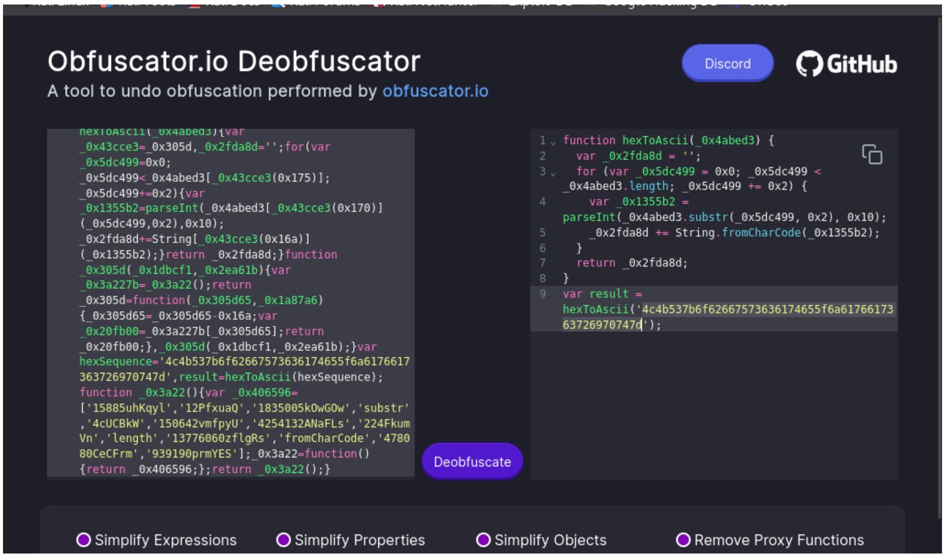
Writeup Jeopardy

LKS Kota 2024

SMKN 4 Bandung
Muhammad Dhafin Ramadhan
Muhamad Ajib Firdaus Supian

Reverse Engineering

gaJelaS



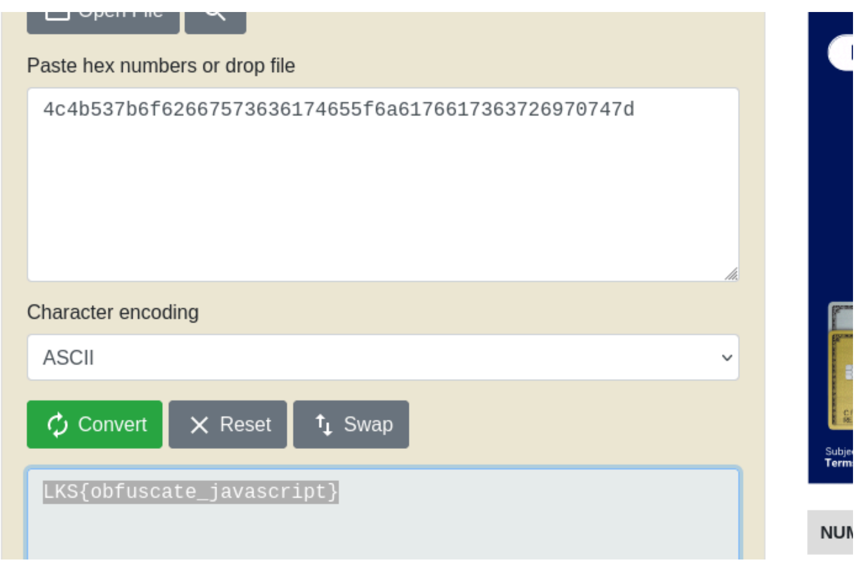
Obfuscator.io Deobfuscator

A tool to undo obfuscation performed by obfuscator.io

```
hexToAscii(_0x4abed3){var
_0x43cce3=_0x305d,_0x2fda8d='';for(var
_0x5dc499=0x0;
_0x5dc499<_0x4abed3[_0x43cce3(0x175)];
_0x5dc499+=0x2){var
_0x1355b2=parseInt(_0x4abed3[_0x43cce3(0x170)]
(_0x5dc499,0x2),0x10);
_0x2fda8d+=String[_0x43cce3(0x16a)]
(_0x1355b2);}return _0x2fda8d;}function
_0x305d(_0x1dbcf1,_0x2ea61b){var
_0x3a227b=_0x3a22();return
_0x305d=function(_0x305d65,_0x1a87a6)
{_0x305d65=_0x305d65-0x16a;var
_0x20fb00=_0x3a227b[_0x305d65];return
_0x20fb00;},_0x305d(_0x1dbcf1,_0x2ea61b);}var
hexSequence='4c4b537b6f626675736361746 55f6a6176617
363726970747d',result=hexToAscii(hexSequence);
function _0x3a22(){var _0x406596=
['15885uhKqyl','12PfxuaQ','1835005kOwGOw','substr'
,'4cUCBkW','150642vmfpyU','4254132ANaFLs','224Fkum
Vn','length','13776060zflgRs','fromCharCode','4780
80CeCFrm','939190prmYES'];_0x3a22=function()
{return _0x406596;};return _0x3a22();}
```

```
function hexToAscii(_0x4abed3) {
  var _0x2fda8d = '';
  for (var _0x5dc499 = 0x0; _0x5dc499 <
_0x4abed3.length; _0x5dc499 += 0x2) {
    var _0x1355b2 =
parseInt(_0x4abed3.substr(_0x5dc499, 0x2), 0x10);
    _0x2fda8d += String.fromCharCode(_0x1355b2);
  }
  return _0x2fda8d;
}
var result =
hexToAscii('4c4b537b6f6266757363617465 5f6a61766173
63726970747d');
```

○ Simplify Expressions ○ Simplify Properties ○ Simplify Objects ○ Remove Proxy Functions



Paste hex numbers or drop file

```
4c4b537b6f626675736361746 55f6a617661736372697074 7d
```

Character encoding

ASCII

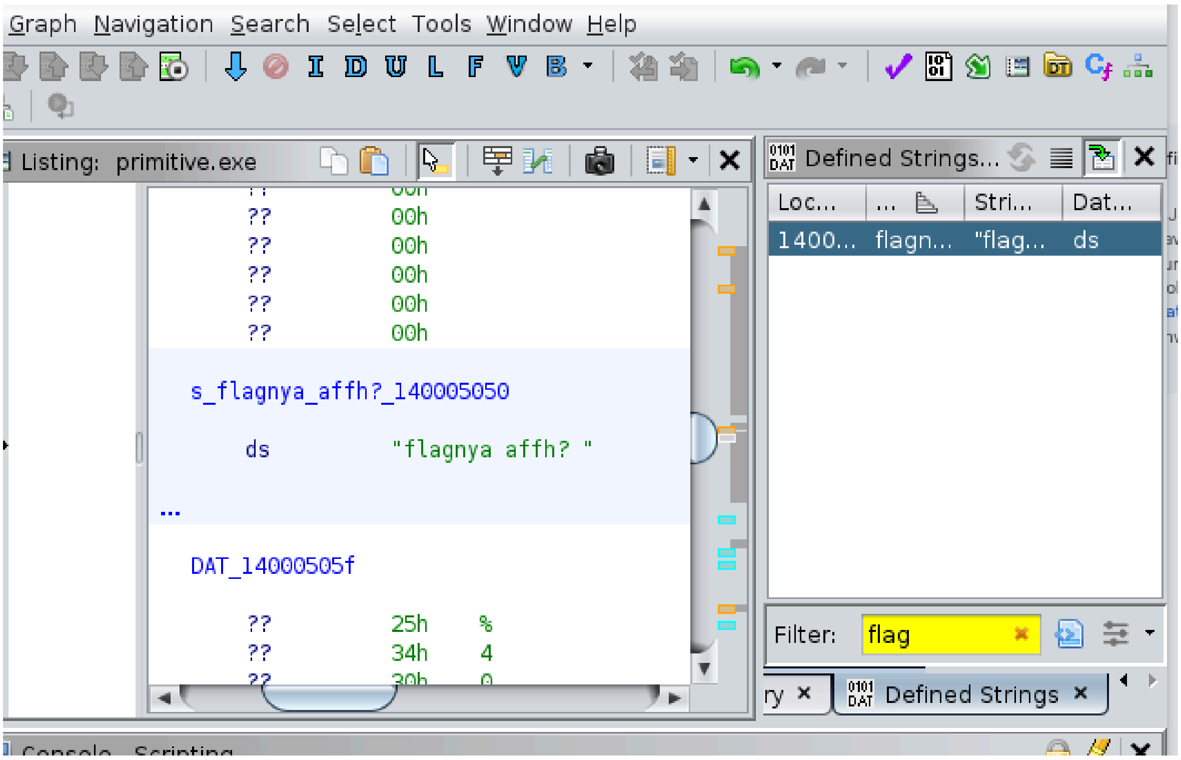
```
LKS{obfuscate_javascript}
```

reverse engineering :gaJelaS

Flag : LKS{Obfuscate_javascript}

Pembahasan : copy seluruh code chall.js yang telah di berikan, lalu lakukan obsfucation pada web https://obf-io.deobfuscate.io/ selanjutnya akan terlihat hex number, convert hex number tersebut dan flag pun ditemukan

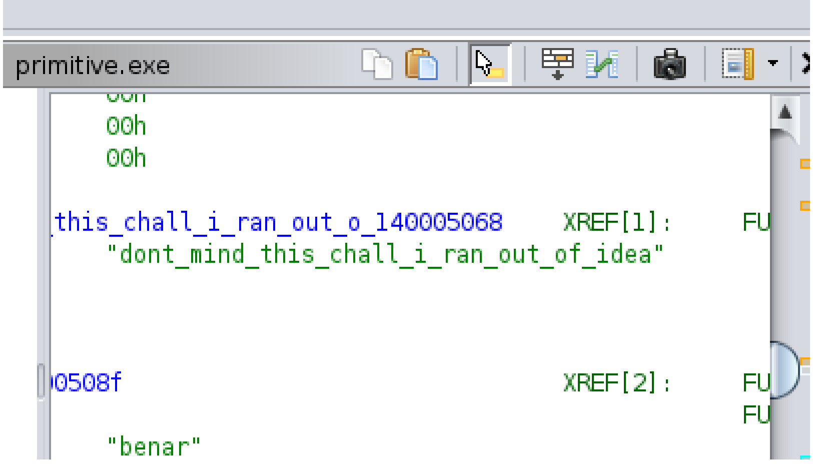
Primitive



```
        ??          00h
        ??          00h
        ??          00h
        ??          00h
        ??          00h

   s_flagnya_affh?_140005050

        ds          "flagnya affh? "

...

   DAT_14000505f

        ??          25h    %
        ??          34h    4
```

Loc...	...	Stri...	Dat...
1400...	flagn...	"flag...	ds

Filter: flag



```
    00h
    00h

this_chall_i_ran_out_o_140005068     XREF[1]:     FU
    "dont_mind_this_chall_i_ran_out_of_idea"



0508f                                XREF[2]:     FU
                                                  FU

    "benar"
```

pertama, saya mencari defined strings, dengan kata kunci flag, setelah itu saya klik 2x lalu muncul flag di gambar ke 2

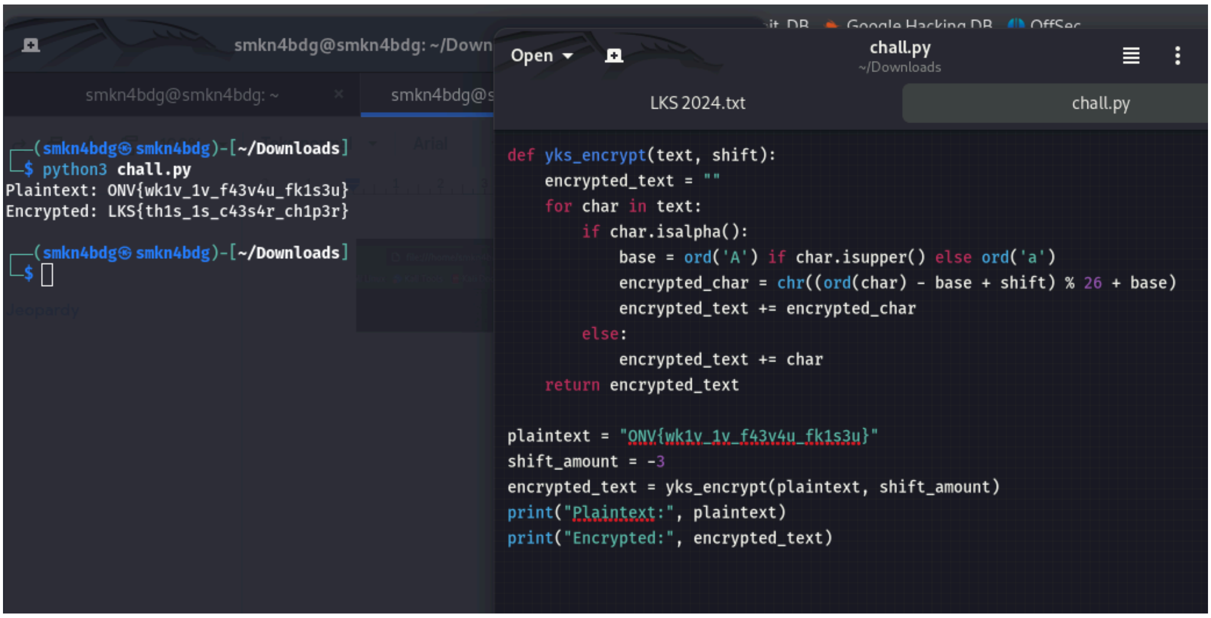
Cryptography

you keep smile

Flag : LKS{th1s_1s_c43s4r_ch1p3r}

dcode caesar cipher

pembahasan : cukup berikan - di shift_amount maka akan mengubah teks yang sudah di encrypt



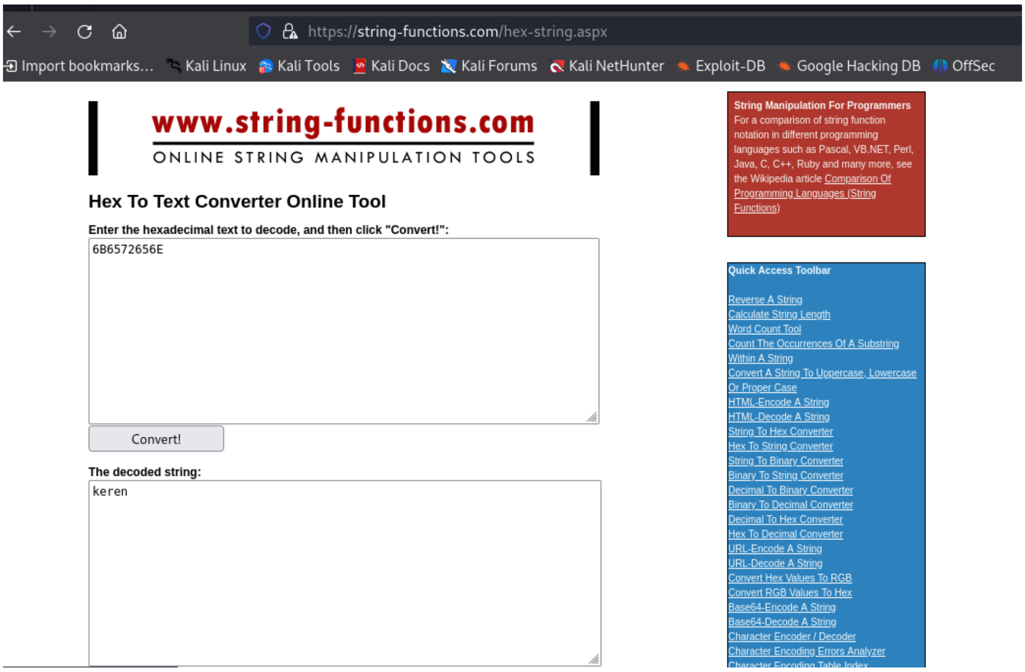
```
┌──(smkn4bdg㉿smkn4bdg)-[~/Downloads]
└─$ python3 chall.py
Plaintext: ONV{wk1v_1v_f43v4u_fk1s3u}
Encrypted: LKS{th1s_1s_c43s4r_ch1p3r}

┌──(smkn4bdg㉿smkn4bdg)-[~/Downloads]
└─$ 
```

```python
def yks_encrypt(text, shift):
    encrypted_text = ""
    for char in text:
        if char.isalpha():
            base = ord('A') if char.isupper() else ord('a')
            encrypted_char = chr((ord(char) - base + shift) % 26 + base)
            encrypted_text += encrypted_char
        else:
            encrypted_text += char
    return encrypted_text

plaintext = "ONV{wk1v_1v_f43v4u_fk1s3u}"
shift_amount = -3
encrypted_text = yks_encrypt(plaintext, shift_amount)
print("Plaintext:", plaintext)
print("Encrypted:", encrypted_text)
```

KARAKTER SPESIAL

flag : LKS{keren}

pembahasan : mencoba mengganti teks: ^b^%&@^%^e sesuai dengan keyboard : 6B6572656E dan descrypt hex to text menggunakan website string-functions.com



https://string-functions.com/hex-string.aspx
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
www.string-functions.com
ONLINE STRING MANIPULATION TOOLS
Convert!
Quick Access Toolbar
Reverse A String
Calculate String Length
Word Count Tool
Count The Occurrences Of A Substring Within A String
Convert A String To Uppercase, Lowercase Or Proper Case
HTML-Encode A String
HTML-Decode A String
String To Hex Converter
Hex To String Converter
String To Binary Converter
Binary To String Converter
Decimal To Binary Converter
Binary To Decimal Converter
Decimal To Hex Converter
Hex To Decimal Converter
URL-Encode A String
URL-Decode A String
Convert Hex Values To RGB
Convert RGB Values To Hex
Base64-Encode A String
Base64-Decode A String
Character Encoder / Decoder
Character Encoding Errors Analyzer
Character Encoding Table Index

Hex To Text Converter Online Tool

Enter the hexadecimal text to decode, and then click "Convert!":

```
6B6572656E
```

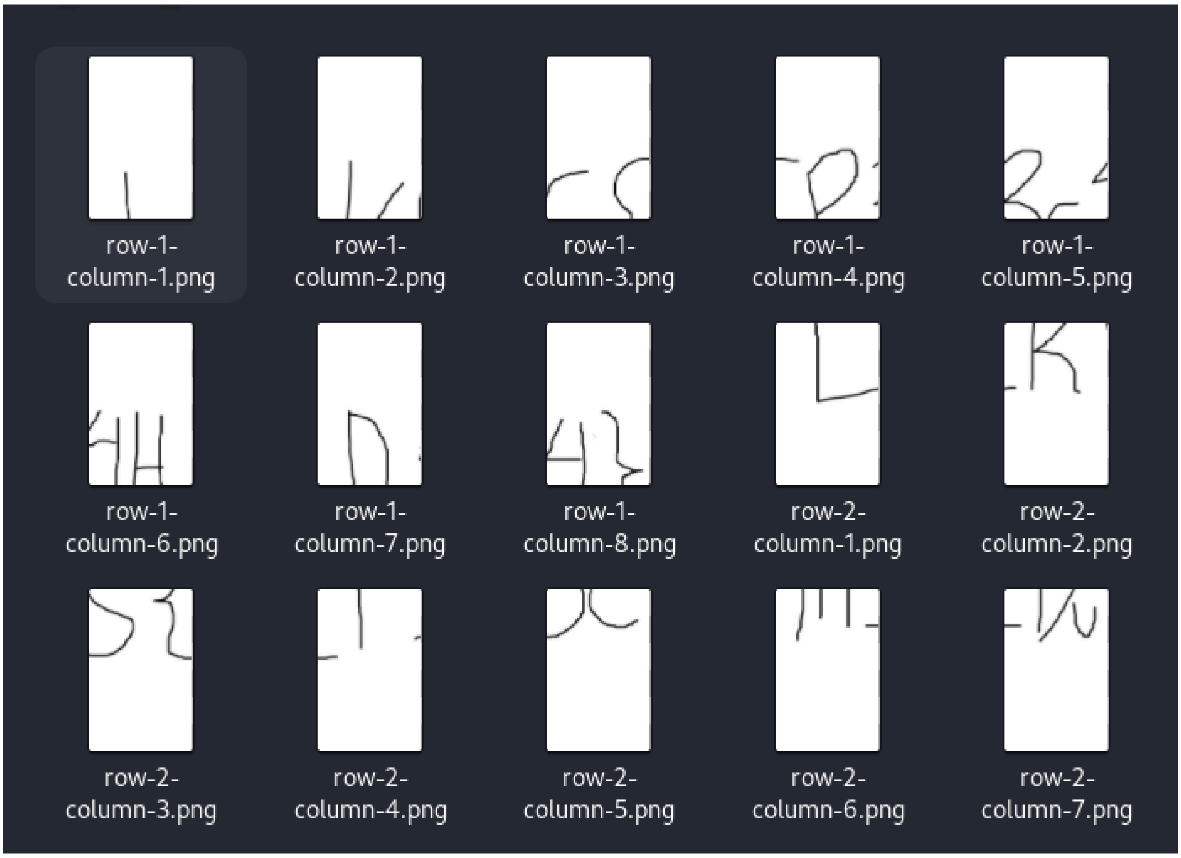
The decoded string:

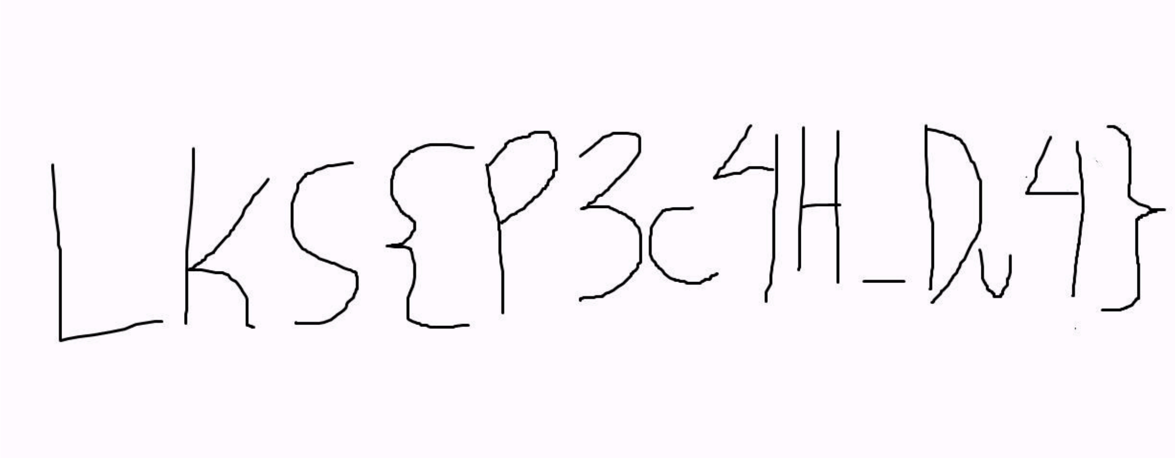
```
keren
```

String Manipulation For Programmers
For a comparison of string function notation in different programming languages such as Pascal, VB.NET, Perl, Java, C, C++, Ruby and many more, see the Wikipedia article Comparison Of Programming Languages (String Functions)

Forensic

Hilang Terbelah





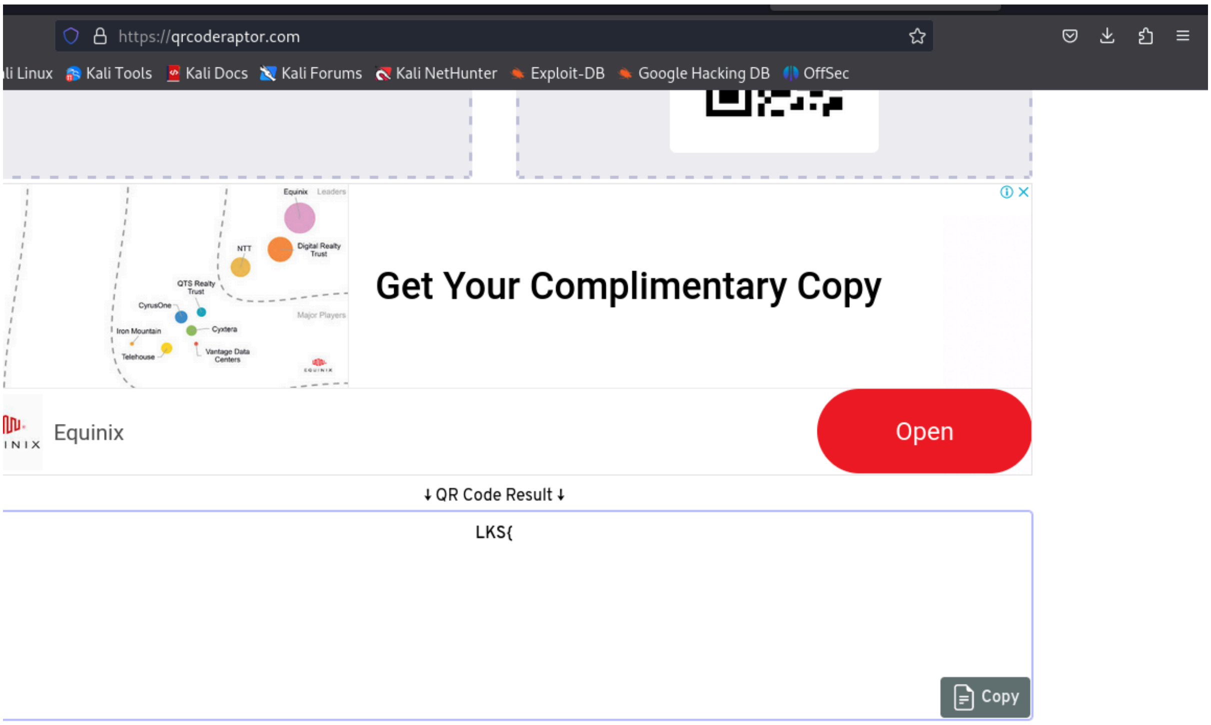
step pertama, buka https://products.aspose.app/words/merger/image# lalu drag semua foto sesuai dengan urutan, dengan begitu kita bisa merge foto tersebut dan mendapatkan flag

QRCODESS

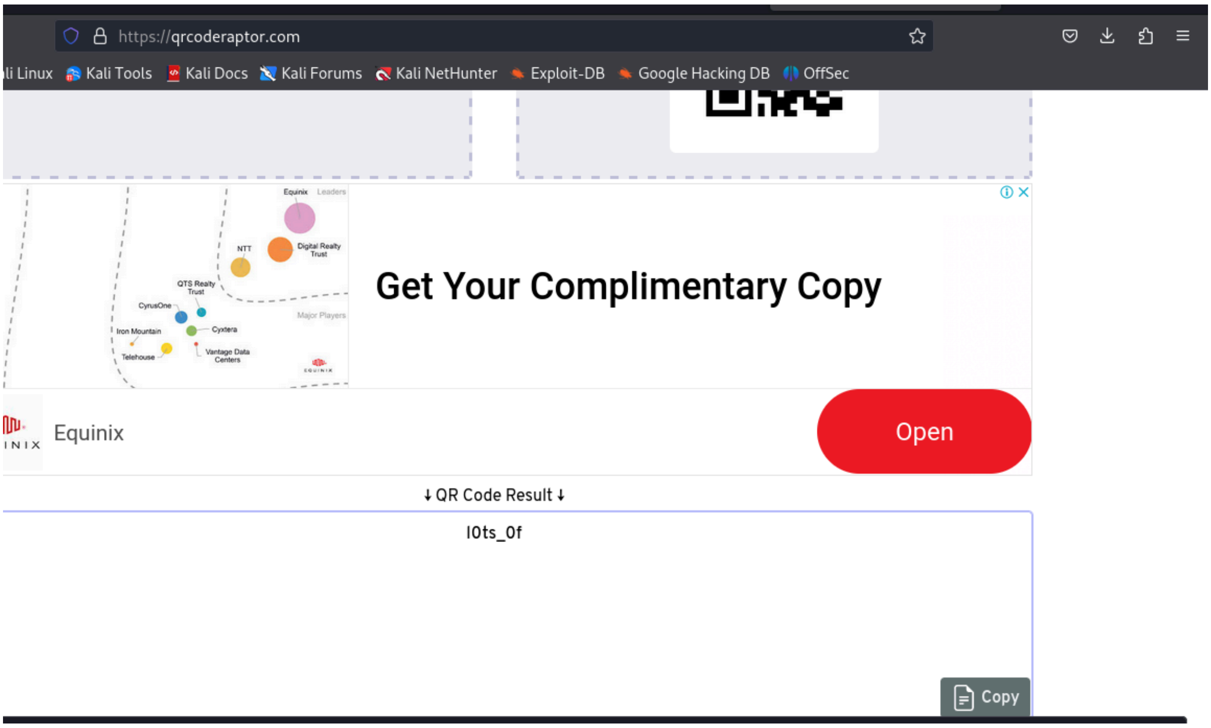
Forensic : QRCODESS

flag : LKS{l0ts_0f_qr_c0d3s}

pembahasan : mencoba menggunakan qrcode converter qr to string di website qrcoderaptor.com dan mengconvert file 7, 18 dan 32 dan menghasilkan flag

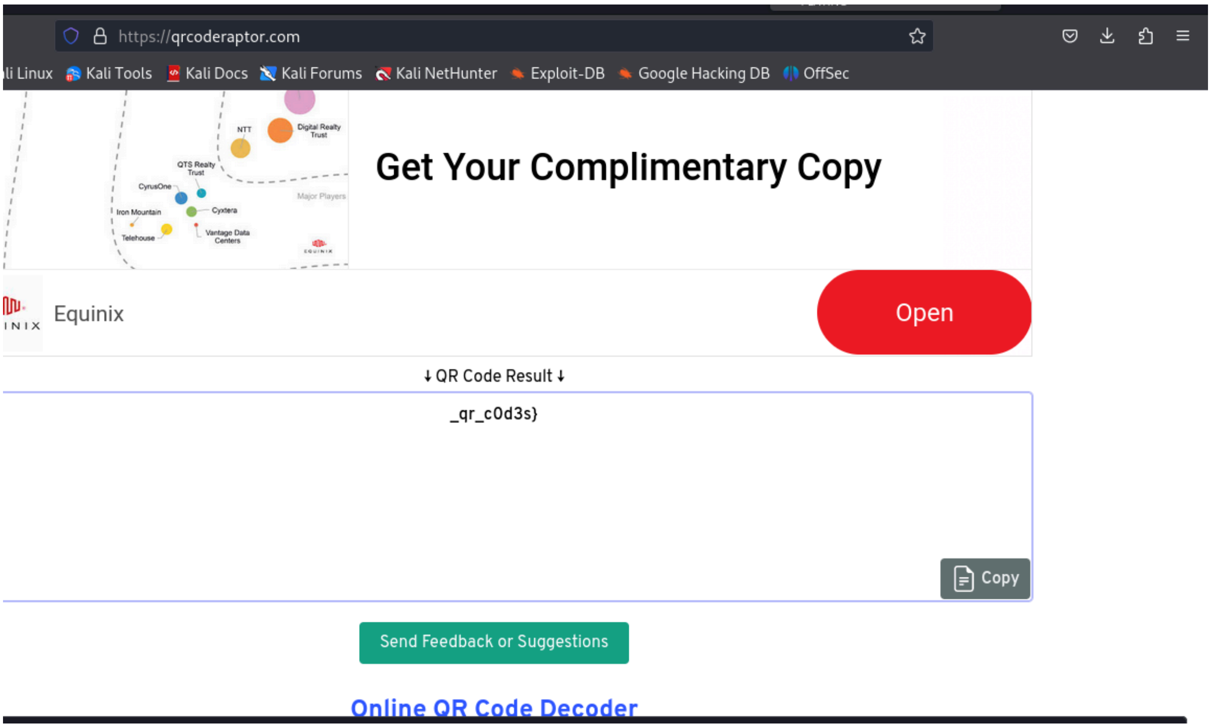


LKS{



↓ QR Code Result ↓

```
l0ts_0f
```



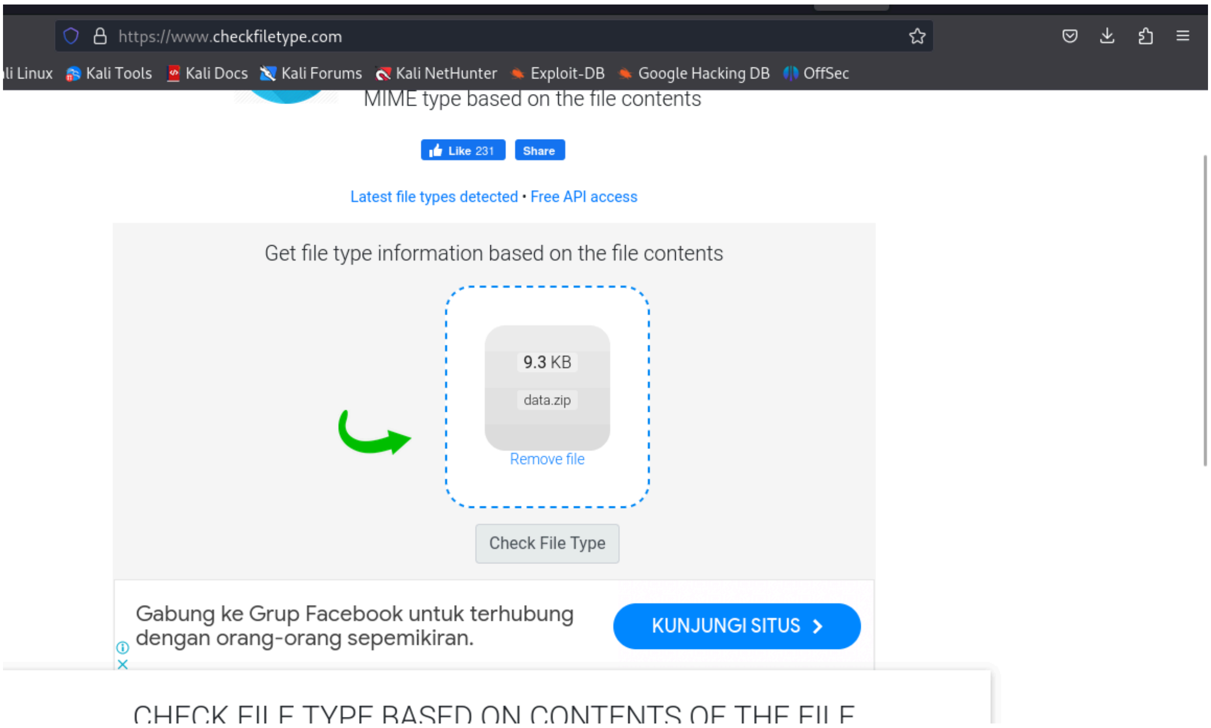
↓ QR Code Result ↓

```
_qr_c0d3s}
```

Data 1

Flag : LKS{this_is_important_data_that_I_must_protect}

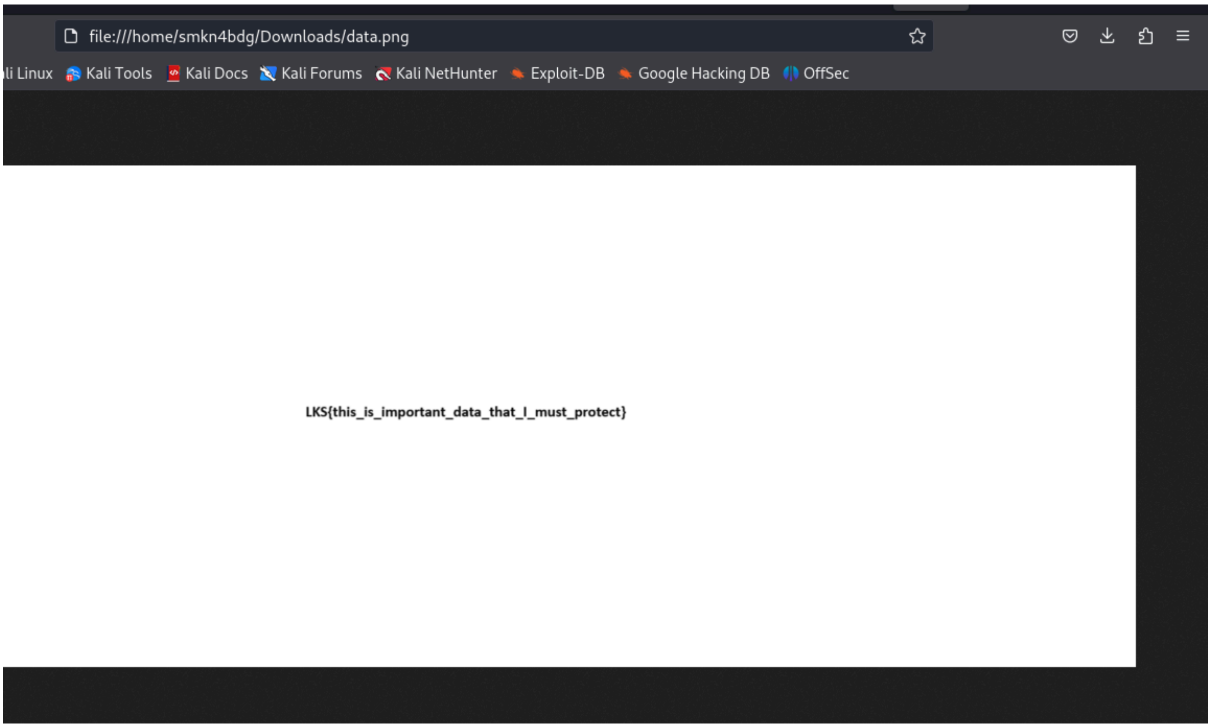
Pembahasan : cek ekstensi file yang sebenarnya di website www.checkfiletype.com dan ekstensi file sebenarnya png dan ubah file zip tadi jadi png



MIME type based on the file contents

Get file type information based on the file contents

CHECK FILE TYPE BASED ON CONTENTS OF THE FILE



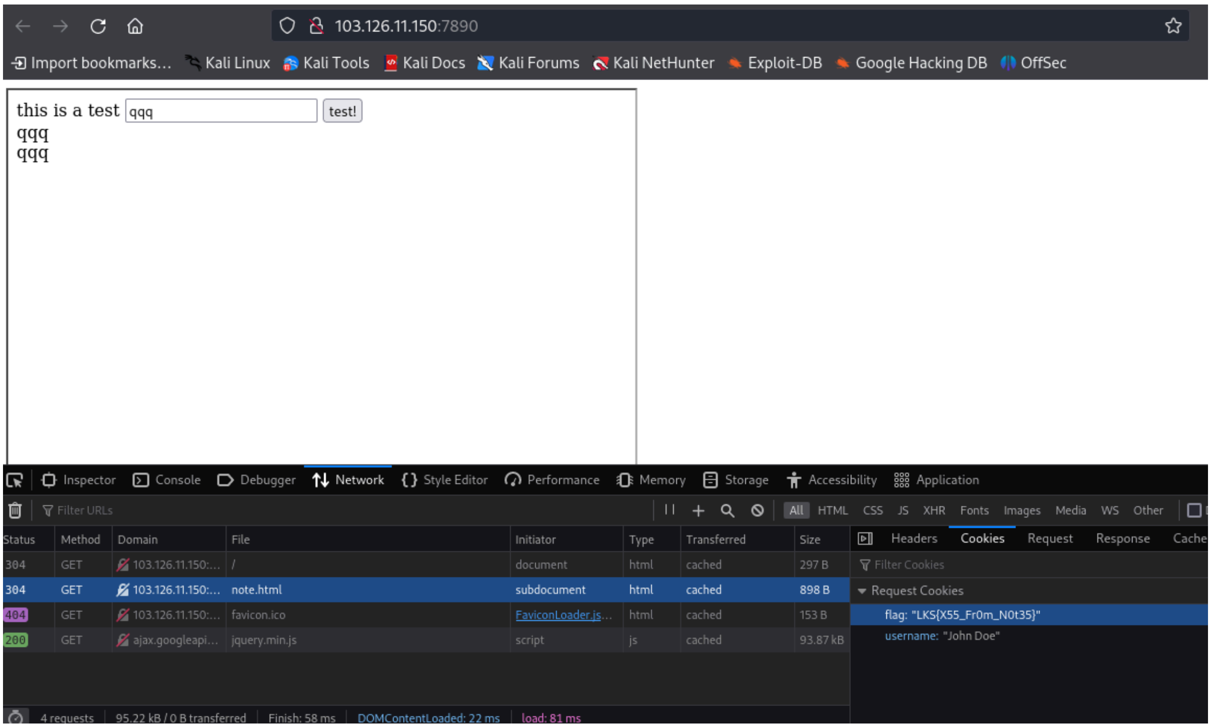
LKS{this_is_important_data_that_I_must_protect}

Web Exploitation

Client Side

Flag : LKS{X55_Fr0m_N0t35}

pembahasan : coba 1x submit form dan lihat request cookies dan muncul flag : LKS{X55_Fr0m_N0t35}



103.126.11.150:7890

this is a test qqq test!
qqq
qqq

Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	103.126.11.150:…	/	document	html	cached	297 B
304	GET	103.126.11.150:…	note.html	subdocument	html	cached	898 B
404	GET	103.126.11.150:…	favicon.ico	FaviconLoader.js…	html	cached	153 B
200	GET	ajax.googleapi…	jquery.min.js	script	js	cached	93.87 kB

4 requests | 95.22 kB / 0 B transferred | Finish: 58 ms | DOMContentLoaded: 22 ms | load: 81 ms

Request Cookies

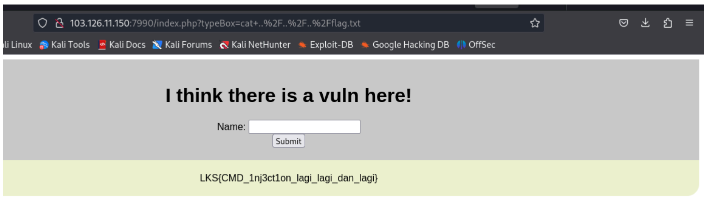
```
flag: "LKS{X55_Fr0m_N0t35}"
username: "John Doe"
```

Import bookmarks… Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Headers Cookies Request Response Cache
Filter Cookies

CMD 2

Flag : LKS{CMD_1nj3ct1on_lagi_lagi_dan_lagi}

pembahasan : karena form nya untuk cmd maka kita cari file flag.txt dan file tersebut ada di ../../../flag.txt



103.126.11.150:7990/index.php?typeBox=cat+..%2F..%2F..%2Fflag.txt

I think there is a vuln here!

Name:

Submit

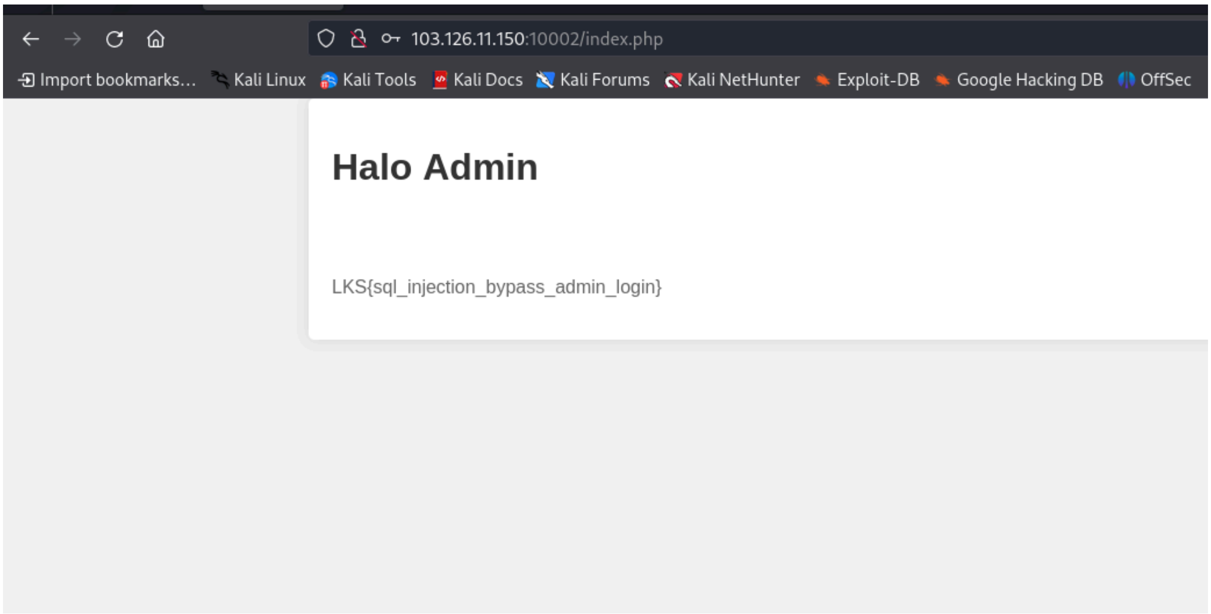
LKS{CMD_1nj3ct1on_lagi_lagi_dan_lagi}

li Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Admin Login

flag : LKS{sql_injection_bypass_admin_login}

pembahasan : disini mencoba injection field nya dengan mengisi username 1' or '1' = '1 dan password : 1' or '1' = '1



103.126.11.150:10002/index.php

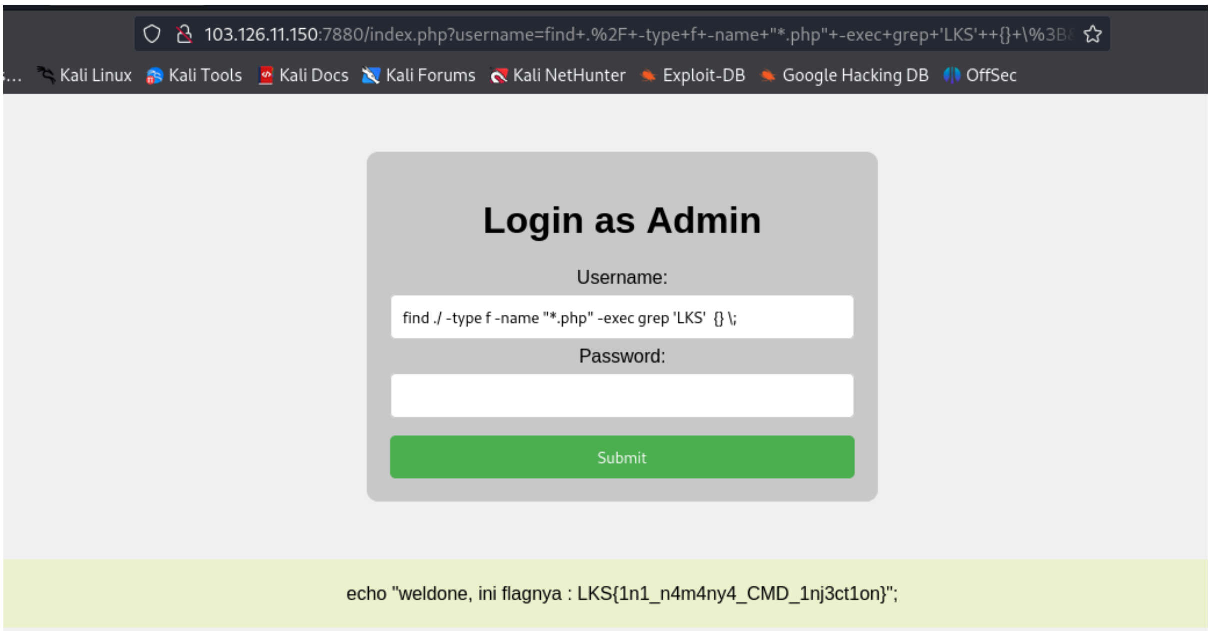
Halo Admin

LKS{sql_injection_bypass_admin_login}

CMD 1

flag : LKS{1n1_n4m4ny4_CMD_1nj3ct1on}

pembahasan : disini menggunakan command find dan exec grep ‘LKS’ dan munculah baris code yang menampilkan flag nya



```
103.126.11.150:7880/index.php?username=find+.%2F+-type+f+-name+"*.php"+-exec+grep+'LKS'++{}+\%3B
```

Login as Admin

Username:

```
find ./ -type f -name "*.php" -exec grep 'LKS'  {} \;
```

Password:

```
echo "weldone, ini flagnya : LKS{1n1_n4m4ny4_CMD_1nj3ct1on}";
```

REVERSE ENGINEERING