Ranjeet Kumar Singh

Follow 103 Followers About

OAuth Misconfiguration | Working of OAuth | Types of vulnerabilities in it and how you can exploit OAuth Misconfigurations To Takeover Accounts

Ranjeet Kumar Singh Jan 22 · 3 min read

Hello Security Researchers, My name is Ranjeet Singh and today I am going to explain what is OAuth, how you can find misconfiguration in it & how you can takeover account and can earn $$$$.Also I am going to share my methodology & some tips / tricks.

WHAT IS OAuth :

It is an authorization framework.

It enables a third party application to obtain limited access to a service.

Example , We have “Login with facebook” buttons on various websites which gets an ‘access token’ of the user from Facebook and uses this limited information form Facebook to create account.

How OAuth works :

1.Authorization Code (Later this exchanged with Access Token to access user own recources)

2.Implicit (The third party app directly gets an access token then this can be used to access resources own by the user)

3.Recource Owner Password Credentials (Third party directly derive an access token by credentials i.e username and password)

4.Client credentials (Application request for access token to use their own recources)

Where OAuth is used ?

>Steal access token of the application and use it to login.

2. Login Request will be something like :
https://facebook.com/v2.3/dialog/oauth?response_type=token&display=popup&client_id=<CLIENT_ID>&redirect_uri=<REDIRECT_URI>&scope=email

METHODOLOGY TO STEAL :

1.Find domain used in ‘ redirect_uri ‘
2.Can you use ‘ subdomains ‘ in the ‘ redirect_uri ‘
3.Point the ‘ redirect_uri ‘ to a page
a>Open redirect(302) to attackers domain
b>Xss which can be used in ‘ redirect_uri ‘ to pass ‘ access_token ‘ to attacker.
c>Subdomain takeover (allowed subdomain in ‘ redirect_uri ‘)
d> Backtrack to a page which can be used to open redirect(302)/XSS

3.Use the stolen ‘ access_token ‘ to login.

2. CODE STEALING :

Main Goal :
>Steal ‘ authorization_code ‘ of the application.
>Use it to login into user’s account to user’s account.

Login Request something like :
https://facebook.com/v2.3/dialog/oauth?response_type=code&display=popup&client_id=<CLIENT_ID>&redirect_uri=<REDIRECT_URI>&scope=email

#Exception :
‘ redirect_uri ‘ while exchanging the ‘ authorization_code ‘ with ‘ access_token ‘ must watch, when we got ‘authorization_code ‘

METHODOLOGY TO STEAL :
1.Find domain used in ‘ redirect_uri ‘

fetching ‘ access_token ‘

4.Poin the ‘ redirect_uri ‘ to a page

>XSS which can be used in ‘ redirect_uri ‘ to pass ‘authorizatoion_code ‘ to attacker.

>Subdomain takeover (allowed subdomain in ‘ redirect_uri ‘)

>Leading user controlled external images, scripts erc (Leaking Refer)

5.Use the stolen ‘ authorization_code ‘ to login.

3. CSRF (MISSING STATE PARAM)

Main Goal :

1.Connect attacker’s {Facbook} account to user’s account.

2.Login via attacker’s {Facebook} account into user’s account.

https://facebook.com/v2.3/dialog/oauth?response_type=code&display=popup&client_id=<Client_id>&reedirect_uri=<Redirect_uri>&scope=email&state=<Some_anti_csrf_token>

METHODOLOGY :

1.Check if ‘ state ‘ param in OAuth Authorization Link is validated.

2.Derive yourself a valid ‘authorization_code’ link and don’t use it.

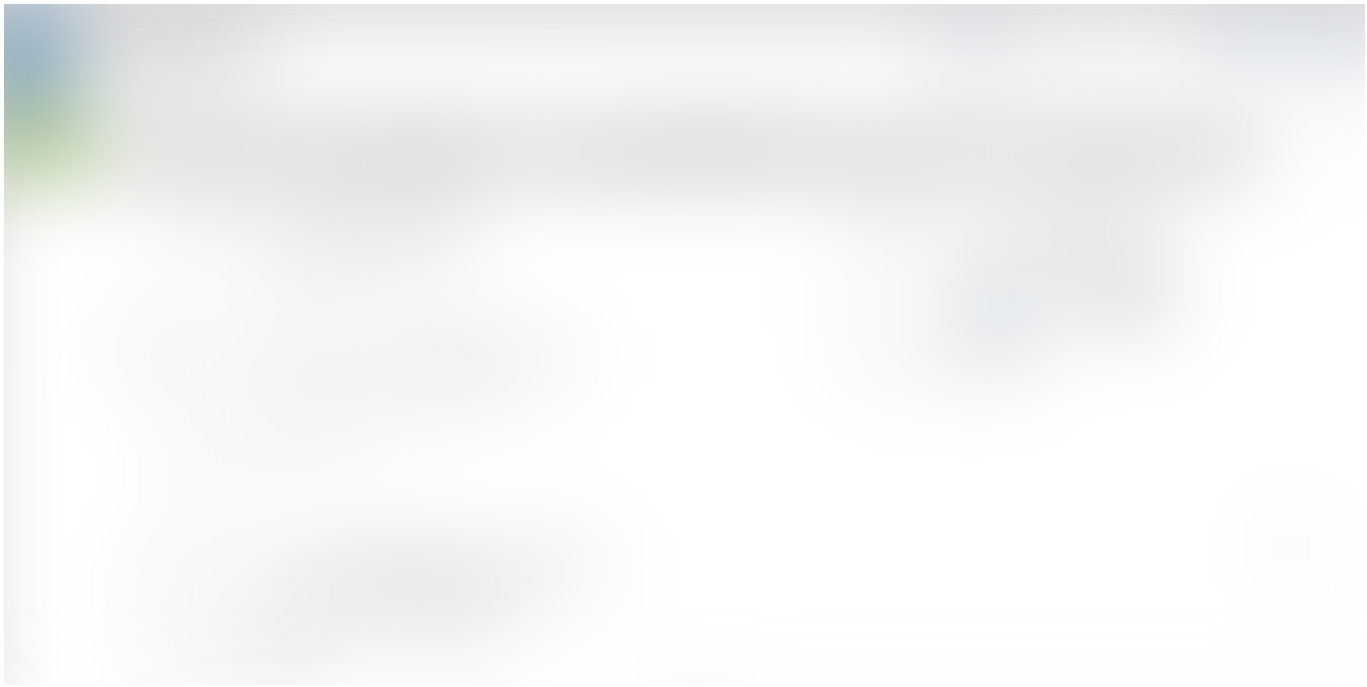
3.Send this active ‘authorization_code’ link to victim

4.Your account will get connected with victim’s account

5.Now login via your own account.

TODAY LEARN & TOMORROW EARN :)

SOME BOUNTY USING THESE METHODOLOGIES :



Hope you have got to know how OAuth works and types of vulnerabilities present here.If you have any doubt or I have done any mistake then please notify me so we can help each other by learning & sharing knowledge:

TWTTER ID : https://twitter.com/geekboyranjeet

Thank you :)

Bug Bounty Bug Bounty Tips Hacking Oauth Ethical Hacking

>SSO

HOPE YOU HAVE GOT AN IDEA HOW OAUTH WORKS !!

TYPES OF ATTACKS :