S.S.R.F.

BY UNCLE RAT

Agenda

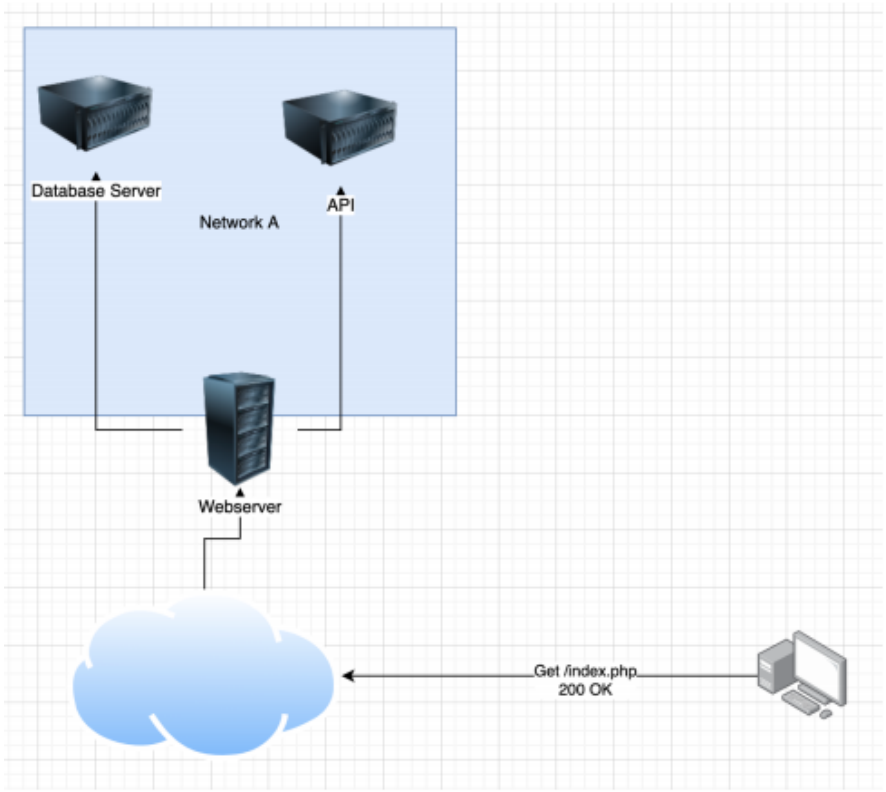
- What is it and how we abuse it?
- Attack strategy
  - Basic SSRF strategy
  - SSRF agaisnt a server itself
  - SSRF against other backened
  - Blind SSRF

What is it and how we abuse it?

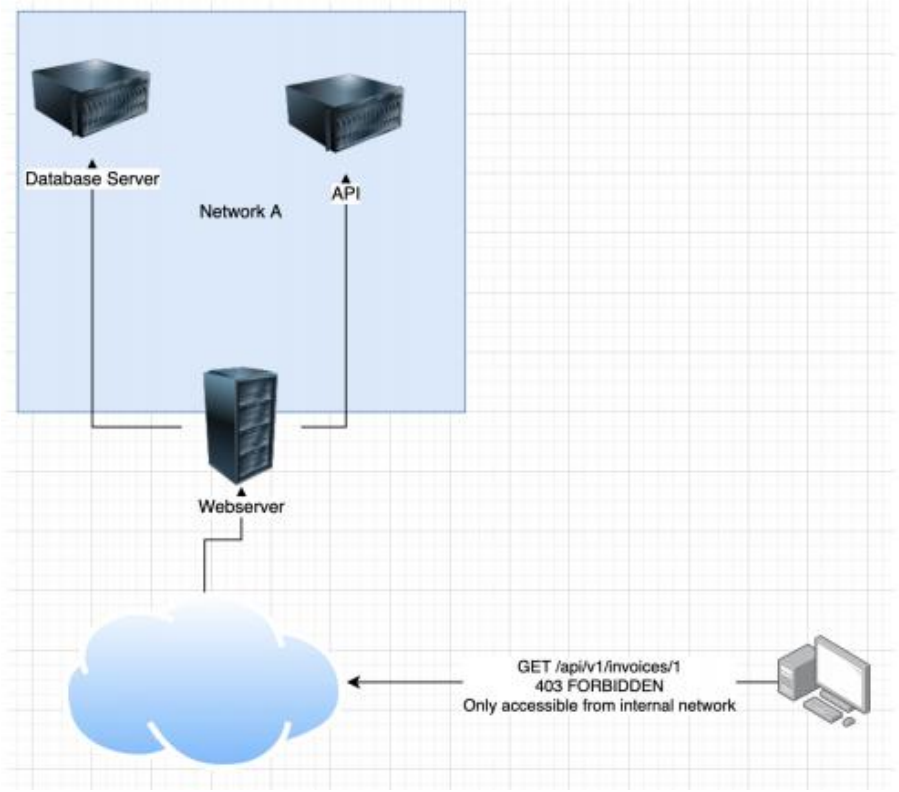
What is it and how we abuse it?

- SSRF - Server Side Request Forgery
  - Server Side Request Forgery can occur in different forms
  - How we normally abuse it?
  - Other ways to abuse it
  - Practical examples

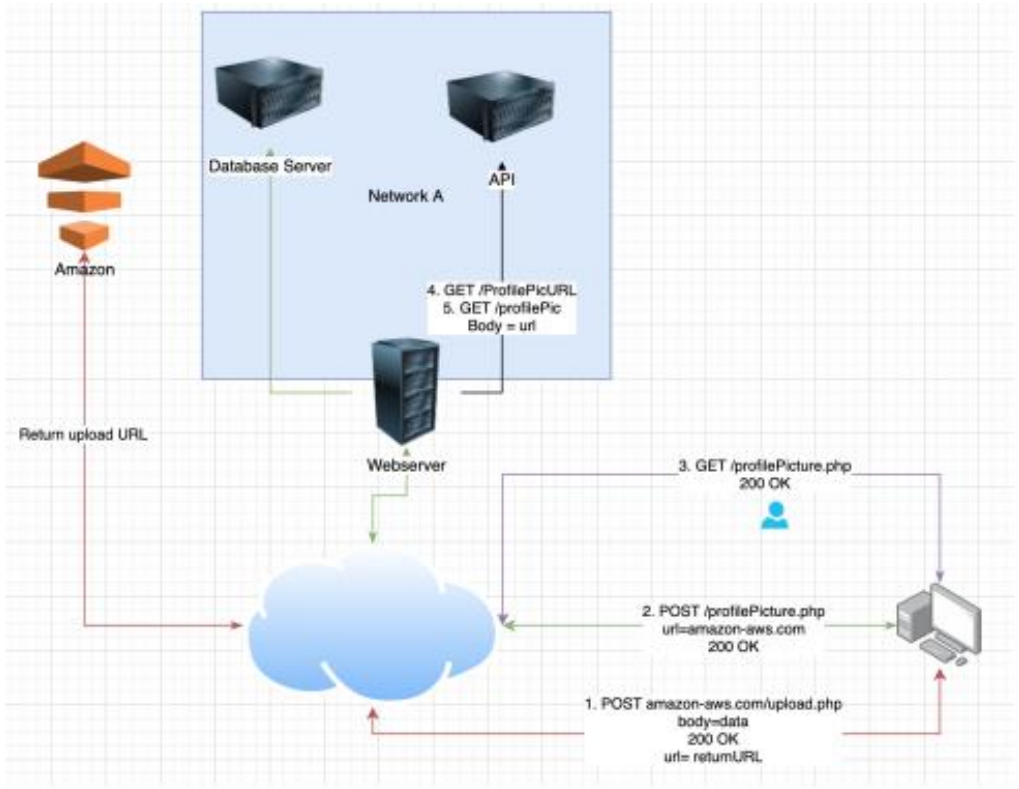
Case 1



Case 2



Case 3



Attack strategies

Basic SSRF strategy

- Bassic types of SSRF attacks
  - SSRF against the server itself
  - SSRF against other backend systems
- If all else fails
  - Blind SSRF
- Where to also look
  - Partial URLs in the body instead of a full URL
  - URLs within data files such as XML files or CSV files (import functionality)
  - The referer header can sometimes contain SSRF defects

SSRF against the server itself

- Where to start
- Attack on loopback ip

Example:

```
POST /profilePicURL.php
url=127.0.0.1:81/getUsers.php
-----------------------
GET /profilePic.php
200 OK
TestName1 TestName2 TestName1@test.test
TestName3 TestName4 TestName5@test.test
```

SSRF against other backend systems

- When can it occur?

Example:

```
POST /profilePicURL.php
url=192.168.32.123:3387/getUsers.php
-----------------------
GET /profilePic.php
200 OK
TestName1 TestName2 TestName1@test.test
TestName3 TestName4 TestName5@test.test
```

Blind SSRF

- How it works?
- Burp collaborator
- RCE
- HTTP request