OWASP Juice Shop – Security Logging and Monitoring Failures
Praktikum Keamanan Jaringan

Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Fifin Nur Rahmawati (3122640040)

Lula Rania Salsabilla (3122640045)

1 D4 – IT B LJ

D4 TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Security Logging and Monitoring Failures

Deskripsi

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 dalamlog. 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 yangsensitive
  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 yanggagal berkali-kali.

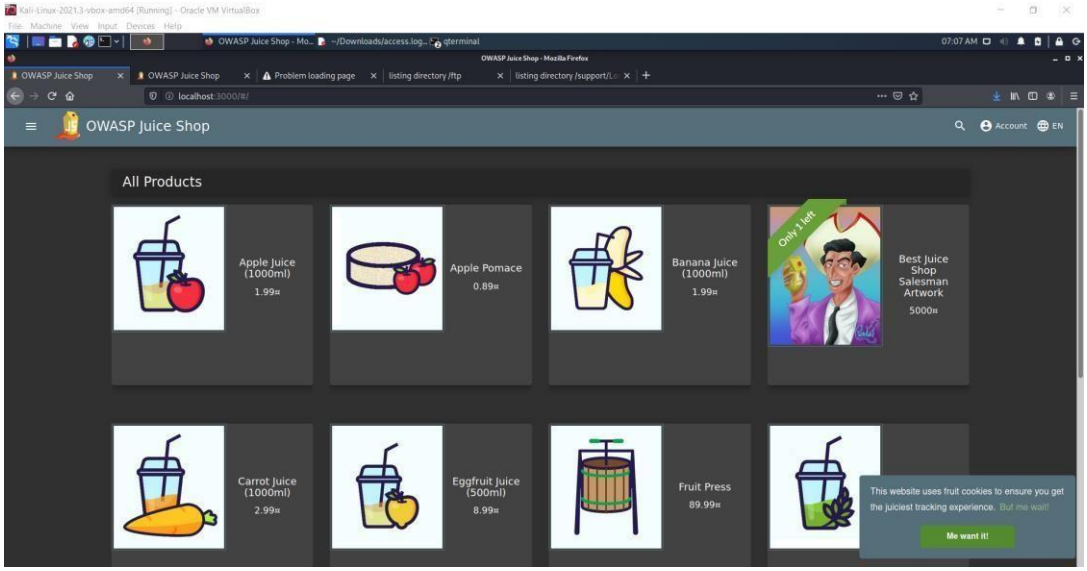
Dalam percobaan kali ini, kali mencoba 2 percobaan yaitu :

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 berulangkali dengan kesalahan username dan password tidak dihiraukan dan tetap bisa memasukkan username dan password yang lainnya).

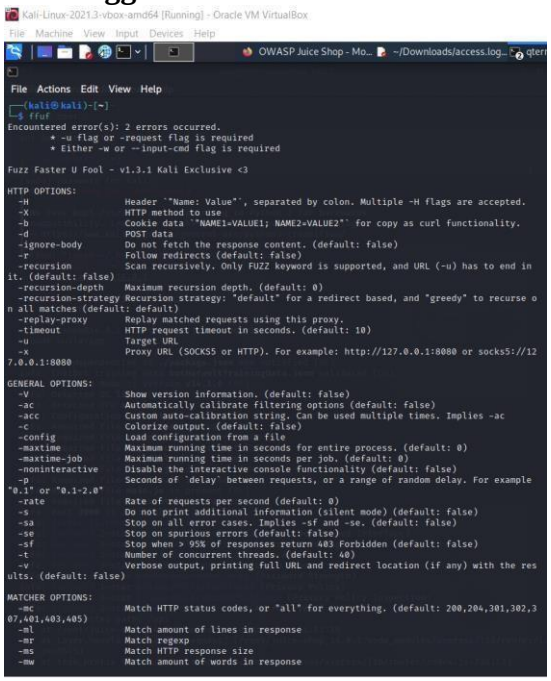
Percobaan

Pada percobaan ini akan menunjukan mendownload file access log.

1. Buka Aplikasi Juice Shop.



2. Menggunakan FFUF.

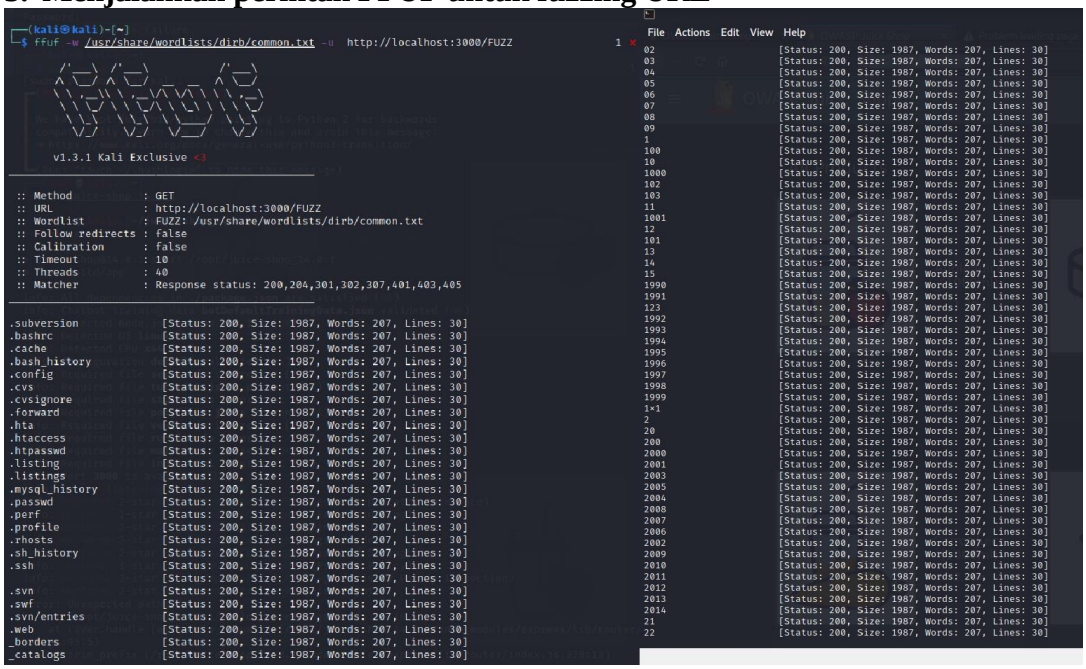


Penjelasan : FFUF merupakan alat untuk melakukan fuzzing pada aplikasi web. Fuzzing adalah proses pengujian perangkat lunak yang melibatkan pengiriman input yang tidak valid, acak, atau tidak terduga ke aplikasi target, dengan tujuan menemukan kelemahan atau kerentanan yang dapat dieksploitasi.

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
```

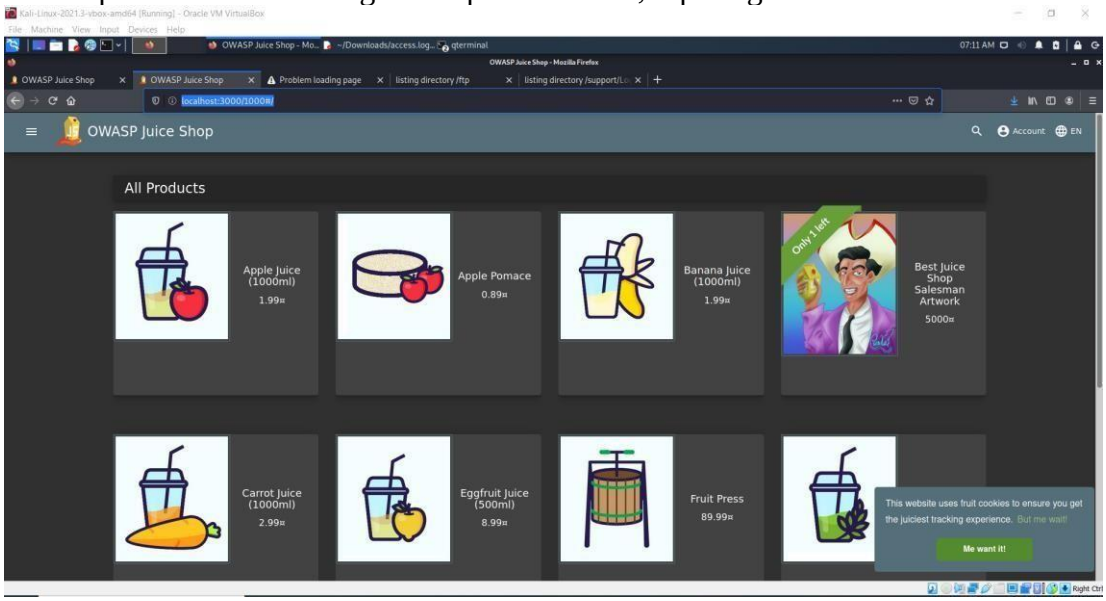
3. Menjalankan perintah FFUF untuk fuzzing URL



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 ataufile yang ada pada server web. Wordlist umum ini biasanya mencakup beberapa namafile umum, direktori umum, atau jalur URL yang sering digunakan dalam aplikasi web.

Dari hasil diatas didapatkan status 200 dan size nya 1987 semua. Disini saya akan mencoba menerapkan salah satu string diatas pada browser, seperti gambar dibawah ini :



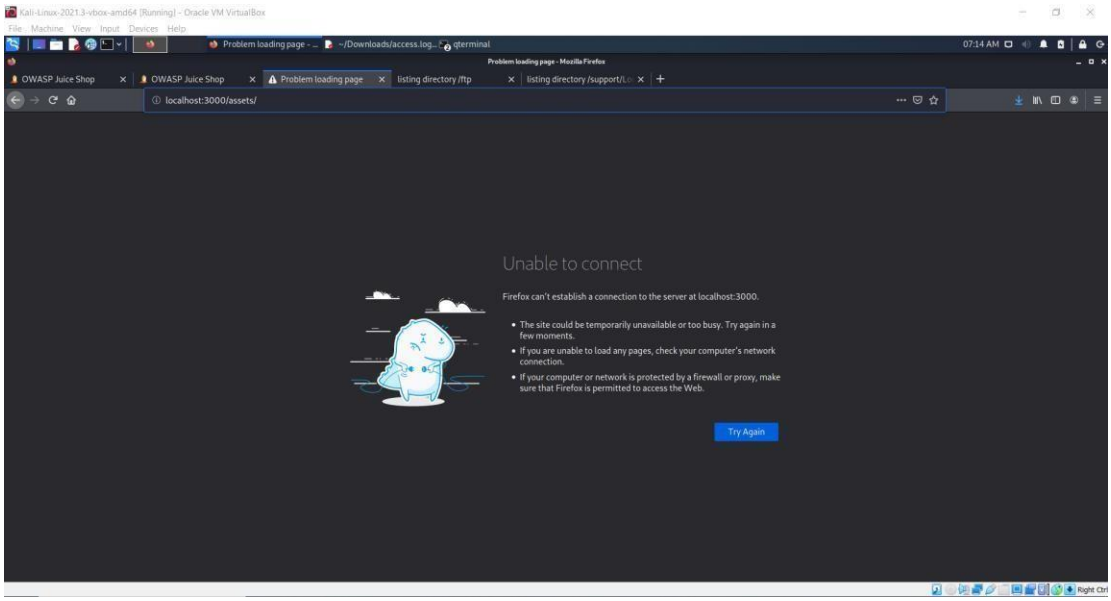
Pada gambar diatas , mencoba mengakses localhost:3000/1000 , dan ternyata untuk halaman yang ditampilkan adalah list product. Dikarenakan pada hasil sebelumnya status dan size nya sama, hal ini memungkinkan bahwa juice shop memang bisa menerima url lain namun diarahkan ke list product.

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

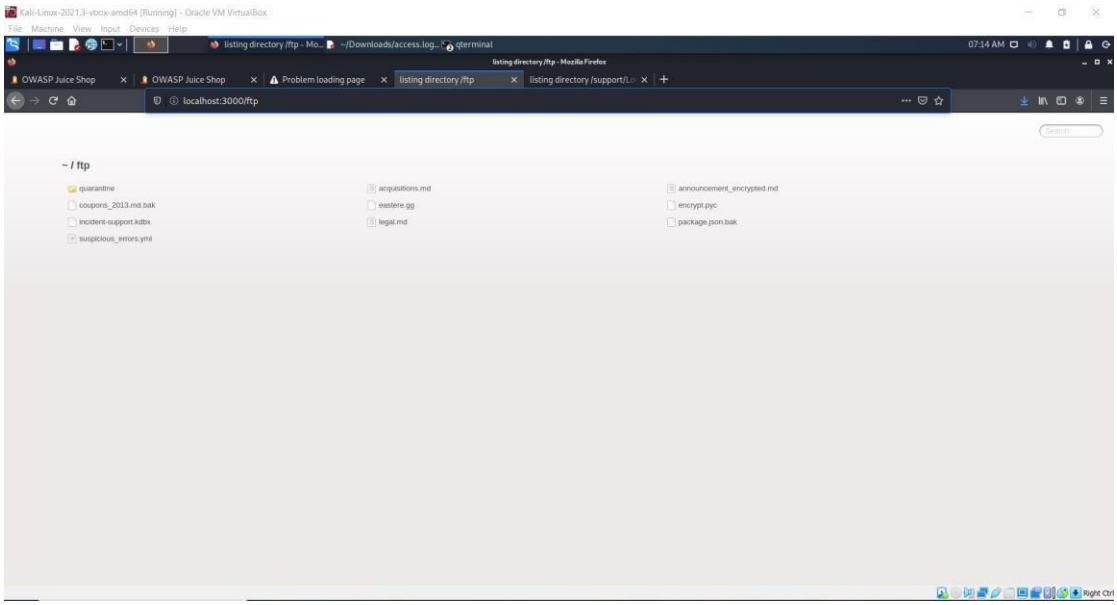
```
┌──(kali㉿kali)-[~]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u  http://localhost:3000/FUZZ -fs 1987

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       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 :

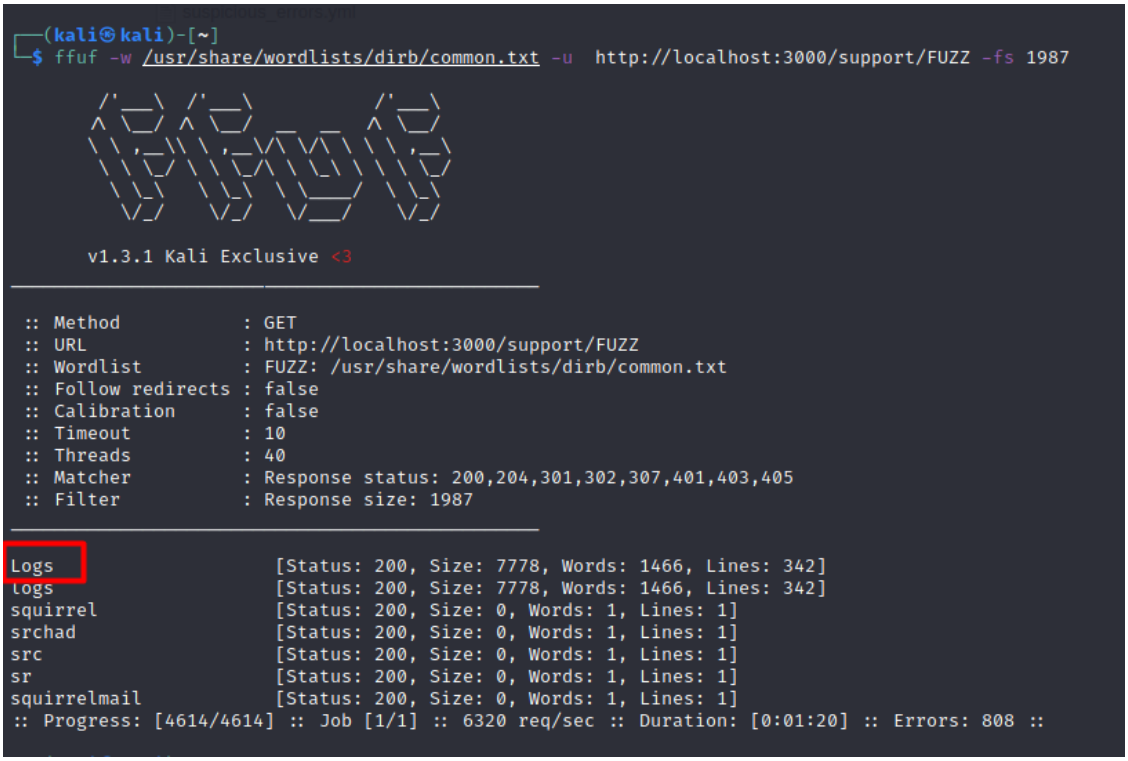


Percobaan pertama /assets tidak didapatkan hasil apapun, selanjutnya mencoba url yang kedua yaitu /ftp dan didapatkan hasil berikut ini :

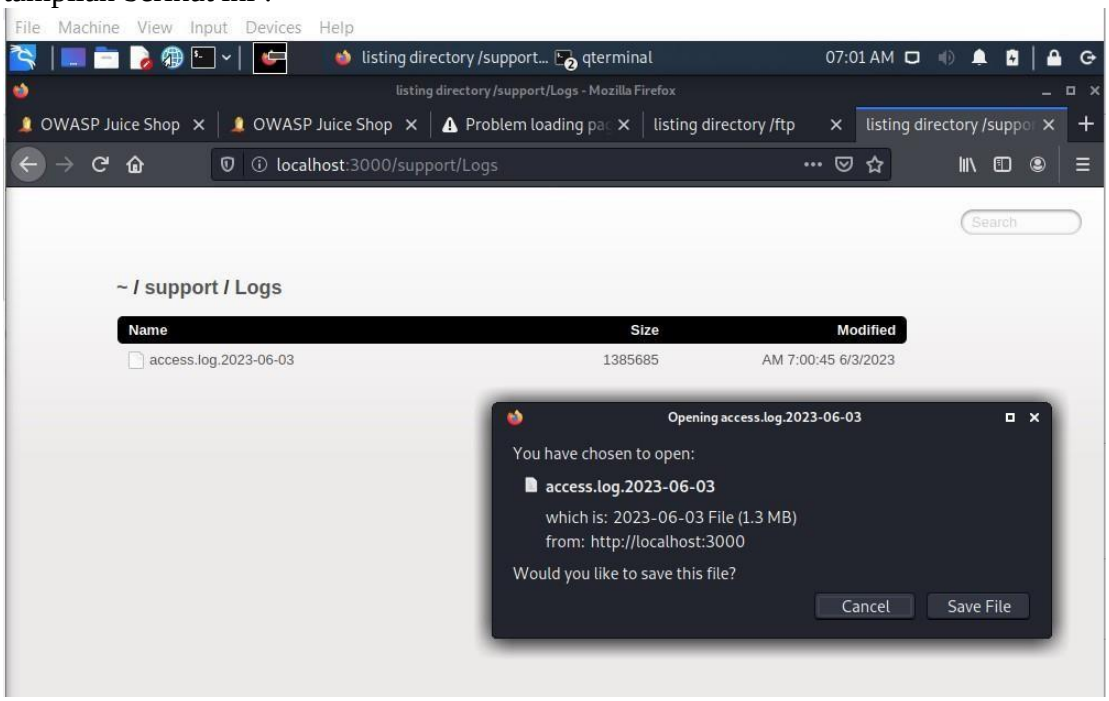


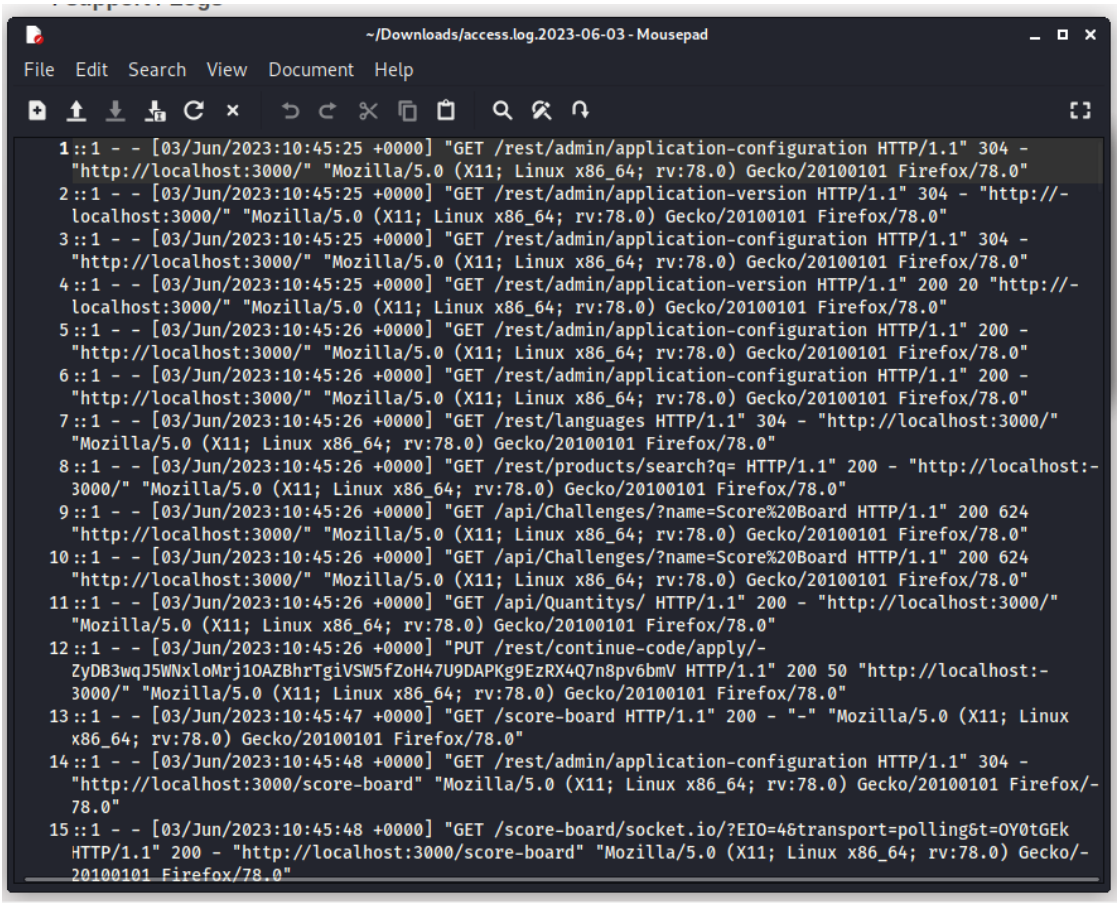
Penjelasan : Dari hasil diatas didapatkan beberapa file, salah satu file yang mungkin bisa mendapatkan informasi lebih detail jika dicari tau lebih dalam adalah file support.

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



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





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

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