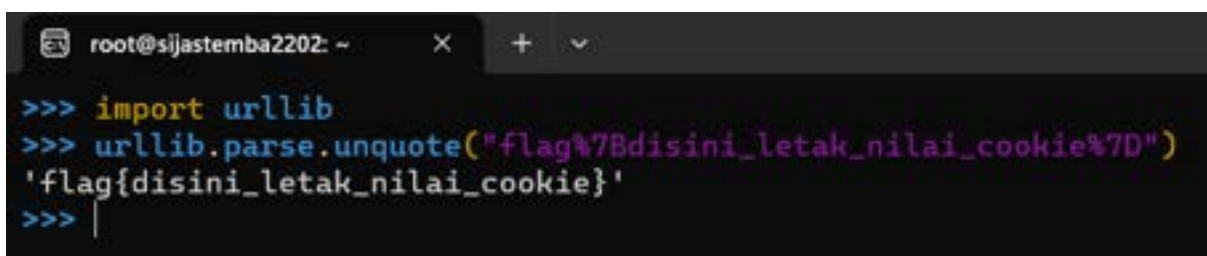
cookie[s]



Diberikan sebuah soal dan deskripsi, didalamnya terdapat sebuah web service yang bisa diakses. Ketika dibuka maka akan menampilkan sebuah web biasa dan sederhana, namun sesuai dengan judul dari soalnya, disini saya langsung untuk mengecek cookie storage yang ada di website tersebut



Dan pada cookie storage benar ada sebuah flag, namun flag tersebut masih dalam format url encoded, lalu kemudian saya lakukan url decode dari flag tersebut untuk mendapatkan flag aslinya



Flag: flag{disini\_letak\_nilai\_cookie}



# Bruteforce

---

Ini Aplikasi Apa?

Challenge

76 Solves

X

## Ini Aplikasi Apa ?

100

dirb <http://192.168.0.92>

\*----- Scanning URL: <http://192.168.0.92/> -----\*

- <http://192.168.0.92/index.html>  
(CODE:200|SIZE:10918)
- <http://192.168.0.92/server-status>  
(CODE:403|SIZE:300) ==> DIRECTORY:  
<http://192.168.0.92/squirrelmail/>

---- Entering directory: <http://192.168.0.92/squirrelmail/> ----

==> DIRECTORY: <http://192.168.0.92/squirrelmail/class/>

==> DIRECTORY: <http://192.168.0.92/squirrelmail/config/>

- <http://192.168.0.92/squirrelmail/configure>  
(CODE:200|SIZE:102)  
==> DIRECTORY:  
<http://192.168.0.92/squirrelmail/contrib/> ==>  
DIRECTORY: <http://192.168.0.92/squirrelmail/data/>  
==> DIRECTORY: <http://192.168.0.92/squirrelmail/doc/>  
==> DIRECTORY:  
<http://192.168.0.92/squirrelmail/functions/> ==>  
DIRECTORY: <http://192.168.0.92/squirrelmail/help/>  
==> DIRECTORY:  
<http://192.168.0.92/squirrelmail/images/> ==>  
DIRECTORY: <http://192.168.0.92/squirrelmail/include/>

Apakah aplikasi web tersebut biasanya digunakan untuk transfer file? Jawab menggunakan format flag[YA] atau flag[TIDAK]

Flag

Submit

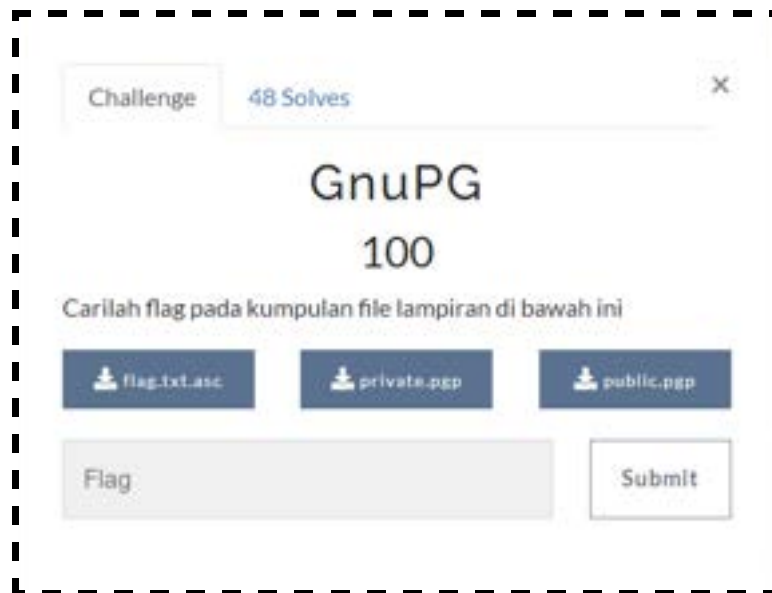
Diberikan sebuah soal dan deskripsinya, didalamnya terdapat hasil scanning url menggunakan **dirb**, lalu diharuskan untuk menjawab apakah aplikasi web tersebut digunakan untuk transfer file atau tidak. Jika dilihat dari hasil scanningnya tidak ada indikasi sama sekali bahwa website tersebut digunakan untuk transfer file, karena pada hasil scanning hanya ditemukan sebuah **web mail service**, dan juga beberapa hal lainnya seperti halaman **index** dan **server-status**

**Flag: {TIDAK}**

# Digital Signature

---

## GnuPG



Diberikan sebuah soal, diberikan juga 3 file yaitu **flag.txt.asc**, **private.pgp**, **public.pgp**. Jika dilihat dalam 3 file tersebut menggunakan sebuah teknik **PGP** (*Pretty Good Privacy*), karena kita diberikan file **private key** dan **public** nya kita bisa dengan mudah melakukan decrypt file **flag.txt.asc**. Sesuai judul soal kita bisa melakukannya dengan menggunakan **GnuPG** atau **GPG**

Pertama kita import dulu private key nya terlebih dulu, setelah berhasil meng import private key kita bisa langsung men decode file **flag.txt.asc**

```
(root@sijastemba2202) - [~/itts/digital-signature/GnuPG]
# gpg --import private.pgp
gpg: key A9D4AA7F82D7442B: public key "CTF Institut Teknologi Tangerang Selatan (CTF) <ctf@itts.ac.id>" imported
gpg: key A9D4AA7F82D7442B: secret key imported
gpg: Total number processed: 1
gpg:      imported: 1
gpg:      secret keys read: 1
gpg:      secret keys imported: 1

(root@sijastemba2202) - [~/itts/digital-signature/GnuPG]
# gpg --decrypt flag.txt.asc
gpg: encrypted with 3072-bit RSA key, ID EC189BC7E10206F3, created 2023-01-29
"CTF Institut Teknologi Tangerang Selatan (CTF) <ctf@itts.ac.id>"
flag{dekripsi-gnupg-ctf@itts.ac.id}
```

Flag: **flag{dekripsi-gnupg-ctf@itts.ac.id}**

## Surat dari Pak Lurah

Challenge 42 Solves

### Surat dari Pak Lurah

100

Silahkan di verify tanda tangan digital dokumen "Formulir\_surat\_keterangan.pdf" terlampir.

Pertanyaan : Pada tanggal berapa dokumen tersebut di tanda tangan ? (jawab dengan menuliskan tanggalnya saja berupa angka)

[doc.sig](#) [Formulir\\_sur...](#) [private.pgp](#)  
[public.pgp](#)

Flag  Submit

Diberikan soal dan beberapa filenya, yaitu **doc.sig**, **Formulir\_surat\_keterangan.pdf**, **private.pgp**, **public.pgp**. Lagi - lagi ini adalah mengenai teknik **PGP**. Tugas kita disini adalah untuk menentukan tanggal berapa **sign** nya dibuat

Karena **private key** dan **public key** nya sama dengan soal sebelumnya (**GnuPG**) kita tidak perlu meng import nya lagi, kita bisa langsung saja memverify file **doc.sig** nya

Dan bisa dilihat hasilnya setelah diverify file sign tersebut dibuat pada **Selasa, 31 Januari 2023**, berarti tanggal yang tepat adalah tanggal **31**, kemudian wrap dengan format flag yang valid

```
(root@sijastamba2202) ~/itts/digital-signature/surat-dari-pak-lurah
# gpg --verify doc.sig
gpg: Signature made Tue 31 Jan 2023 05:59:35 AM WIB
gpg: using RSA key 5E995372DC90BA726AD74210A9D4AA7F82D7442B
gpg: Good signature from "CTF Institut Teknologi Tangerang Selatan (CTF) <ctf@itts.ac.id>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 5E99 5372 DC90 BA72 6AD7 4210 A9D4 AA7F 82D7 442B
```

Flag: flag{31}

## PROKLAMASI '45

Challenge

69 Solves

X

PROKLAMASI '45

100

Periksa lampiran file berikut

[pidato-presiden-soekarno-17-agustus-1945.txt](#)[private-1.pgppublic-1.pgptandatangan.sig](#)

Pertanyaan : Periksa apakah tanda tangan digital yang digunakan adalah tanda tangan yang baik atau tidak baik.

Jawab dengan flag{GOOD} atau flag{BAD}

Flag

Submit

Diberikan sebuah soal dan beberapa file yaitu **pidato-presiden-soekarno-17-agustus-1945.txt**, **private-1.pgp**, **public-1.pgp**, dan **tandatangan.sig**. Pada soal ini kita hanya diperintahkan untuk memeriksa/verify apakah file sign tersebut valid atau tidak.

Karena **public key** dan **private key** nya masih sama kita tidak perlu mengimport nya lagi, langsung saja kita verify

```
(root@sijasterba2202) ~/itts/digital-signature/proklamasi
$ gpg --verify tandatangan.sig pidato-presiden-soekarno-17-agustus-1945.txt
gpg: Signature made Tue 31 Jan 2023 02:36:30 PM WIB
gpg: using RSA key 5E995372DC90BA726AD74210A9D4AA7F82D7442B
gpg: Good signature from "CTF Institut Teknologi Tangerang Selatan (CTF) <ctf@itts.ac.id>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 5E99 5372 DC90 BA72 6AD7 4210 A9D4 AA7F 82D7 442B
```

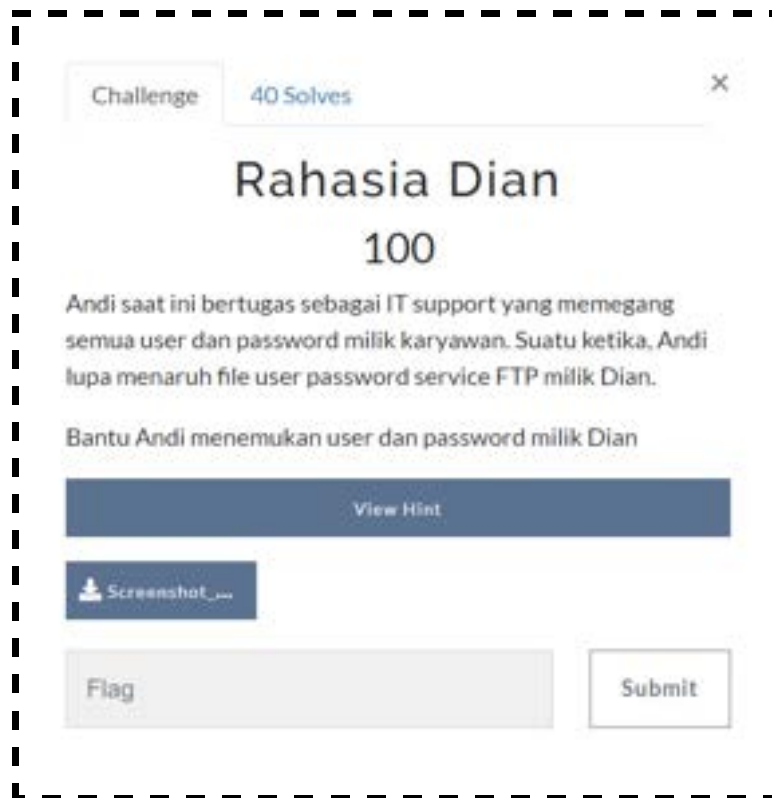
Bisa dilihat hasilnya adalah **Good Signature**.

Flag: **flag{GOOD}**

# Credential Leak

---

## Rahasia Dian



Challenge 40 Solves

### Rahasia Dian

100

Andi saat ini bertugas sebagai IT support yang memegang semua user dan password milik karyawan. Suatu ketika, Andi lupa menaruh file user password service FTP milik Dian.

Bantu Andi menemukan user dan password milik Dian

View Hint

Screenshot

Flag Submit

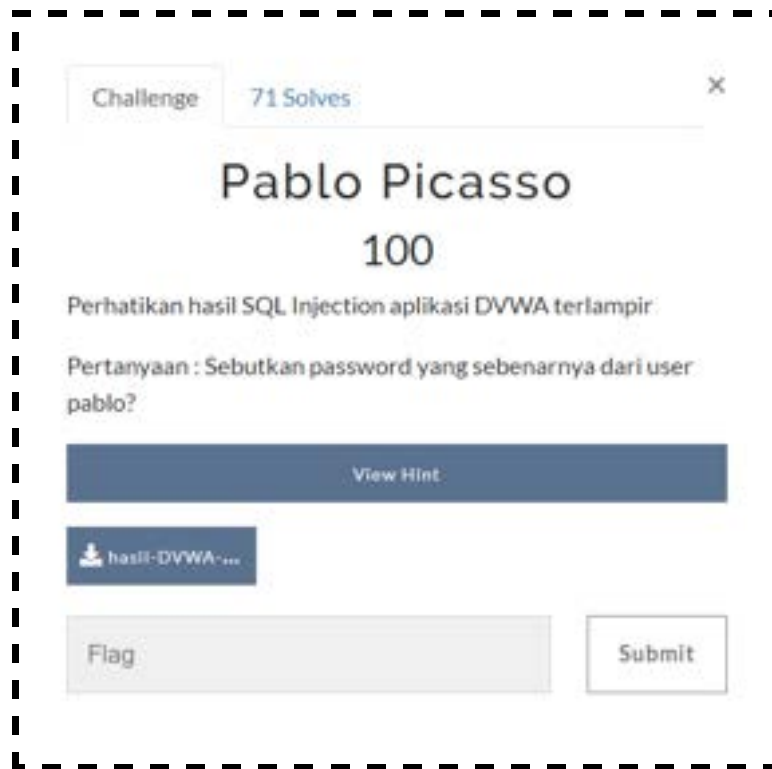
**NOTE:** Service sudah mati atau ditakedown, dan saya tidak bisa memberikan screenshot hasilnya beserta flagnya

Diberikan sebuah soal dan deskripsi, kita diharuskan untuk mencari password FTP dari user Dian. Diberikan juga sebuah file screenshot dari service ssh beserta user nya

no	karyawan	server	service	user	password
1	Andi	180.214.246.108:2204	SSH	user4	password4

Kemudian kita bisa langsung masuk ke machine nya menggunakan SSH, sesuai dengan informasi pada gambar tersebut. Setelah masuk kita langsung mencari password Dian, berdasarkan hint kita bisa mencarinya pada **temporary folder**. Awalnya saya mencari di **/tmp** folder ternyata tidak ada, kedua kemudian saya mencari di **/var/tmp** dan ternyata ada file **account.txt** yang isinya adalah password dari beberapa user.

## Pablo Picasso



The screenshot shows a web challenge interface for 'Pablo Picasso' with a score of 100. It includes a 'Challenge' tab, a '71 Solves' count, and a question in Indonesian asking for the password of the user 'pablo' based on a provided SQL injection result. There are buttons for 'View Hint', a download icon for the SQL result file, a 'Flag' input field, and a 'Submit' button.

Diberikan sebuah soal dan deskripsinya, juga diberikan sebuah file hasil SQL Injection dari aplikasi DVWA, kita diharuskan untuk mencari password dari user pablo. Dengan mudah kita bisa melihat hasil SQL Injectionnya, dan mencari user pablo

```
ID: 'X' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
```

Password pablo adalah **0d107d09f5bbe40cade3de5c71e9e9b7**, namun sepertinya password tersebut masih terenkripsi dengan MD5, kemudian saya melakukan decode hash tersebut secara online

**Found : letmein**  
(hash = 0d107d09f5bbe40cade3de5c71e9e9b7)

**Flag: flag{letmein}**

# Data Leak

---

## MyWEB



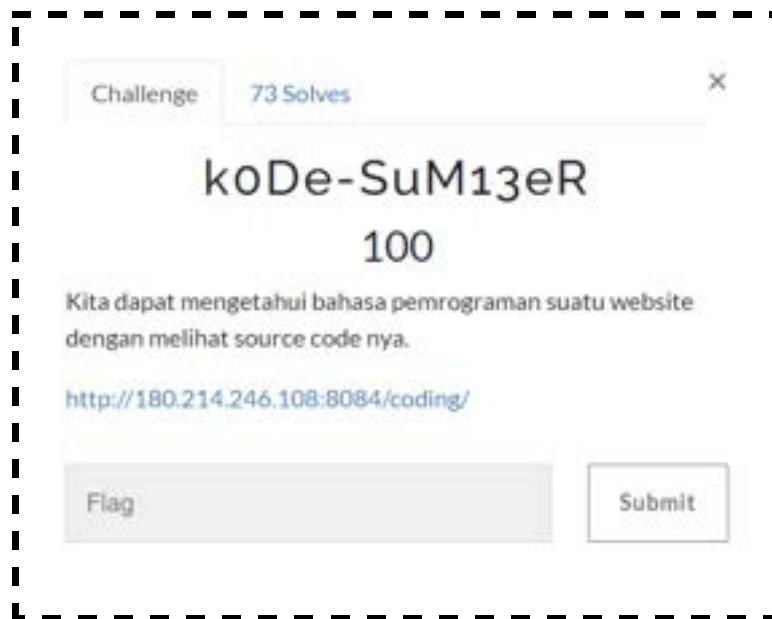
**NOTE:** Service sudah mati atau ditakedown, dan saya tidak bisa memberikan screenshot hasilnya beserta flagnya

Diberikan sebuah web service, didalam deskripsi dikatakan bahwa web tersebut menyimpan sebuah pesan yang disimpan disebuah direktori

Saya kemudian mengecek page source nya, dan melihat kira kira ada direktori apa saja yang digunakan, setelah dicek ada beberapa direktori yaitu direktori **js**, **css**, dan **assets** kemudian saya cek satu persatu hingga saya menemukan ada yang unik didalam direktori **assets**, dimana didalamnya ada direktori lagi, dan kemudian saya buka hingga saya menemukan sebuah file yang isinya adalah sebuah flag



## k0De-SuM13eR



**NOTE:** Service sudah mati atau ditakedown, dan saya tidak bisa memberikan screenshot hasilnya beserta flagnya

Diberikan sebuah web service, sesuai judul soal dan deskripsi kita bisa mengecek kode sumber nya

Dengan cara bisa melalui **inspect element** atau langsung mengecek melalui **view page source**, setelah dicek nanti akan ada sebuah flag yang dicomment

# Reconnaissance

---

## Scan Me!

Challenge

57 Solves

X

Scan Me!

100

Sebuah website dengan alamat <http://180.214.246.148> mempunyai beberapa service port. Dengan menggunakan teknik portscanning, service XMPP ada di port berapa ?

Flag

Submit

Diberikan sebuah soal dan deskripsinya, tugas kita adalah untuk mencari port berapa yang digunakan untuk service XMPP sesuai dengan alamat website yang diberikan. Kita akan menggunakan port scanning menggunakan NMAP

```
(root@sijastemba2202)-[~/itts/stego/ctrl+a]
# nmap -sS -P 180.214.246.148
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 09:21 WIB
Nmap scan report for 180.214.246.148
Host is up (0.026s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
113/tcp   closed ident
8010/tcp  open  xmpp
8082/tcp  open  blackice-alerts

Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
```

Dari hasil Nmap, service XMPP running pada port 8010

**Flag: flag{8010}**

## NM4P

Challenge

69 Solves

X

# NM4P

## 100

Dari hasil nmap sebuah server, diperoleh hasil sebagai berikut :

```
nmap -sT -p- -A 192.168.0.92 Starting Nmap 7.93 (  
https://nmap.org) at 2023-02-02 19:33 EST Nmap scan report  
for 192.168.0.92 Host is up (0.00049s latency). Not shown:  
65524 closed tcp ports (conn-refused)
```

- PORT STATE SERVICE VERSION
- 21/tcp open ftp vsftpd 3.0.3
- 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
- 23/tcp open telnet Linux telnetd
- 25/tcp open smtp Postfix smtpd
- 53/tcp open domain ISC BIND 9.11.3-1ubuntu1.5 (Ubuntu Linux)
- 80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
- 110/tcp open pop3 Dovecot pop3d
- 143/tcp open imap Dovecot imapd (Ubuntu)
- 993/tcp open ssl/imap Dovecot imapd (Ubuntu)
- 995/tcp open ssl/pop3 Dovecot pop3d
- 3306/tcp open mysql MySQL (unauthorized) Nmap

done: 1 IP address (1 host up) scanned in 31.98 seconds

Pertanyaan : Sebutkan nomor port yang terdeteksi, berurutan dari kecil ke besar dan dipisahkan dengan spasi

Flag

Submit

Diberikan sebuah soal dan log dari hasil scanning port menggunakan nmap, kita diharuskan untuk menuliskan port yang terdeteksi dari hasil scanning tersebut, dengan mudah kita bisa susun hasilnya menjadi sebuah flag dipisahkan dengan spasi mulai dari yang terkecil

**Flag: flag{21 22 23 25 53 80 110 143 993 995 3306}**

# Steganography

---

Ctrl + A



Diberikan sebuah soal, yang awalnya deskripsi dari soal tersebut blank, tapi sesuai dengan judul soal **Ctrl + A**, kita bisa melihat bahwa deskripsi soal tersebut sebenarnya ada tapi warnanya putih jadi ketika di select tetap bisa terlihat.

Dijelaskan bahwa kita perlu mengganti ekstensi file yang diberikan dengan ekstensi file gambar, berarti dengan mudah kita bisa download file yang diberikan dan mengganti ekstensi nya, misal disini saya ganti dari **.txt** menjadi **.jpg**



Flag: `flag{SmkBisaHebatSiapKerjaSantunMandiriKreatif}`