

PRAKTIKUM A09
SECURITY LOGGING AND MONITORING FAILURES



DI SUSUN OLEH :
Nadya Indah Trisnawati (3122640034)
Mochammad Jauhar Ulul Albab (3122640044)
LJ D4 IT B

PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

1. Pengertian Security Logging dan Monitoring Failures

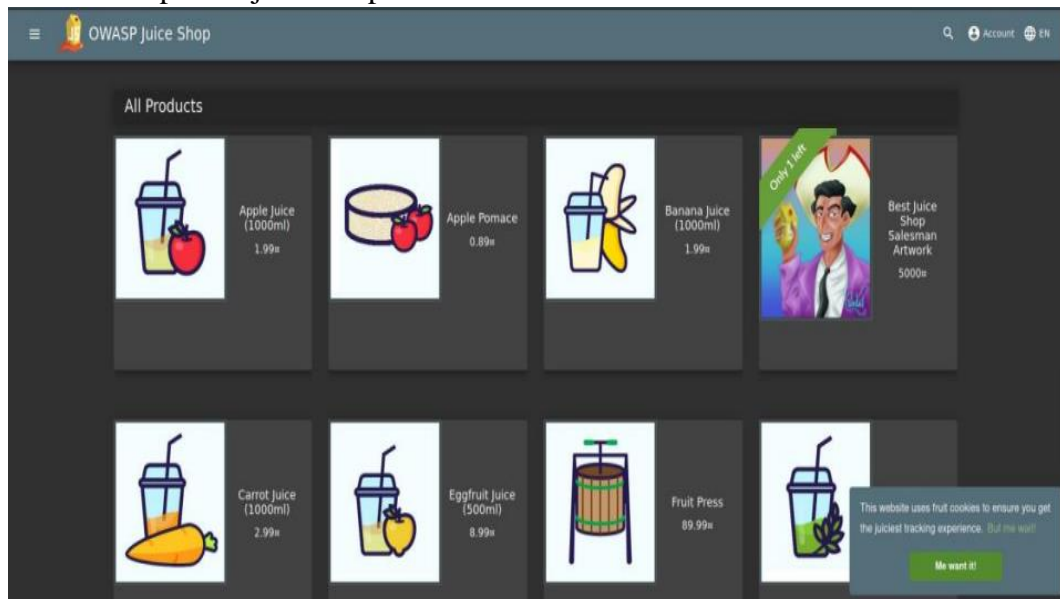
Security logging and monitoring failures adalah salah satu kerentanan keamanan pada aplikasi web yang terjadi ketika sistem atau aplikasi web tidak memiliki mekanisme pengawasan dan pencatatan yang memadai untuk aktivitas pengguna dan akses sistem. Hal ini dapat menyebabkan para penyerang untuk dapat melakukan serangan yang tidak terdeteksi atau menghindari pengawasan oleh para security professional.

Contoh kasus yang dapat terjadi pada security logging and monitoring failures adalah ketika sistem atau aplikasi web tidak memiliki logging dan monitoring yang memadai, sehingga aktivitas yang mencurigakan atau aneh tidak terdeteksi oleh sistem atau para security professional. Hal ini dapat memberikan kesempatan bagi para penyerang untuk mengambil alih sistem atau mencuri data penting tanpa diketahui.

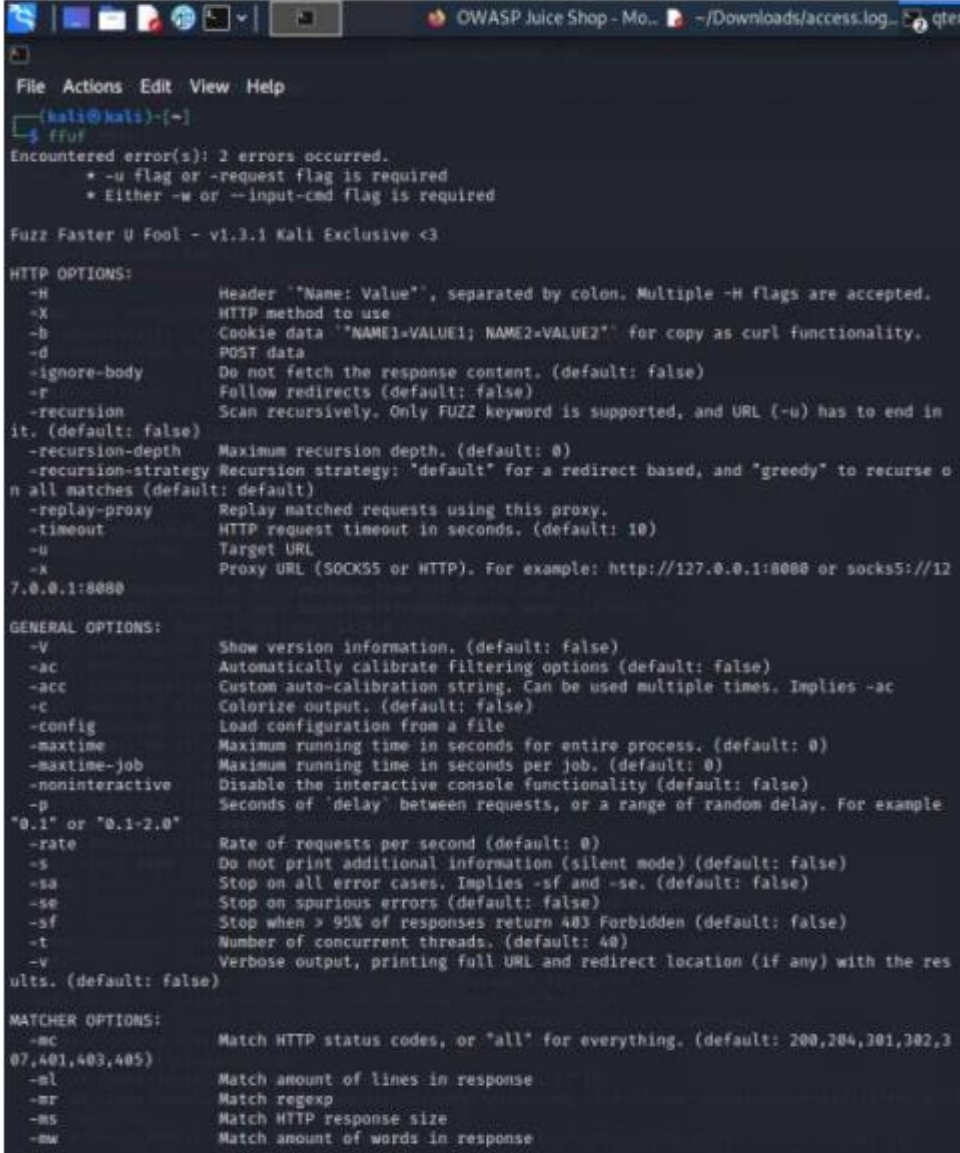
Untuk menghindari kerentanan security logging and monitoring failures, para pengembang dan security professional harus memastikan bahwa sistem atau aplikasi web yang mereka kelola dilengkapi dengan mekanisme logging dan monitoring yang memadai. Hal ini dapat dilakukan dengan cara memasang perangkat lunak logging dan monitoring atau memanfaatkan layanan dari penyedia layanan cloud yang sudah memiliki mekanisme tersebut.

2. Mendownload file access log

- Membuka aplikasi juice shop



- Ketik perintah FFUF pada terminal kali



```

kali@kali:~$ ffuf
Encountered error(s): 2 errors occurred.
  * -u flag or -request flag is required
  * Either -w or --input-cmd flag is required

Fuzz Faster U Fool - v1.3.1 Kali Exclusive <3

HTTP OPTIONS:
-H          Header "Name: Value", separated by colon. Multiple -H flags are accepted.
-X          HTTP method to use
-b          Cookie data "NAME1=VALUE1; NAME2=VALUE2" for copy as curl functionality.
-d          POST data
-ignore-body Do not fetch the response content. (default: false)
-r          Follow redirects (default: false)
-recursion  Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in
it. (default: false)
-recursion-depth Maximum recursion depth. (default: 0)
-recursion-strategy Recursion strategy: "default" for a redirect based, and "greedy" to recurse o
n all matches (default: default)
-replay-proxy Replay matched requests using this proxy.
-timeout     HTTP request timeout in seconds. (default: 10)
-u          Target URL
-k          Proxy URL (SOCKS5 or HTTP). For example: http://127.0.0.1:8080 or socks5://12
7.0.0.1:8080

GENERAL OPTIONS:
-V          Show version information. (default: false)
-ac         Automatically calibrate filtering options (default: false)
-acc        Custom auto-calibration string. Can be used multiple times. Implies -ac
-c          Colorize output. (default: false)
-config     Load configuration from a file
-maxtime    Maximum running time in seconds for entire process. (default: 0)
-maxtime-job Maximum running time in seconds per job. (default: 0)
-noninteractive Disable the interactive console functionality (default: false)
-p          Seconds of 'delay' between requests, or a range of random delay. For example
"0.1" or "0.1-2.0"
-rate       Rate of requests per second (default: 0)
-s          Do not print additional information (silent mode) (default: false)
-sa         Stop on all error cases. Implies -sf and -se. (default: false)
-se         Stop on spurious errors (default: false)
-sf         Stop when > 95% of responses return 403 Forbidden (default: false)
-t          Number of concurrent threads. (default: 40)
-v          Verbose output, printing full URL and redirect location (if any) with the res
ults. (default: false)

MATCHER OPTIONS:
-mc         Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,3
07,401,403,405)
-mL         Match amount of lines in response
-mR         Match regexp
-mS         Match HTTP response size
-mW         Match amount of words in response
  
```

Analisa : FFUF (Fuzz Faster U Fool) adalah alat web fuzzing yang open source, dimana alat ini memiliki fungsi untuk menemukan elemen dan konten tersembunyi dalam aplikasi atau server web. FFUF merupakan aplikasi berbasis baris perintah (command line) yang berjalan di terminal Linux atau command prompt Windows, yang berarti tool FFUF tidak menyediakan GUI interaktif dalam pengoperasiannya

- Menjalankan FFUF untuk fuzzing URL dengan menjalankan perintah :
“ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ”

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

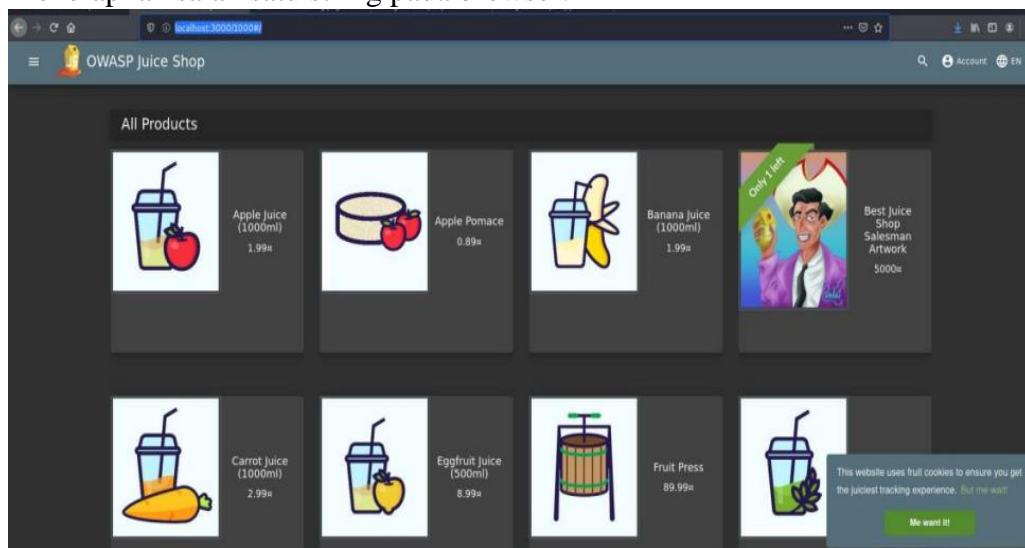
v1.3.1 Kali Exclusive <3>

:: 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]
.swf       [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]
```

Analisa : perintah ffuf ini digunakan untuk mencoba menemukan direktori atau file yang tidak terpublikasi secara langsung pada sebuah situs web dengan mencoba semua kata dari wordlist yang diberikan.

- Menerapkan salah satu string pada browser.



Analisa : pada FFUF diatas didapatkan hasil status 200 dan semua size 1987. Mencoba mengakses localhost:3000/1000 dan hasilnya halaman yang ditampilkan adalah list product.

- Menjalankan Fuzzing URL dengan perintah “-fs”

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

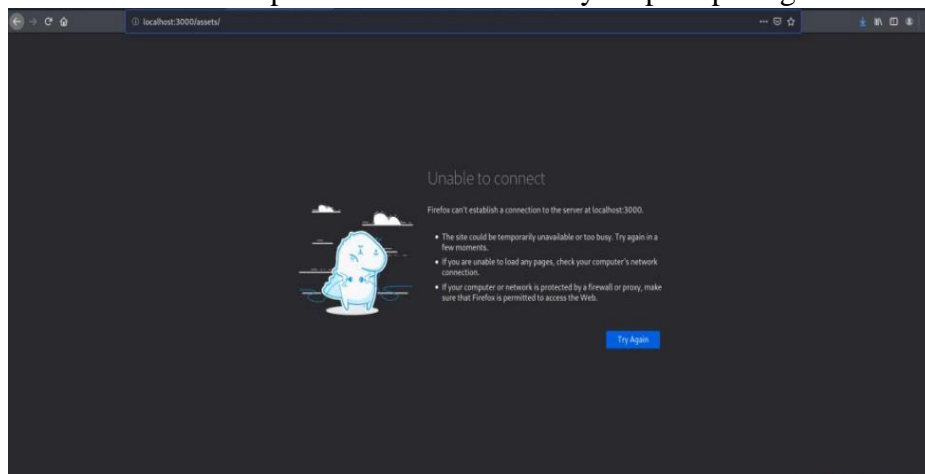
v1.3.1 Kali Exclusive <3>

:: 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 ::
```

Analisa : Perintah -fs pada Fuzzing URL digunakan untuk menemukan size selain 1987.

- Mencoba url /assets pada browser dan hasilnya seperti pada gambar.

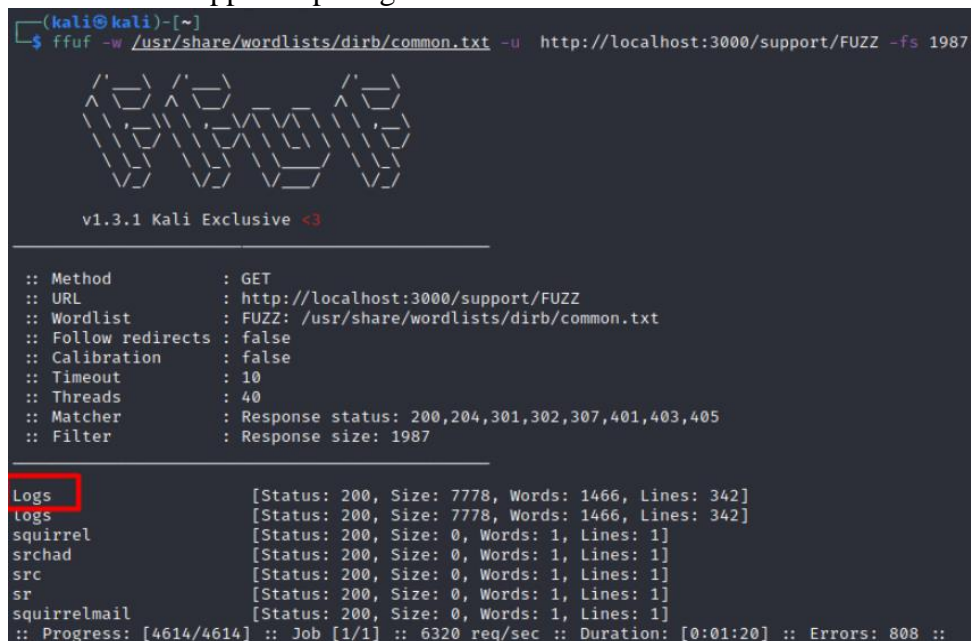


- Kemudian mencoba url yang kedua yaitu /ftp



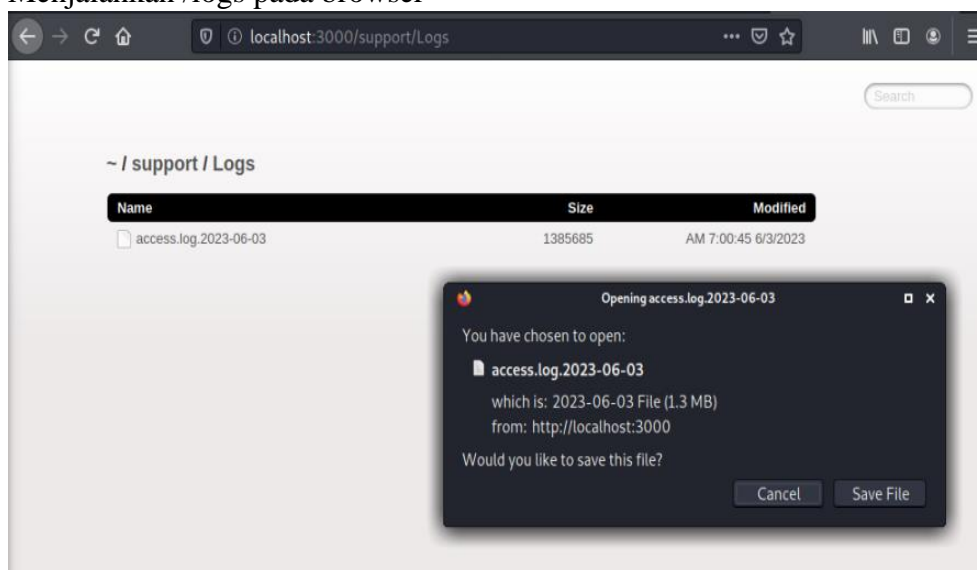
Analisa : didapatkan beberapa file, pada file tersebut salah satu yang dapat mendapatkan informasi lebih detail adalah file support.

- Mencari file /support seperti gambar dibawah



Analisa : Pada hasil pertama didapatkan string “Logs”.

- Menjalankan /logs pada browser




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

1::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/-
ZyDB3wqJ5WNxloMrj10AZBhrTgiVSW5fZoH47U9DAPK9EzRX4Q7n8pv6bmV 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&st=0Y0tGEK
HTTP/1.1" 200 - "http://localhost:3000/score-board" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/-
```

Analisa : pada file yang telah didownload berisi file yang sangat rahasia dan penting karena memberikan informasi tentang aktivitas akses ke sistem.

- Kembali pada aplikasi juice shop, dan didapatkan alert berhasil menyelesaikan access log.

