Developer Tools Bug Hunting Methodology

Become a Successful Bug Bounty Hunter

DEVELOPER TOOLS

- Testing webhooks
- Oauth flows
- GraphQL explorers

DEVELOPER TOOLS

- Where are they hosted?

- If on AWS, try to read AWS keys (SSRF)

- What tools are available to developers?

- Can I test a webhook event?

- Google SSRF webhook

DEVELOPER TOOLS

- Can I see response on any tools?

- If yes, focus on response

- Can I create my own app and do permissions work correctly?

DEVELOPER TOOLS

- When you click No to an action (for example generating an access token), access may still be there!

- Generate an API key in Dev tools

- Check which permissions are allowed by default

- Maybe Oauth states that resources can only be accessed with an API key.

- Is that the case?

DEVELOPER TOOLS

- Press cancel and see what happens. Maybe we can control cancel parameter or returnTo etc.

- After creating app, how does the login flow work?

- When I disconnect the app from my profile, is the token invalidated?

- Are there new return_uri parameters, how do they work?

DEVELOPER TOOLS

- Certain domains may be whitelisted for debugging purposes

- Try theirdomain.com as redirectUri as well as amazonaws.com, .aws.amazon.com, http://localhost/

- Does the wiki/help docs reveal any info on how the API works?

DEVELOPER TOOLS

- Can I upload any files such as app image? If the filtering the same as on account profile?

- Does it use different codebase?

- example.com may not vulnerable

- test developer.example.com

DEVELOPER TOOLS

- Can I create a separate account on dev site or does it share the same session from main domain?

- What does the login process look like?

- Sometimes you can login to developer.example.com via you main session from example.com

DEVELOPER TOOLS

- There might be some token exchange handled by a redirect

- Check the redirect functionality

- Re-enter the process of checking what's reflected and where and if sessions are not shared

- If session not shared - complete new target

Thank You!

Become a Successful
Bug Bounty Hunter