

PRAKTIKUM 2
CRYPTOGRAPHIC 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. Cryptographic Failures

Cryptographic adalah salah satu teknologi yang digunakan untuk melindungi data dan informasi dari serangan cyber dan tindakan kriminal lainnya. Teknologi ini digunakan untuk memastikan kerahasiaan, integritas, dan otentikasi data, sehingga hanya pihak yang diizinkan yang dapat mengakses atau memodifikasi informasi tersebut.

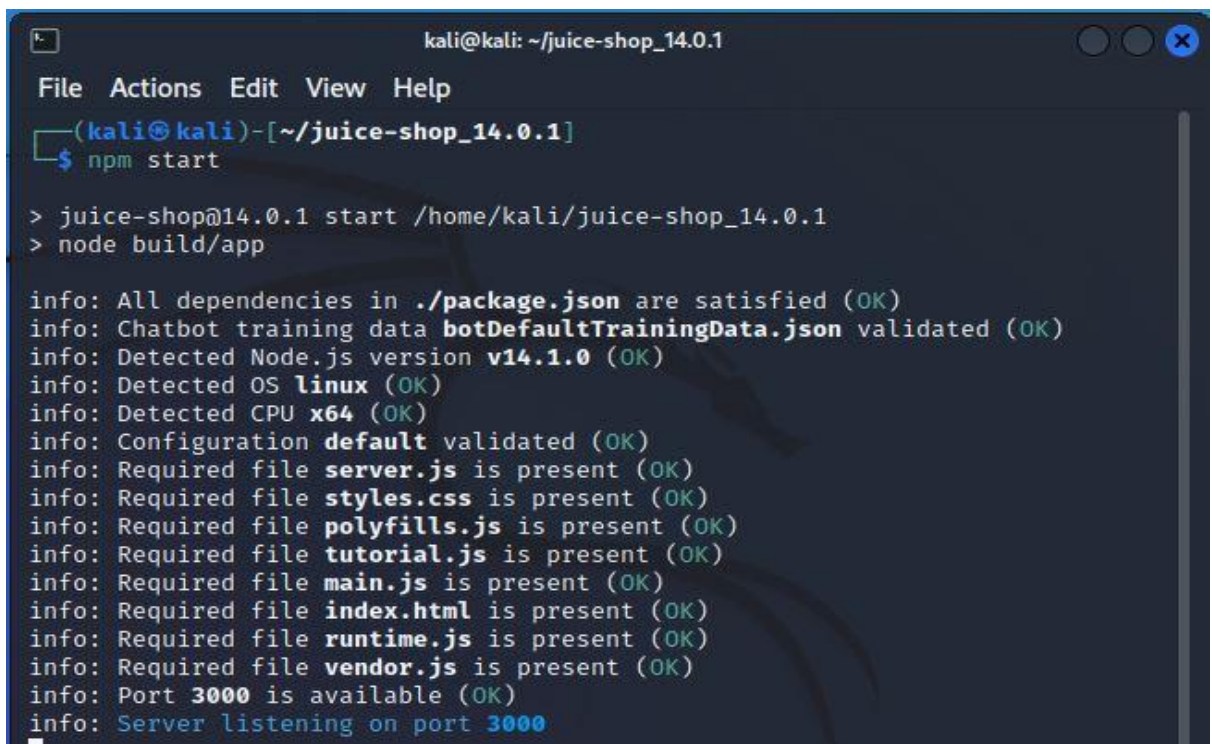
Kriptografi digunakan dalam berbagai aspek keamanan cyber, termasuk enkripsi data yang disimpan atau ditransmisikan melalui jaringan, autentikasi pengguna dan sistem, penggunaan digital signatures untuk memastikan integritas dan otentikasi dokumen dan pesan digital, serta penggunaan protokol keamanan seperti SSL/TLS untuk melindungi komunikasi di jaringan publik.

Namun, seperti halnya teknologi keamanan lainnya, kriptografi juga dapat mengalami kegagalan jika tidak diimplementasikan dengan benar atau terdapat celah keamanan dalam implementasi kriptografi. Oleh karena itu, para ahli keamanan cyber selalu melakukan pengujian dan audit kriptografi secara berkala untuk memastikan bahwa sistem keamanan yang digunakan tetap aman dan terus berkembang seiring dengan berkembangnya ancaman keamanan cyber yang baru dan semakin canggih.

Nested Easter Egg

Easter egg adalah suatu fitur atau pesan tersembunyi dalam sebuah perangkat lunak atau aplikasi. Easter egg dapat berupa berbagai macam hal, seperti animasi, lagu, atau pesan rahasia yang muncul ketika pengguna melakukan suatu tindakan atau memasukkan kode tertentu pada perangkat atau aplikasi yang digunakan.

- Memanggil aplikasi owasp juice shop dengan masuk ke terminal kemudian memasukkan perintah “npm start”

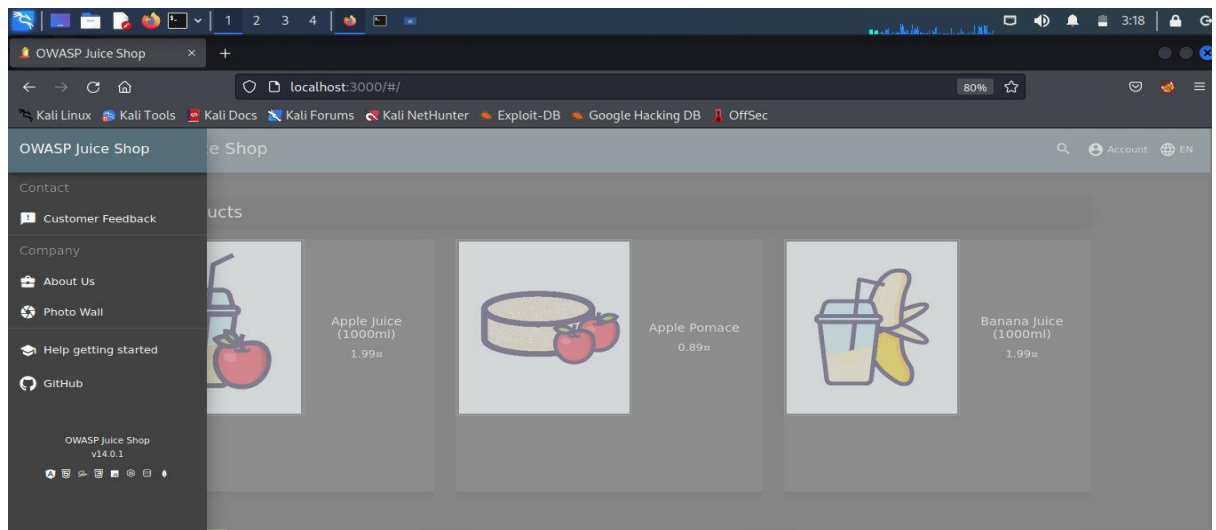


```
kali@kali: ~/juice-shop_14.0.1
File Actions Edit View Help
(kali@kali)-[~/juice-shop_14.0.1]
$ npm start

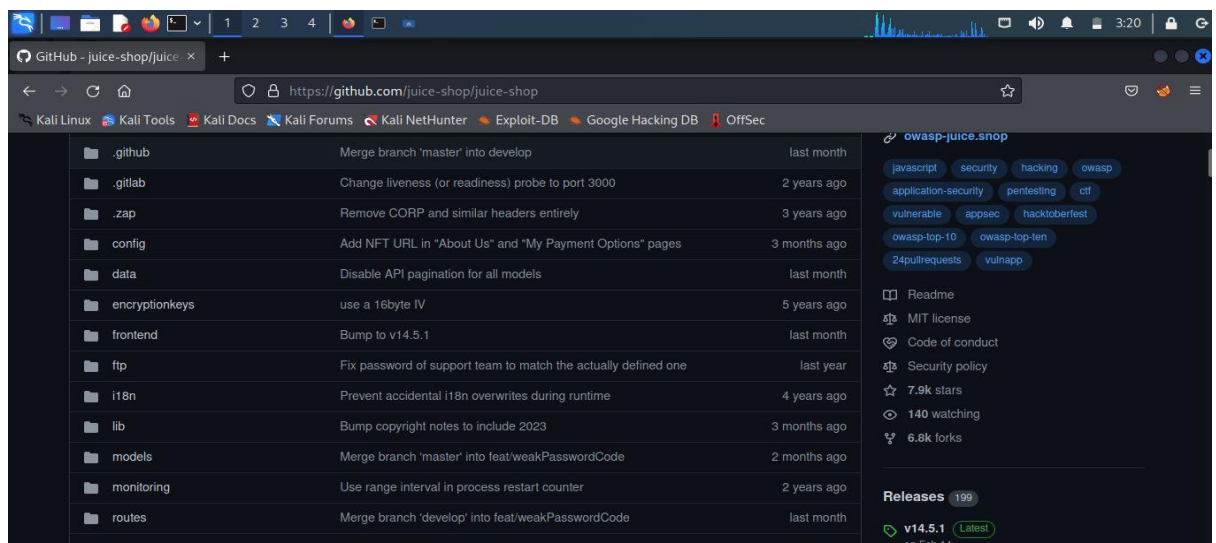
> juice-shop@14.0.1 start /home/kali/juice-shop_14.0.1
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v14.1.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file main.js is present (OK)
info: Required file index.html is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

- Memanggil owasp juice shop dengan alamat “localhost:3000”, kemudian masuk ke direktori ftp dengan klik github.



- Masuk ke folder ftp, kemudian mencari file eastere.gg didalam folder ftp dan membuka file tersebut, terdapat pesan pada file.

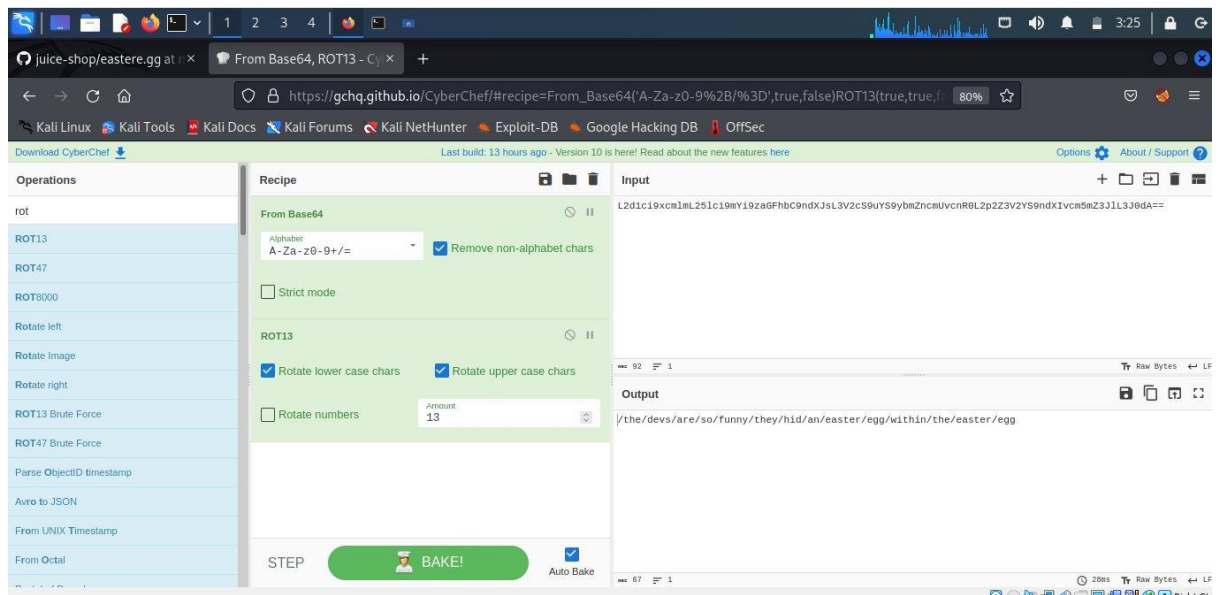


- pada eastere.gg terdapat pesan enkripsi yang dimana pada file tersebut muncul pesan yang memberitahukan bahwa pesan tersebut bukan eastere.gg yang asli dan terdapat kode untuk menemukan eastere.gg. kemudian diharuskan memecahkan kode enkripsi tersebut.

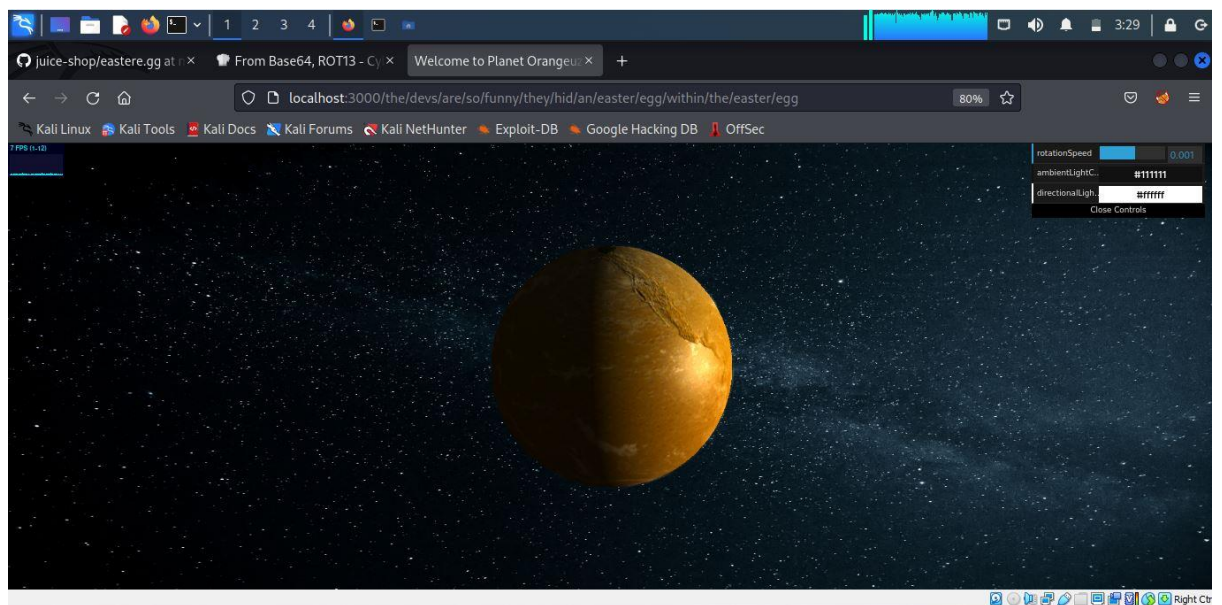
A screenshot of a web browser showing a GitHub repository page for 'juice-shop/eastere.gg'. The browser's address bar shows the URL 'https://github.com/juice-shop/juice-shop/blob/master/ftp/eastere.gg'. The repository page shows a commit by 'bkimminich' with the message 'Move /ftp folder out of /app/public'. The file 'eastere.gg' is displayed with 14 lines of text. The text content is as follows:

```
1 "Congratulations, you found the easter egg!"
2 - The incredibly funny developers
3
4 ...
5
6 ...
7
8 ...
9
10 Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:
11
12 L2d1ci9xcmImL251ci9mY19zaGFhC9ndXJsL3V2cS9uYS9ybWZncmUvcnR0L2p2Z3V2YS9ndXIvcn5mZ3JlL3J0dA==
13
14 Good luck, egg hunter!
```

- Membuka tab baru dan masuk ke Cyber Chef
Cyber Chef adalah sebuah aplikasi web open source yang dapat digunakan untuk melakukan berbagai jenis transformasi data dan manipulasi string. Aplikasi ini dirancang khusus untuk keperluan keamanan informasi dan forensik digital. Cyber Chef dapat digunakan untuk mengubah format file, memecahkan kode, mengekstrak data, mengenkripsi atau mendekripsi data, dan melakukan transformasi data lainnya.
- Copy kode pada eastere.gg, kemudian paste kode di cyber chef.
- Menambahkan base64
Base64 adalah suatu teknik encoding atau pengkodean karakter dalam bentuk ASCII yang sering digunakan dalam aplikasi web dan komunikasi data lainnya. Base64 mengubah data biner menjadi format karakter yang dapat ditransmisikan melalui protokol yang hanya mendukung karakter ASCII. Teknik ini sering digunakan untuk mengirim data biner seperti gambar atau file melalui protokol email atau HTTP.
- Menambahkan ROT13
ROT13 (rotate by 13 places) adalah sebuah metode substitusi sederhana dalam kriptografi yang mengenkripsi suatu pesan dengan menggeser setiap huruf sebanyak 13 posisi dalam alfabet. Setelah 13 posisi digeser, jika suatu huruf melebihi posisi "Z" atau "z", maka akan diulang dari awal alfabet. Contohnya, huruf "A" akan diganti dengan huruf "N", huruf "B" akan diganti dengan huruf "O", dan seterusnya. Oleh karena itu, ROT13 juga dapat dianggap sebagai enkripsi yang sangat lemah, karena mudah untuk mengembalikan pesan yang dienkripsi dengan cara menggeser setiap huruf sebanyak 13 posisi ke arah sebaliknya.
Meskipun ROT13 bukanlah metode enkripsi yang aman, namun kadang-kadang masih digunakan dalam konteks tertentu untuk tujuan tertentu, misalnya untuk mempermainkan tulisan agar tidak mudah dibaca oleh orang yang tidak berwenang atau untuk menghasilkan easter egg pada aplikasi dan game.



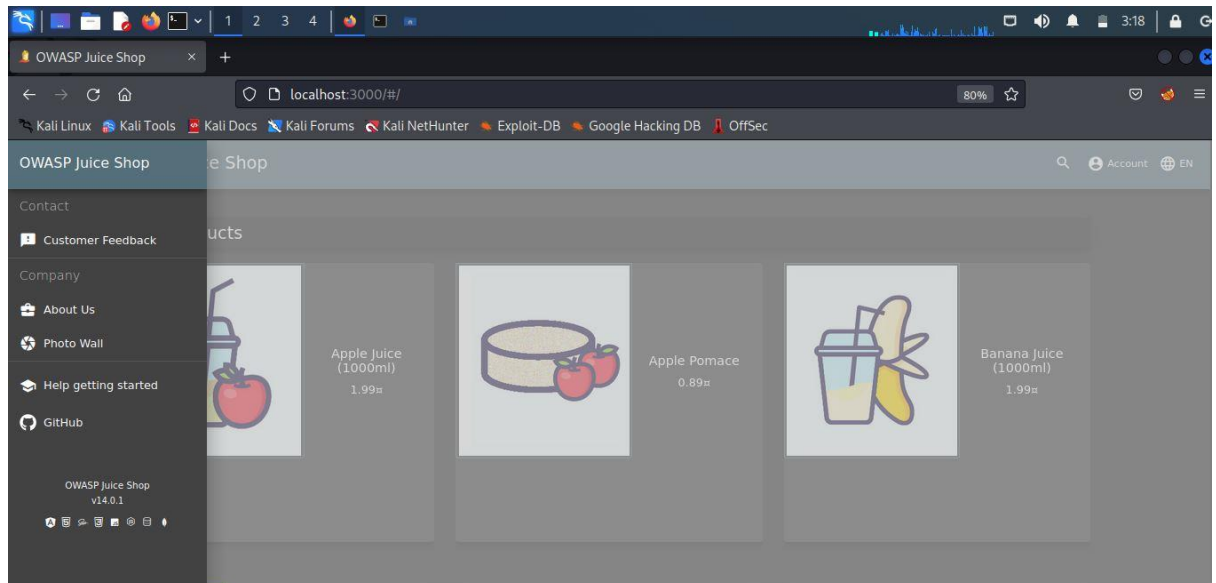
- Copy output pada cyber chef kemudian gabungkan alamat pesan tersembunyi kedalam alamat owasp juice shop. Maka akan muncul hasil seperti pada gambar dibawah.



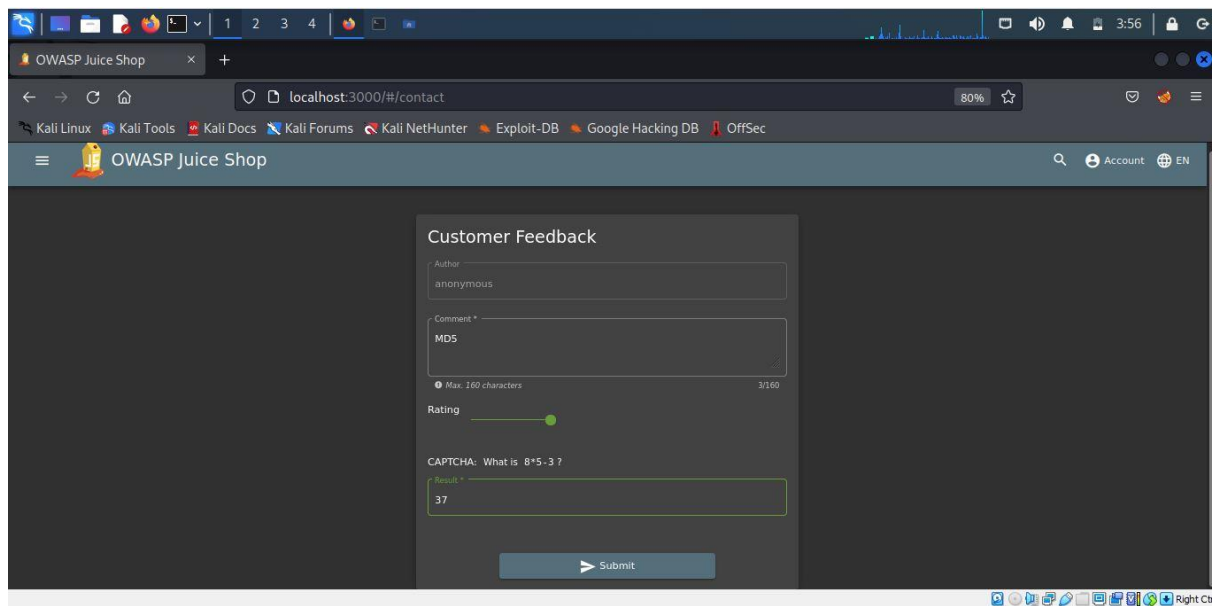
2. Weird Crypto (Cryptographic issue)

Weird Crypto adalah sebuah istilah yang digunakan dalam dunia keamanan informasi untuk menggambarkan suatu masalah keamanan yang terkait dengan penggunaan algoritma kriptografi yang tidak umum atau tidak terdokumentasi dengan baik. Masalah ini muncul ketika para pengembang menggunakan algoritma kriptografi yang kurang dikenal atau terdokumentasi dengan buruk dalam desain sistem keamanan mereka.

- Membuka aplikasi owasp juice shop, kemudian klik Customer feedback pada sidebar menu yang terdapat pada pojok kiri atas.



- Setelah masuk ke menu Customer feedback, masukkan kata MD5 pada comment, mengisi rating dan captcha, kemudian klik submit.
- MD5 (Message-Digest Algorithm 5) adalah algoritma hash kriptografi yang digunakan untuk menghasilkan nilai hash yang mewakili sebuah pesan atau data. Algoritma ini mengambil input berupa pesan dengan panjang variabel dan menghasilkan output berupa nilai hash tetap dengan panjang 128 bit. MD5 awalnya dikembangkan sebagai sebuah alat untuk memverifikasi integritas data, tetapi kemudian digunakan dalam berbagai aplikasi keamanan seperti enkripsi kata sandi dan autentikasi. Meskipun MD5 masih digunakan dalam beberapa konteks, namun algoritma ini telah diketahui memiliki beberapa kelemahan keamanan yang memungkinkan untuk melakukan serangan hash collision dan memalsukan pesan.



- Setelah klik submit akan muncul notifikasi bahwa kita telah menyelesaikan challenge yang diberikan.

