

KEAMANAN JARINGAN

Praktikum Cryptographic Failures



Disusun Oleh :

Choirun Annas 3122640032

Muhammad Dzaky Mahfuzh 3122640050

D4 LJ B

Teknik Informatika

Politeknik Elektronika Negeri Surabaya

Kampus ITS Keputih Sukolilo Surabaya 60111

Telp. 031-5947280, 031-5946114, Fax:031-5946114

Laporan Praktikum

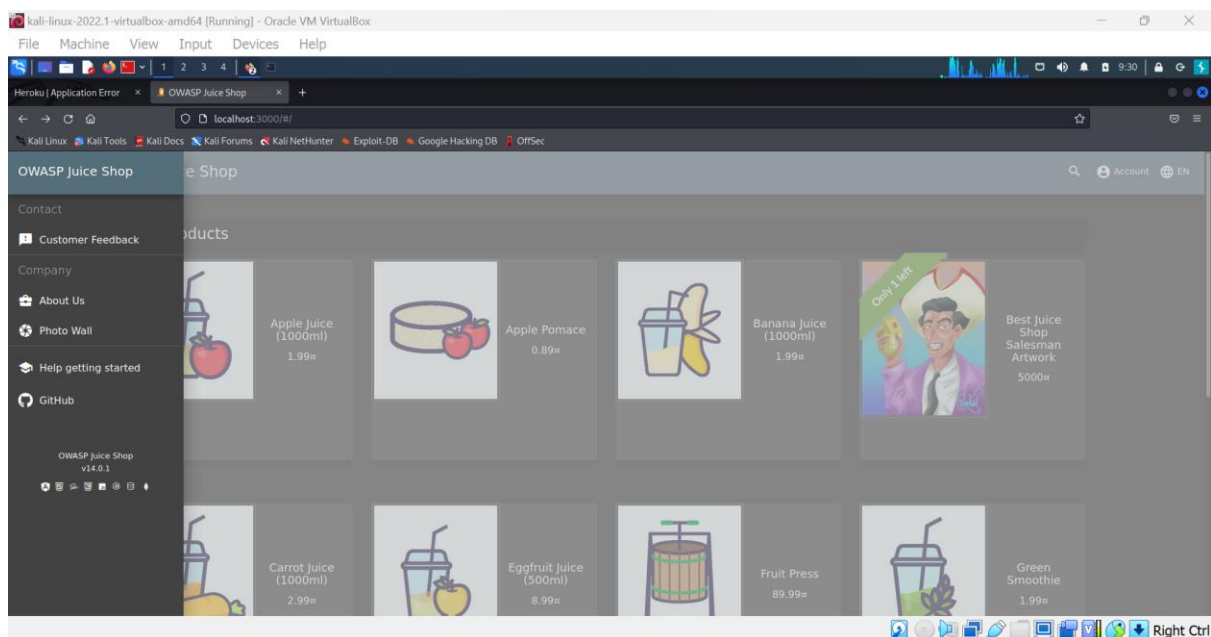
Cryptographic Failures

Kerentanan keamanan aplikasi web kritis yang memaparkan data aplikasi sensitif pada algoritme kriptografi yang lemah atau tidak ada . Itu bisa berupa kata sandi, catatan kesehatan pasien, rahasia bisnis, informasi kartu kredit, alamat email, atau informasi pengguna pribadi lainnya.

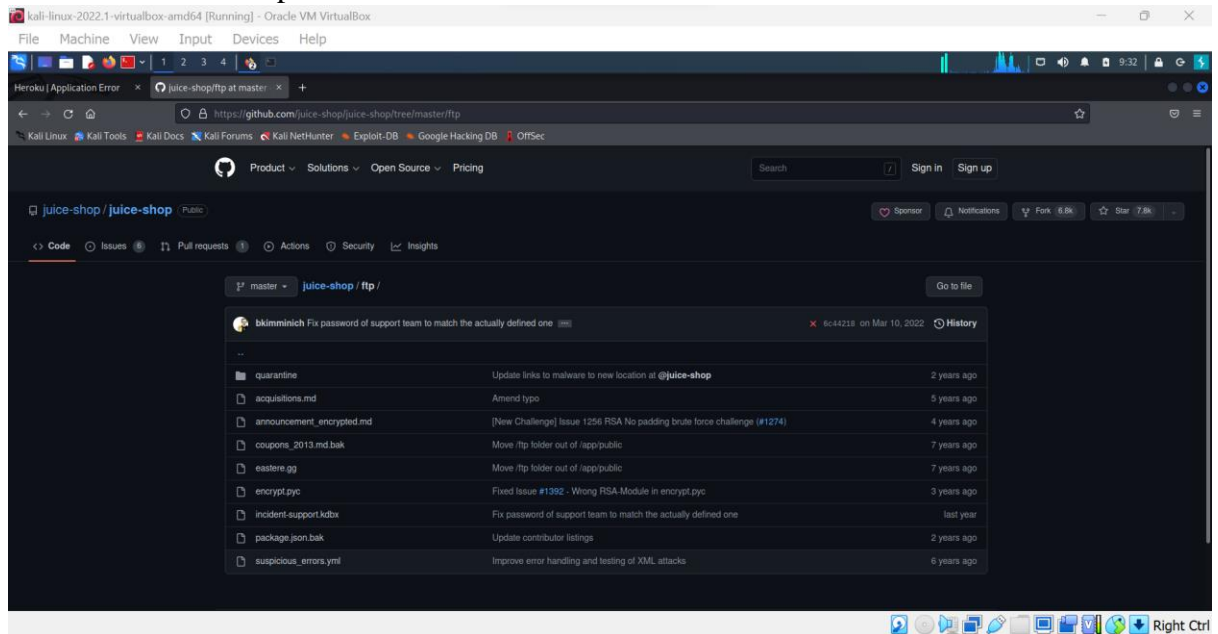
Nested Easter Egg

Easter Egg merupakan pesan tersembunyi yang telah disisipkan kedalam website

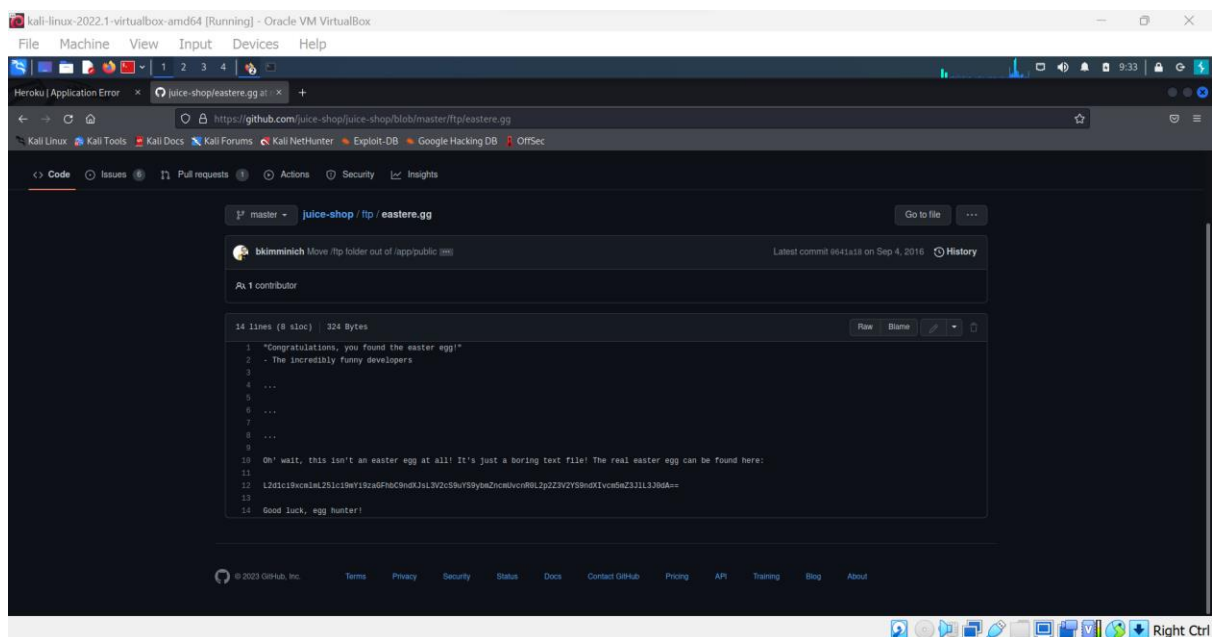
1. Untuk masuk ke direktori ftp klik github



2. Masuk ke folder ftp

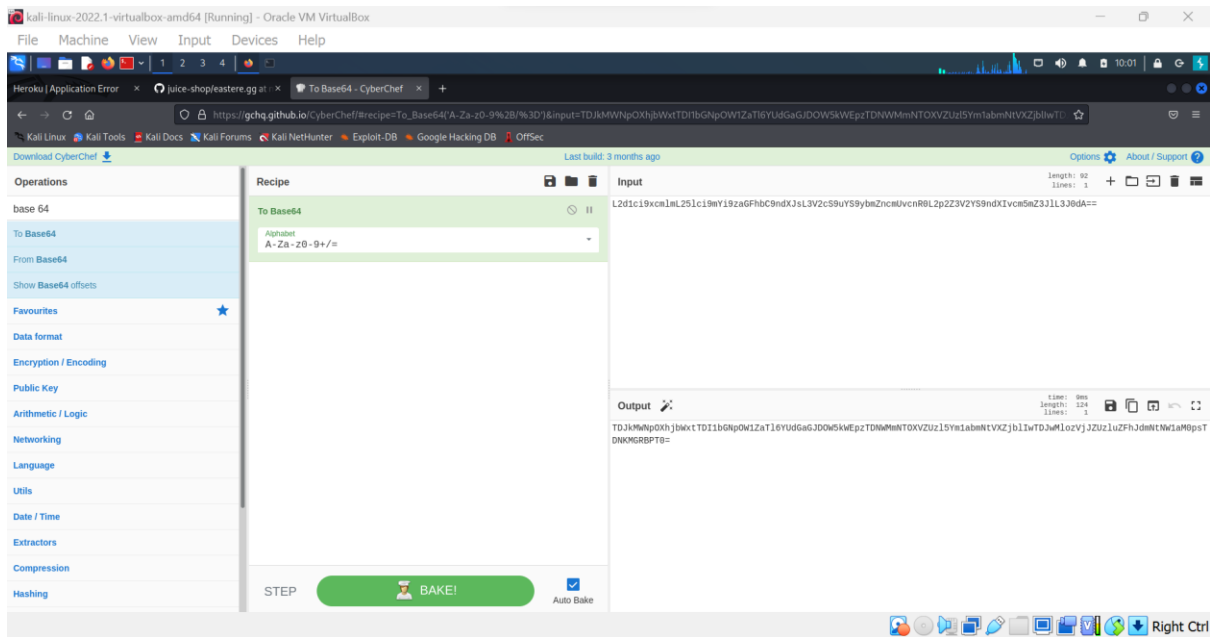


3. Klik file eastere.gg



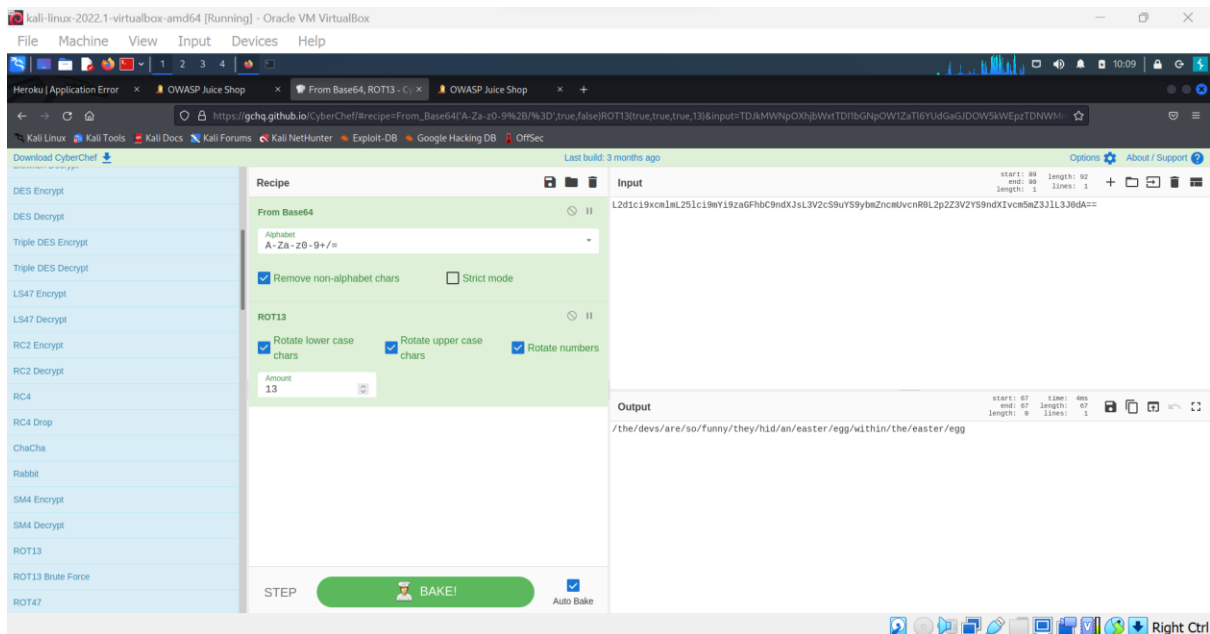
Pada file eastere.gg akan muncul pesan memberitahu bahwa file tersebut bukan eastere.gg yang asli dan ada kode yang ditampilkan untuk menemukan easter egg.

4. Buka Cyber Chef



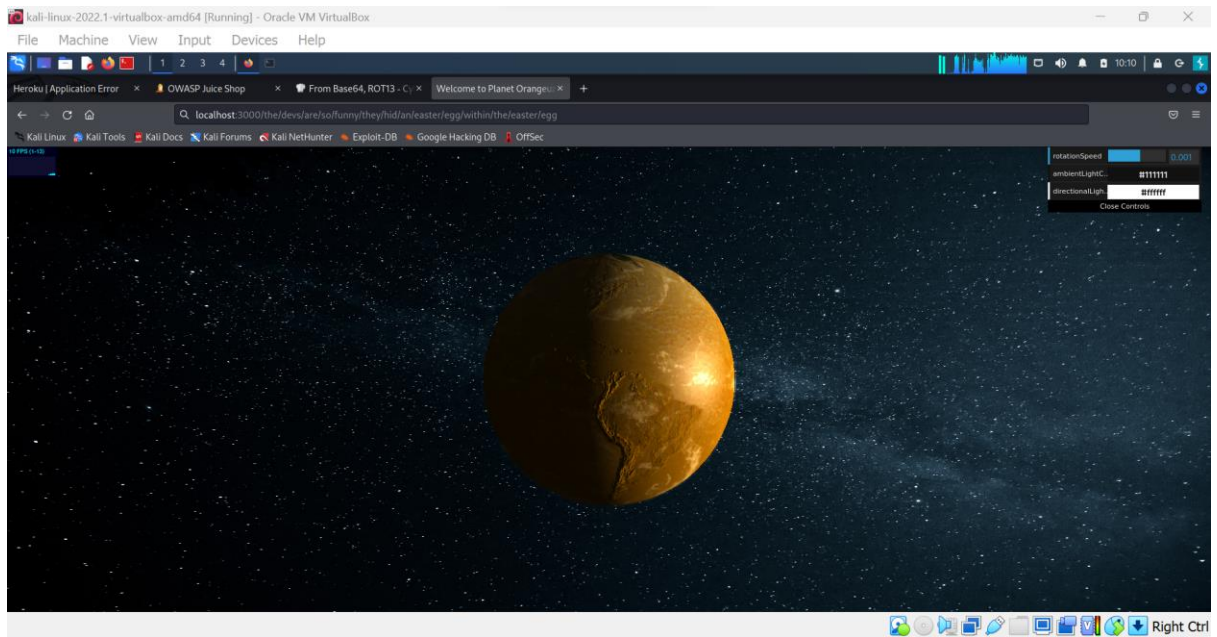
Buka link <https://gchq.github.io/CyberChef/> . Kemudian copy kode dari file eastere.gg ke cyber chef dan drop base 64.

5. Tambah base 64 dan encryption ROT 13



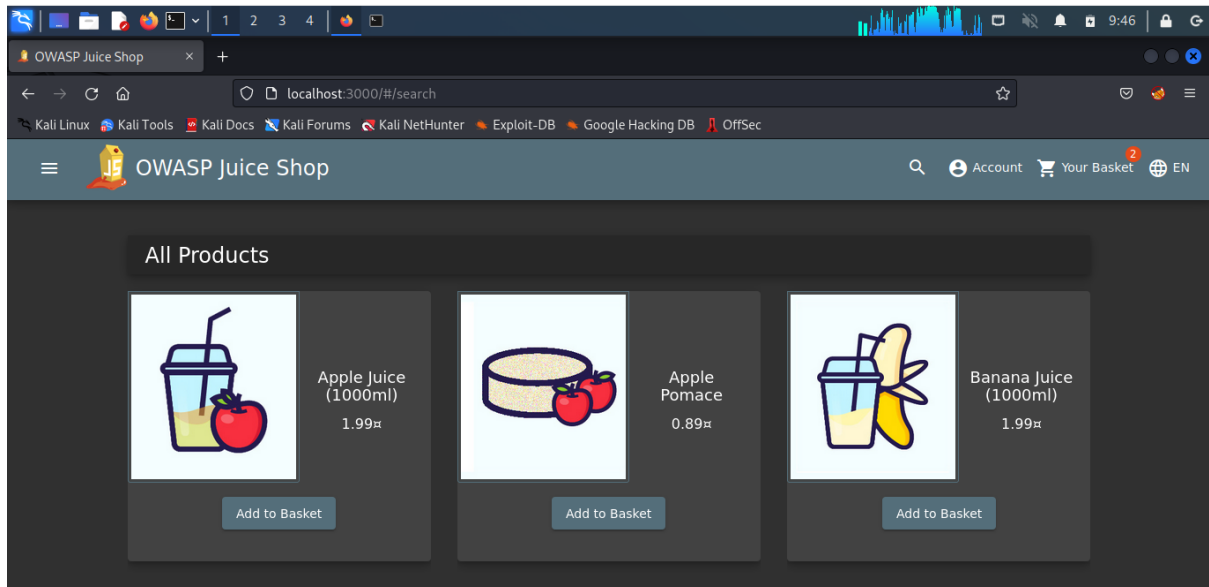
Setelah menambahkan base 64 dan ROT 13 kedalam recipe maka muncul link menuju file tersembunyi.

6. Hasil setelah menggabungkan alamat pesan tersembunyi di alamat juice shop

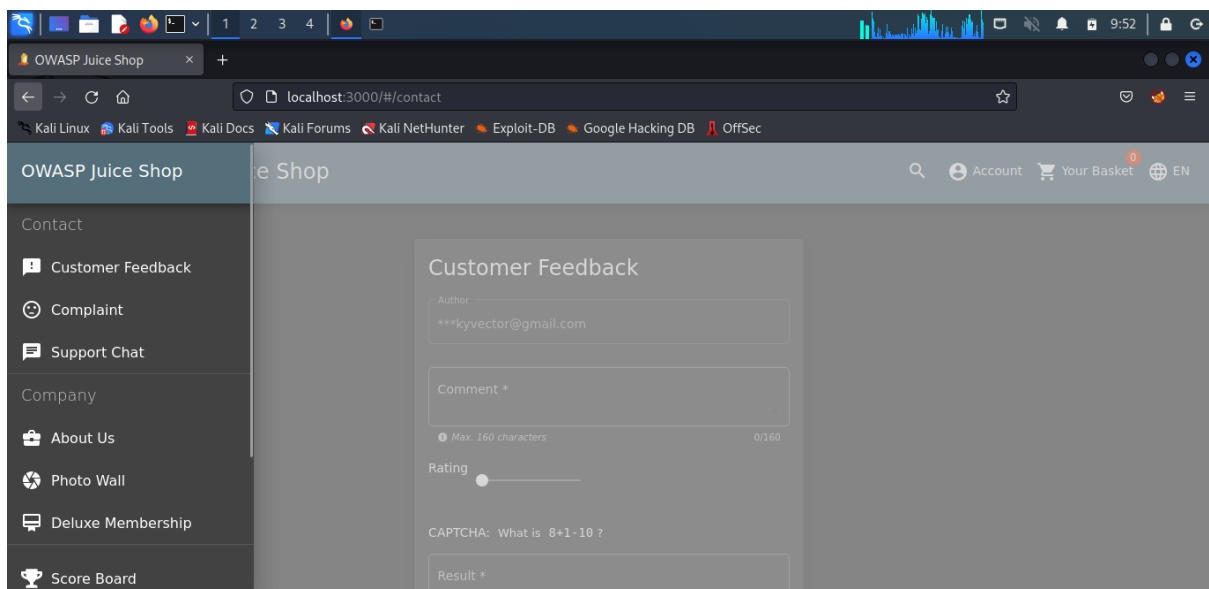


Weird Crypto (Cryptographic Issues)

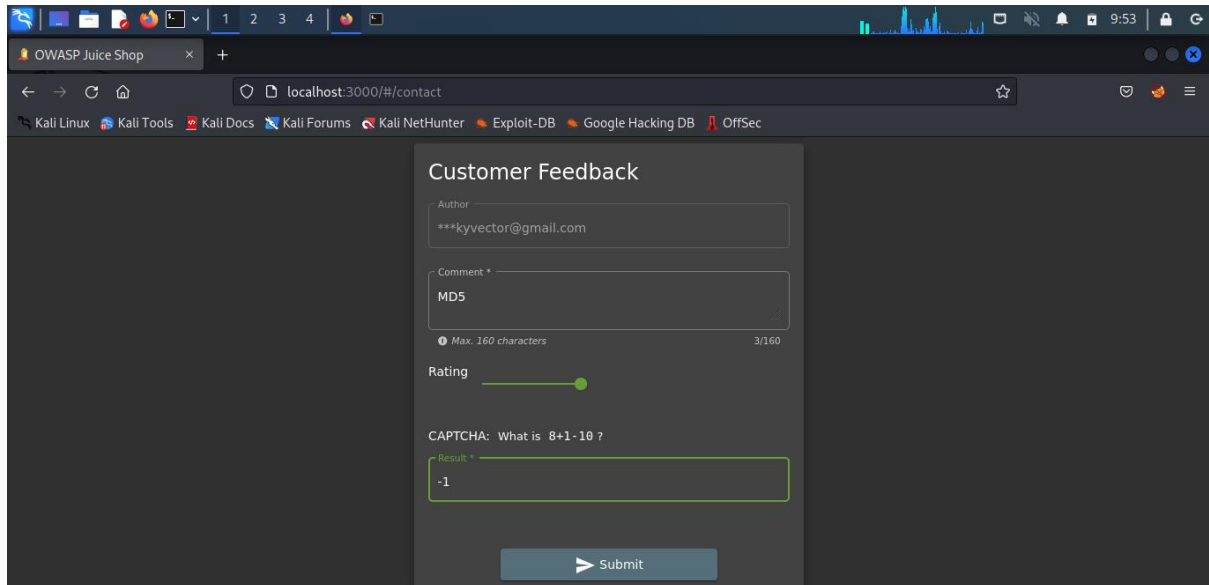
1. buka laman juice-shop terlebih dahulu.



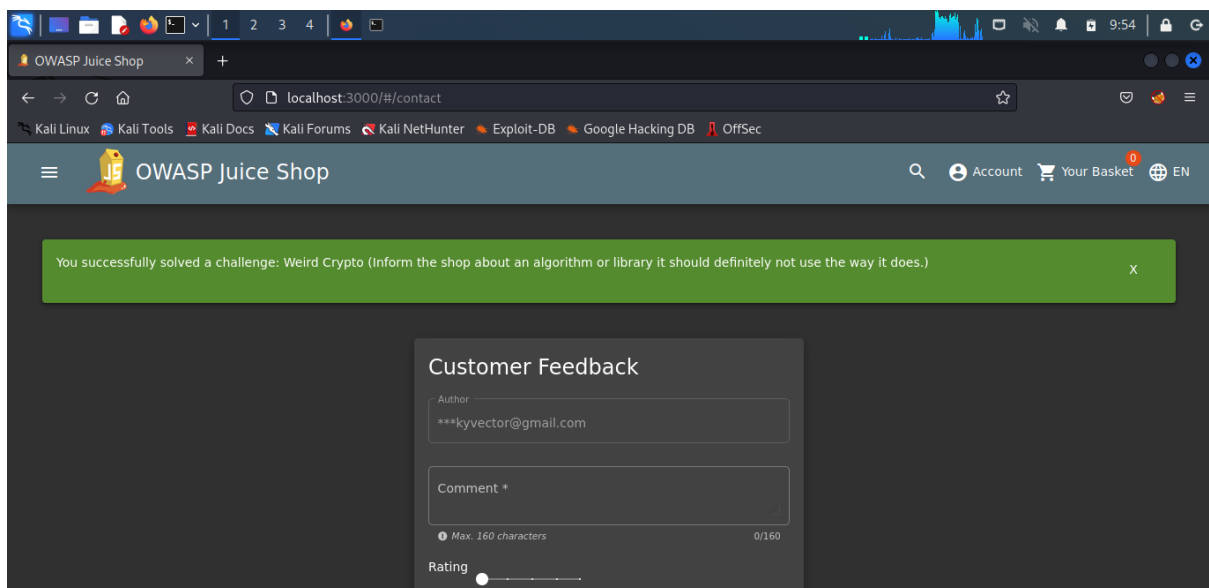
2. klik pada sidebar menu yang ada di pojok kiri atas, lalu pilih menu **Customer Feedback**.



3. lalu pada menu Customer Feedback masukan kata **MD5** pada comment, masukan rating dan chaptcha, dan submit.



4. setelah disubmit maka akan muncul notifikasi bahwa kita telah menyelesaikan challenge yang diberikan.



Analisa :

pada tantangan kali ini, kita ditantang untuk menemukan beberapa *weak cryptographic algorithm* atau algoritma yang lemah namun sering digunakan untuk melakukan kriptografi atau melakukan enkripsi pada data-data krusial, yang seharusnya memiliki privasi dan keamanan lebih. Mengacu pada website <https://pwning.owasp-juice.shop/part2/cryptographic-issues.html> disini kita harus menemukan 5 *weak cryptographic algorithm* yang sering digunakan

- Use the *Contact Us* form to submit a feedback mentioning the abused algorithm or library.
- There are five possible answers and you only need to identify one to solve the challenge.

Setelah mencari dari beberapa artikel terkait, berikut adalah beberapa *weak cryptographic algorithm* yang dianggap sudah tidak layak digunakan namun masih sering digunakan pada berbagai platform,

1. **MD4 / MD5** sangat umum digunakan, terutama dalam mengenkripsi password yang akan disimpan dalam database. Salah satu kelemahan dari MD4 / MD5 ini merupakan **Collision Vulnerability**, dikarenakan berapapun panjang dari sebuah text, maka tetap akan dirubah menjadi 128 bit saja. yang mana dalam skala penyimpanan data yang sangat besar akan ada kemungkinan 2 file yang berbeda akan memiliki nilai hash yang sama, seperti contoh berikut :

```

$ ls -l hello erase
-rwxr-xr-x 1 masecho masecho 4072 Feb 22  2006 erase
-rwxr-xr-x 1 masecho masecho 4072 Feb 22  2006 hello
$ ./erase
This program is evil!!!
Erasing hard drive...1Gb...2Gb... just kidding!
Nothing was erased.

(press enter to quit)
$ ./hello
Hello, world!

(press enter to quit)
$ md5sum erase hello
da5c61e1edc0f18337e46418e48c1290  erase
da5c61e1edc0f18337e46418e48c1290  hello
$ diff hello erase
Binary files hello and erase differ
  
```

File 1:

```

0000000: d131 dd02 c5e6 eec4 693d 9a06 98af f95c .1..
0000010: 2fca b507 1246 7eab 4004 583e b8fb 7f89 /...
0000020: 55ad 3406 09f4 b302 83e4 8883 25f1 415a U.4.
0000030: 0851 25e8 f7cd c99f d91d bdf2 8037 3c5b .Q%.
0000040: d882 3e31 5634 8f5b ae6d acd4 36c9 19c6 ..>1
0000050: dd53 e234 87da 03fd 0239 6306 d248 cda0 .S.4
0000060: e99f 3342 0f57 7ee8 ce54 b670 8028 0d1e ..3B
0000070: c698 21bc b6a8 8393 96f9 65ab 6ff7 2a70 ..!..
  
```

File 2:

```

0000000: d131 dd02 c5e6 eec4 693d 9a06 98af f95c .1..
0000010: 2fca b587 1246 7eab 4004 583e b7fb 7f89 /...
0000020: 55ad 3406 09f4 b302 83e4 8883 2571 415a U.4.
0000030: 0851 25e8 f7cd c99f d91d bdf2 8037 3c5b .Q%.
0000040: d882 3e31 5634 8f5b ae6d acd4 36c9 19c6 ..>1
0000050: dd53 e2b4 87da 03fd 0239 6306 d248 cda0 .S..
0000060: e99f 3342 0f57 7ee8 ce54 b670 80a8 0d1e ..3B
0000070: c698 21bc b6a8 8393 96f9 652b 6ff7 2a70 ..!..
  
```

dan masih ada beberapa kelemahan lagi yang masih berhubungan dengan **collision** sebagai contohnya adalah **Executables File Collision**, **Postscript File Collision**, **SSL Certificate Collision**. dan karna terbatasnya hasil enkripsi hash yang dapat dilakukan semakin memudahkan pihak lain untuk melakukan bruteforce.

sumber : <https://www.ilmuhacking.com/cryptography/md5-itu-berbahaya/>

2. RC4 / RC2,
3. DES / 3DES,
4. Blowfish,
5. SHA-1