

# **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, mengeskalsi, 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.

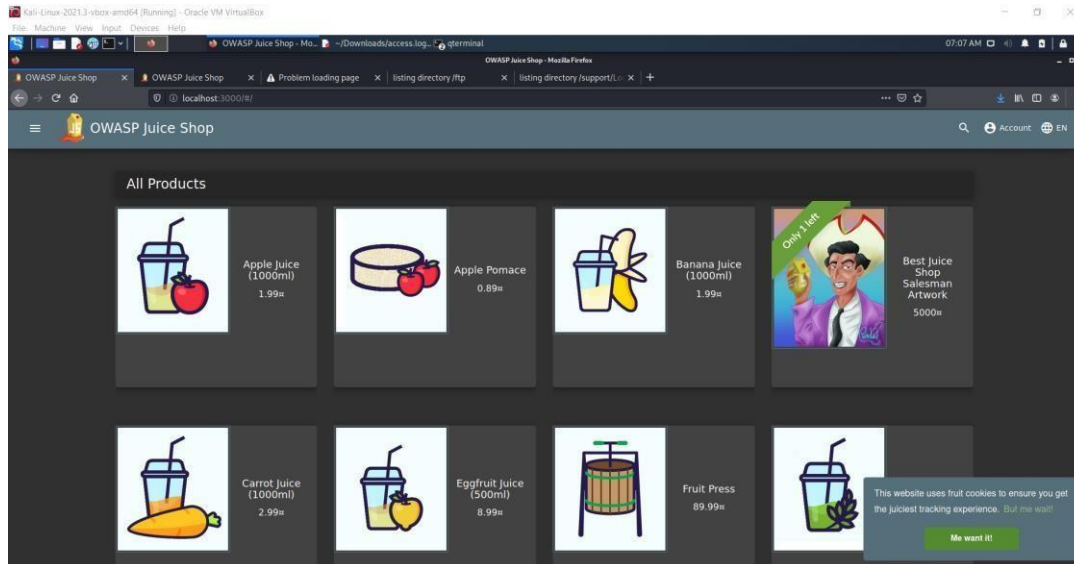
Dalam percobaan kali ini, kali mencoba 2 percobaan yaitu :

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).

## Percobaan

Pada percobaan ini akan menunjukkan mendownload file access log.

### 1. Buka Aplikasi Juice Shop.



### 2. Menggunakan FFUF.

```
Kali-Linux-2021.3-vm-amd64 [Running] - Oracle VM VirtualBox
OWASP Juice Shop - Mozilla Firefox
localhost:3000/

OWASP Juice Shop
All Products
Apple Juice (1000ml) 1.99€
Apple Pomace 0.89€
Banana Juice (1000ml) 1.99€
Carrot Juice (1000ml) 2.99€
Eggfruit Juice (500ml) 8.99€
Fruit Press 89.99€
Best Juice Shop Salesman Artwork 5000€
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait! Me want it!

Kali-Linux-2021.3-vm-amd64 [Running] - Oracle VM VirtualBox
OWASP Juice Shop - Mozilla Firefox
~/Downloads/access.log

File Actions Edit View Help
[kali@kali]~$ ffuf
ffuf: Fuzz Faster U Fool - v1.3.1 Kali Exclusive C3
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 C3

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
-i ignore-body Do not fetch the response content. (default: false)
-r Follow redirects (default: false)
-s Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in it. (default: false)
-R recursion-depth Maximum recursion depth. (default: 0)
-rs recursion-strategy Recursion strategy: "default" for a redirect based, and "greedy" to recurse on all matches (default: default)
-rp replay-proxy Replay matched requests using this proxy.
-t HTTP request timeout in seconds. (default: 10)
-u Target URL
-x Proxy URL (SOCKS5 or HTTP). For example: http://127.0.0.1:8080 or socks://127.0.0.1:8080

GENERAL OPTIONS:
-v Show version information. (default: false)
-ac Automatically calibrate filtering options (default: false)
-c Custom auto-calibration string. Can be used multiple times. Implies -ac
-cs Colorize output. (default: false)
-cf Load configuration from a file
-mx Maximum running time in seconds for entire process. (default: 0)
-mt Maximum running time in seconds per job. (default: 0)
-ni Disable the interactive console functionality (default: false)
-p Seconds of "delay" between requests, or a range of random delay. For example "0.1" or "0.1-2.8"
-r 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 > 92% 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 results. (default: false)

MATCHER OPTIONS:
-mc Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,307,401,403,405)
-ml Match amount of lines in response
-mr Match regex
-ms Match HTTP response size
-mw Match amount of words in response
```

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 :

### 3. Menjalankan perintah FFUF untuk fuzzing URL

```

kali@kali:~$ FFUF -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ
  1 x
  1
  2
  3
  4
  5
  6
  7
  8
  9
  10
  11
  12
  13
  14
  15
  16
  17
  18
  19
  20
  21
  22
  23
  24
  25
  26
  27
  28
  29
  30
  31
  32
  33
  34
  35
  36
  37
  38
  39
  40
  41
  42
  43
  44
  45
  46
  47
  48
  49
  50
  51
  52
  53
  54
  55
  56
  57
  58
  59
  60
  61
  62
  63
  64
  65
  66
  67
  68
  69
  70
  71
  72
  73
  74
  75
  76
  77
  78
  79
  80
  81
  82
  83
  84
  85
  86
  87
  88
  89
  90
  91
  92
  93
  94
  95
  96
  97
  98
  99
  100
  101
  102
  103
  104
  105
  106
  107
  108
  109
  110
  111
  112
  113
  114
  115
  116
  117
  118
  119
  120
  121
  122
  123
  124
  125
  126
  127
  128
  129
  130
  131
  132
  133
  134
  135
  136
  137
  138
  139
  140
  141
  142
  143
  144
  145
  146
  147
  148
  149
  150
  151
  152
  153
  154
  155
  156
  157
  158
  159
  160
  161
  162
  163
  164
  165
  166
  167
  168
  169
  170
  171
  172
  173
  174
  175
  176
  177
  178
  179
  180
  181
  182
  183
  184
  185
  186
  187
  188
  189
  190
  191
  192
  193
  194
  195
  196
  197
  198
  199
  200
  201
  202
  203
  204
  205
  206
  207
  208
  209
  210
  211
  212
  213
  214
  215
  216
  217
  218
  219
  220
  221
  222
  223
  224
  225
  226
  227
  228
  229
  230
  231
  232
  233
  234
  235
  236
  237
  238
  239
  240
  241
  242
  243
  244
  245
  246
  247
  248
  249
  250
  251
  252
  253
  254
  255
  256
  257
  258
  259
  260
  261
  262
  263
  264
  265
  266
  267
  268
  269
  270
  271
  272
  273
  274
  275
  276
  277
  278
  279
  280
  281
  282
  283
  284
  285
  286
  287
  288
  289
  290
  291
  292
  293
  294
  295
  296
  297
  298
  299
  300
  301
  302
  303
  304
  305
  306
  307
  308
  309
  310
  311
  312
  313
  314
  315
  316
  317
  318
  319
  320
  321
  322
  323
  324
  325
  326
  327
  328
  329
  330
  331
  332
  333
  334
  335
  336
  337
  338
  339
  340
  341
  342
  343
  344
  345
  346
  347
  348
  349
  350
  351
  352
  353
  354
  355
  356
  357
  358
  359
  360
  361
  362
  363
  364
  365
  366
  367
  368
  369
  370
  371
  372
  373
  374
  375
  376
  377
  378
  379
  380
  381
  382
  383
  384
  385
  386
  387
  388
  389
  390
  391
  392
  393
  394
  395
  396
  397
  398
  399
  400
  401
  402
  403
  404
  405
  406
  407
  408
  409
  410
  411
  412
  413
  414
  415
  416
  417
  418
  419
  420
  421
  422
  423
  424
  425
  426
  427
  428
  429
  430
  431
  432
  433
  434
  435
  436
  437
  438
  439
  440
  441
  442
  443
  444
  445
  446
  447
  448
  449
  450
  451
  452
  453
  454
  455
  456
  457
  458
  459
  460
  461
  462
  463
  464
  465
  466
  467
  468
  469
  470
  471
  472
  473
  474
  475
  476
  477
  478
  479
  480
  481
  482
  483
  484
  485
  486
  487
  488
  489
  490
  491
  492
  493
  494
  495
  496
  497
  498
  499
  500
  501
  502
  503
  504
  505
  506
  507
  508
  509
  510
  511
  512
  513
  514
  515
  516
  517
  518
  519
  520
  521
  522
  523
  524
  525
  526
  527
  528
  529
  530
  531
  532
  533
  534
  535
  536
  537
  538
  539
  540
  541
  542
  543
  544
  545
  546
  547
  548
  549
  550
  551
  552
  553
  554
  555
  556
  557
  558
  559
  560
  561
  562
  563
  564
  565
  566
  567
  568
  569
  570
  571
  572
  573
  574
  575
  576
  577
  578
  579
  580
  581
  582
  583
  584
  585
  586
  587
  588
  589
  590
  591
  592
  593
  594
  595
  596
  597
  598
  599
  600
  601
  602
  603
  604
  605
  606
  607
  608
  609
  610
  611
  612
  613
  614
  615
  616
  617
  618
  619
  620
  621
  622
  623
  624
  625
  626
  627
  628
  629
  630
  631
  632
  633
  634
  635
  636
  637
  638
  639
  640
  641
  642
  643
  644
  645
  646
  647
  648
  649
  650
  651
  652
  653
  654
  655
  656
  657
  658
  659
  660
  661
  662
  663
  664
  665
  666
  667
  668
  669
  670
  671
  672
  673
  674
  675
  676
  677
  678
  679
  680
  681
  682
  683
  684
  685
  686
  687
  688
  689
  690
  691
  692
  693
  69
```

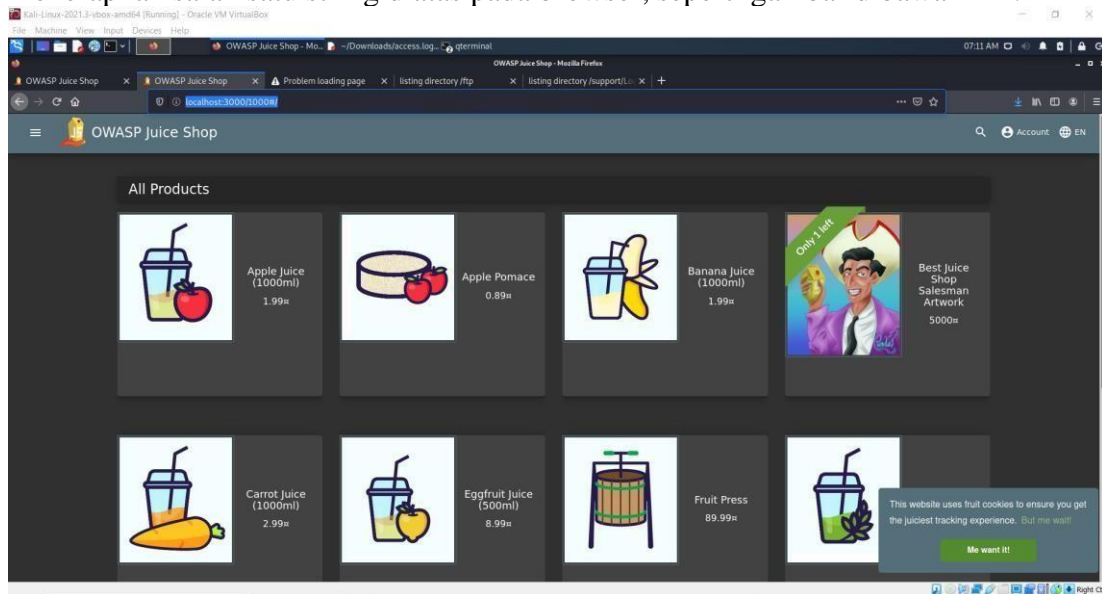
Penjelasan :

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.

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

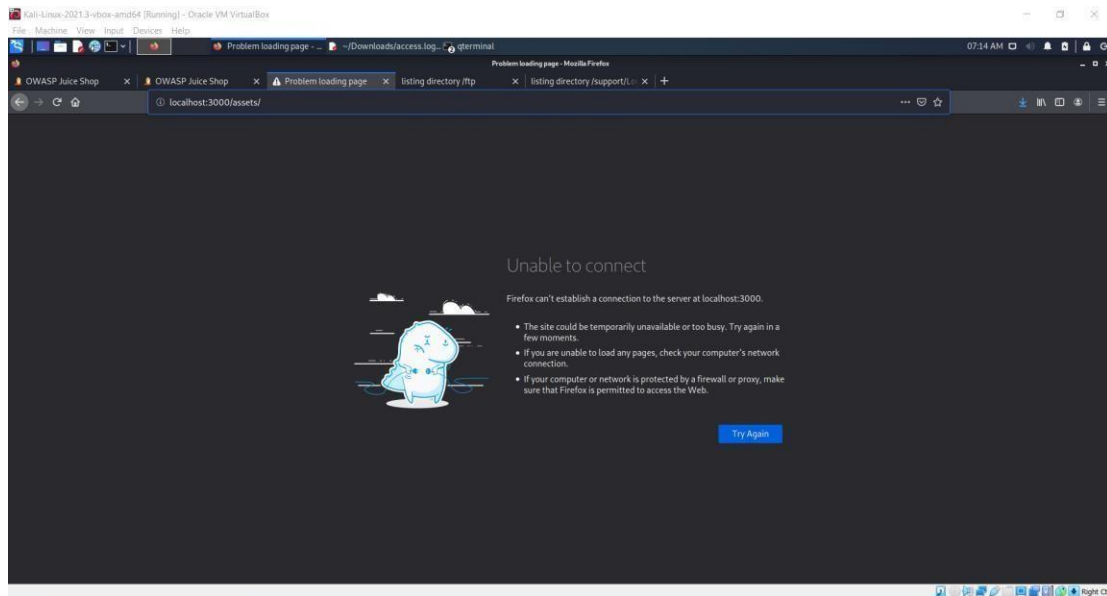
v1.3.1 Kali Exclusive <3>

:: 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

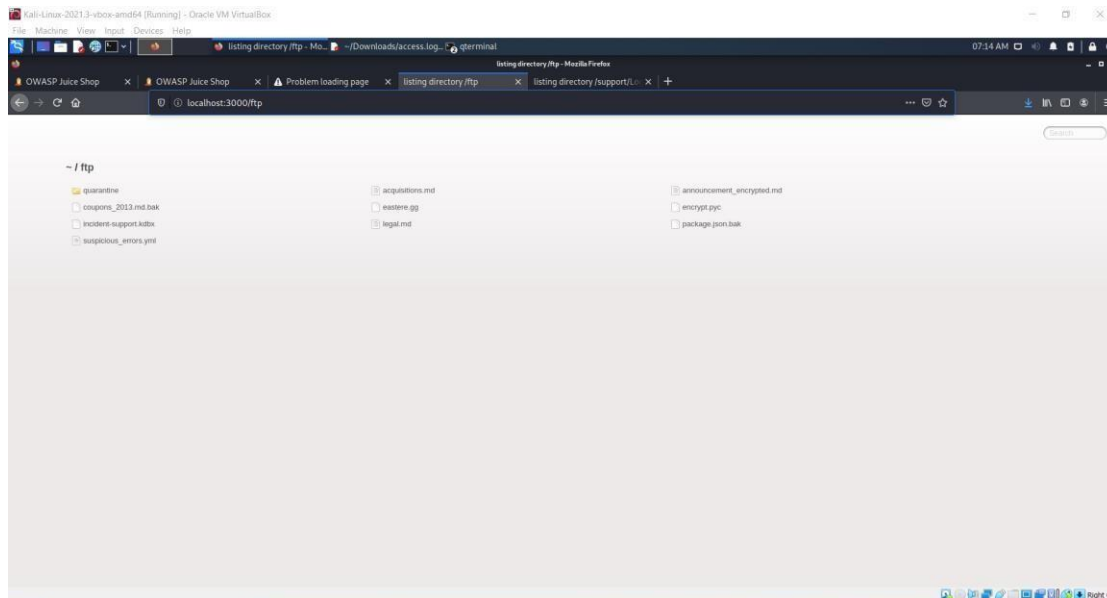
assets      [Status: 301, Size: 179, Words: 7, Lines: 11]
ftp         [Status: 200, Size: 11061, Words: 1568, Lines: 357]
promotion   [Status: 200, Size: 6586, Words: 560, Lines: 177]
robots.txt  [Status: 200, Size: 28, Words: 3, Lines: 2]
snippets    [Status: 200, Size: 683, Words: 1, Lines: 1]
sql-admin   [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.



```
(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 ::
```

The screenshot shows a web browser window with the address bar set to `localhost:3000/support/Logs`. The page displays a directory listing for `~ / support / Logs`. The listing table has three columns: Name, Size, and Modified. One file is listed: `access.log.2023-06-03` with a size of 1385685 and a modified time of AM 7:00:45 6/3/2023. A modal dialog titled "Opening access.log.2023-06-03" is open in the foreground, asking "You have chosen to open:" followed by the file name `access.log.2023-06-03`, which is noted as a 1.3 MB file from `http://localhost:3000`. The dialog asks "Would you like to save this file?" and provides "Cancel" and "Save File" buttons.

Name	Size	Modified
access.log.2023-06-03	1385685	AM 7:00:45 6/3/2023

```
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/-  
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&t=0Y0tGEk  
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.

