LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A09 SECURITY LOGGING AND MONITORING FAILURES

Oleh :

Tarisa Dinda Deliyanti **3122640037**

Fisabili Maghfirona Firdaus **3122640051**

D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

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.

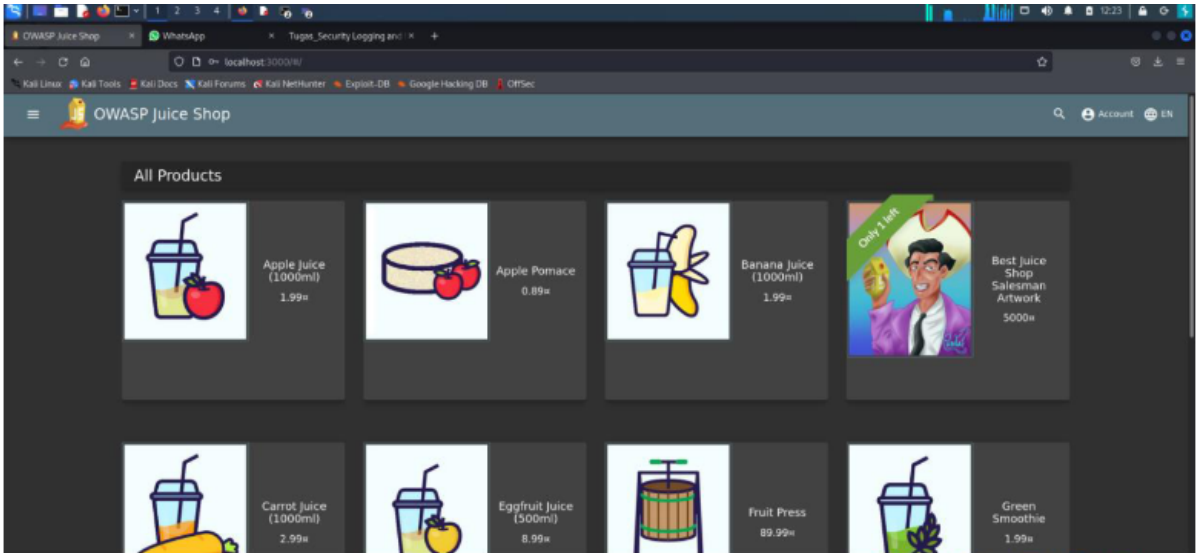
- CWE-778 Insufficient Logging

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.

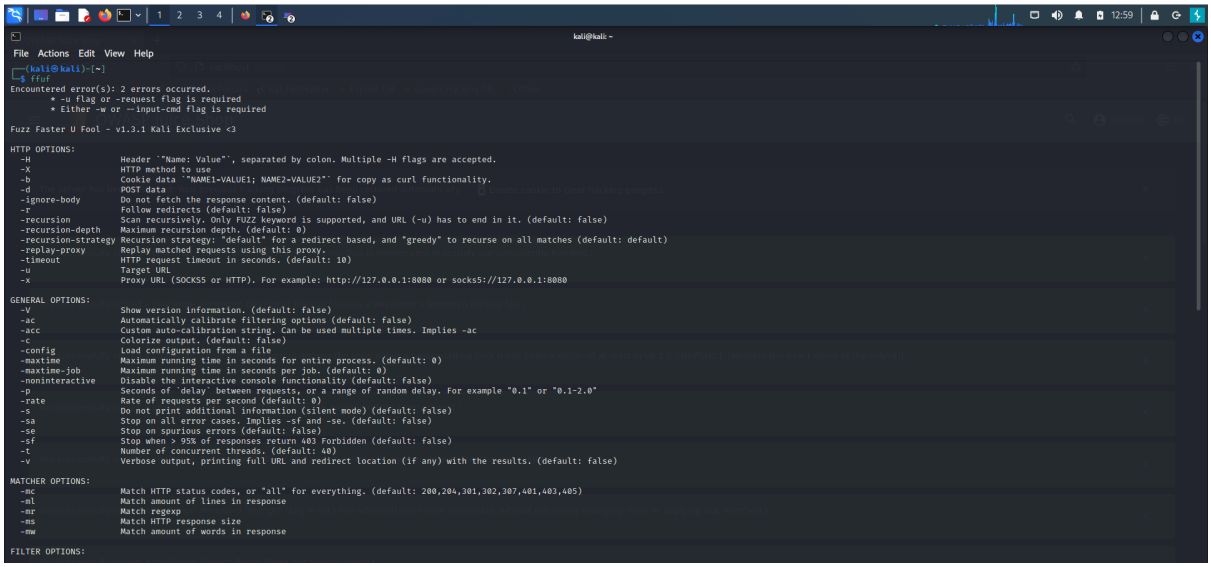
Percobaan

Percobaan dapat dilakukan dengan FFUF untuk melakukan fuzzing pada aplikasi web.

1. Buka Aplikasi Juice Shop.



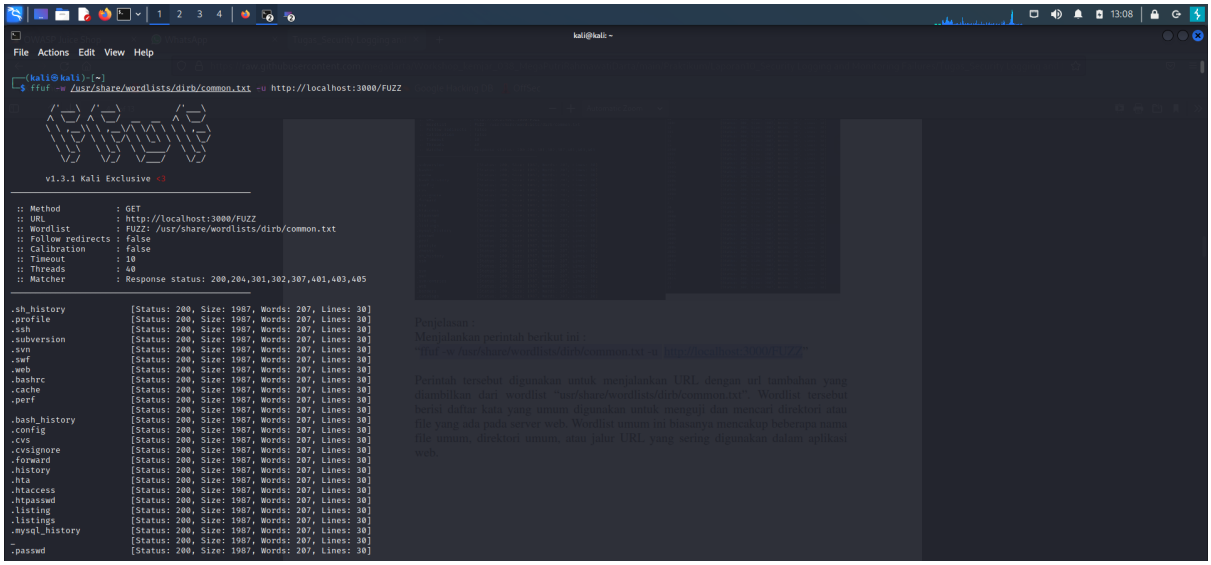
2. Jalankan FFUF



3. Menjalankan perintah berikut ini :

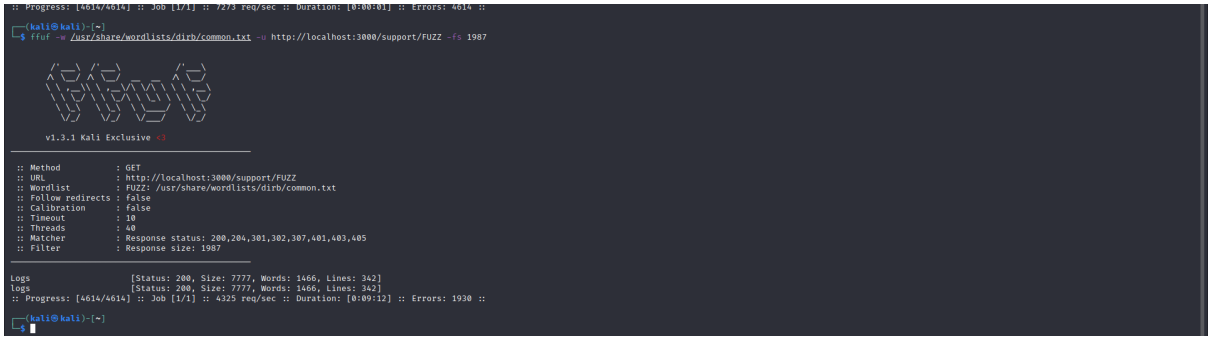
“ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ”

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.

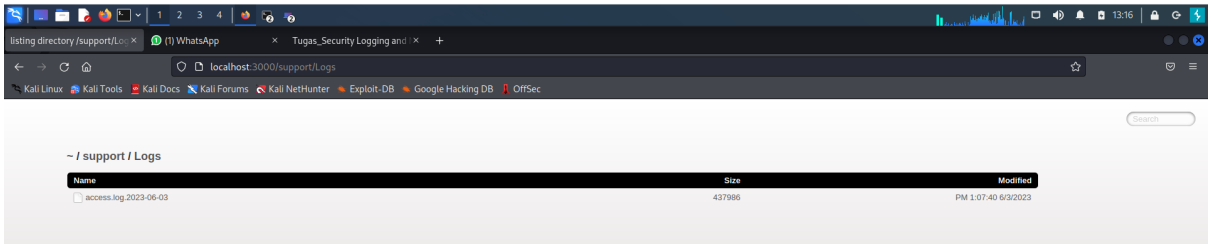


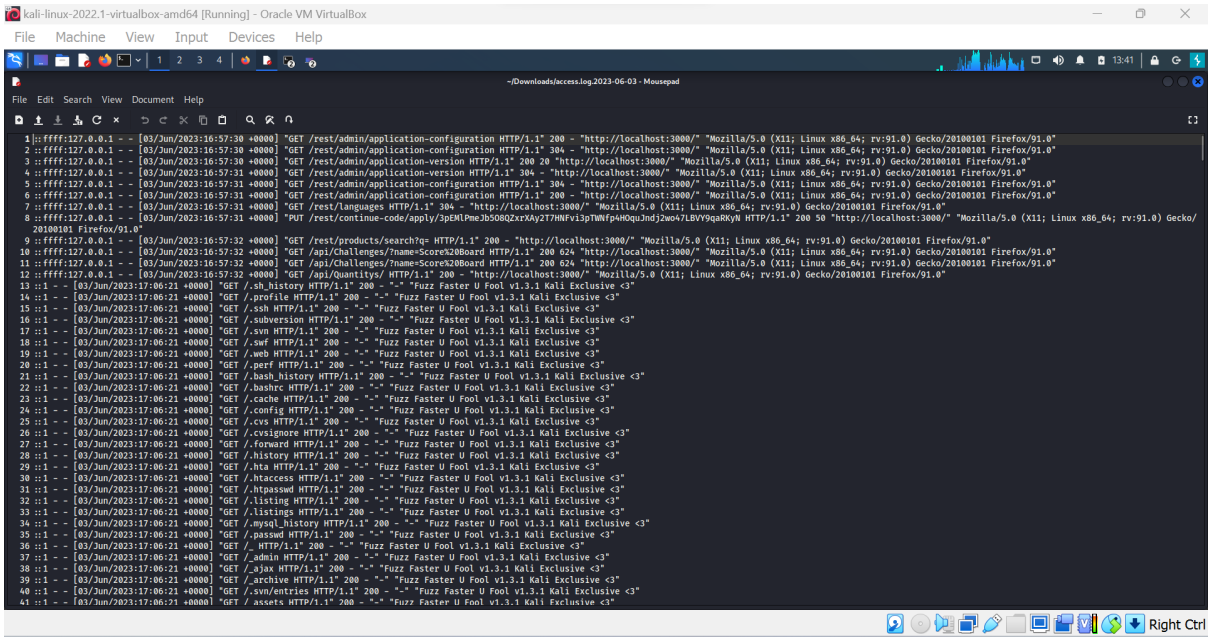
4. Menambahkan perintah

ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/support/FUZZ -fs 1987



5. Mendapatkan file acces log yang bersifat rahasia dari website




kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~/Downloads/access.log.2023-06-03 - Mousepad
File Edit Search View Document Help
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:30 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:30 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:30 +0000] "GET /rest/admin/application-version HTTP/1.1" 200 20 "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:31 +0000] "GET /rest/admin/application-version HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:31 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:31 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:31 +0000] "GET /rest/languages HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:31 +0000] "PUT /rest/continue-code/apply/3pEMlPmeJb508QZxrXAy2T7HNFvi3pTWNFp4HOquJndj2wo47LBVY9qaRKyN HTTP/1.1" 200 50 "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:32 +0000] "GET /rest/products/search?q= HTTP/1.1" 200 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:32 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 624 "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:32 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 624 "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::ffff:127.0.0.1 - - [03/Jun/2023:16:57:32 +0000] "GET /api/Quantitys/ HTTP/1.1" 200 - "http://localhost:3000/" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.sh_history HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.profile HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.ssh HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.subversion HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.svn HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.swf HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.web HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.perf HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.bash_history HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.bashrc HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.cache HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.config HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.cvs HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.cvsignore HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.forward HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.history HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.hta HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.htaccess HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.htpasswd HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.listing HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.listings HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.mysql_history HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.passwd HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /_ HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /_admin HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /_ajax HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /_archive HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /.svn/entries HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
::1 - - [03/Jun/2023:17:06:21 +0000] "GET /_assets HTTP/1.1" 200 - "-" "Fuzz Faster U Fool v1.3.1 Kali Exclusive <3"
Right Ctrl