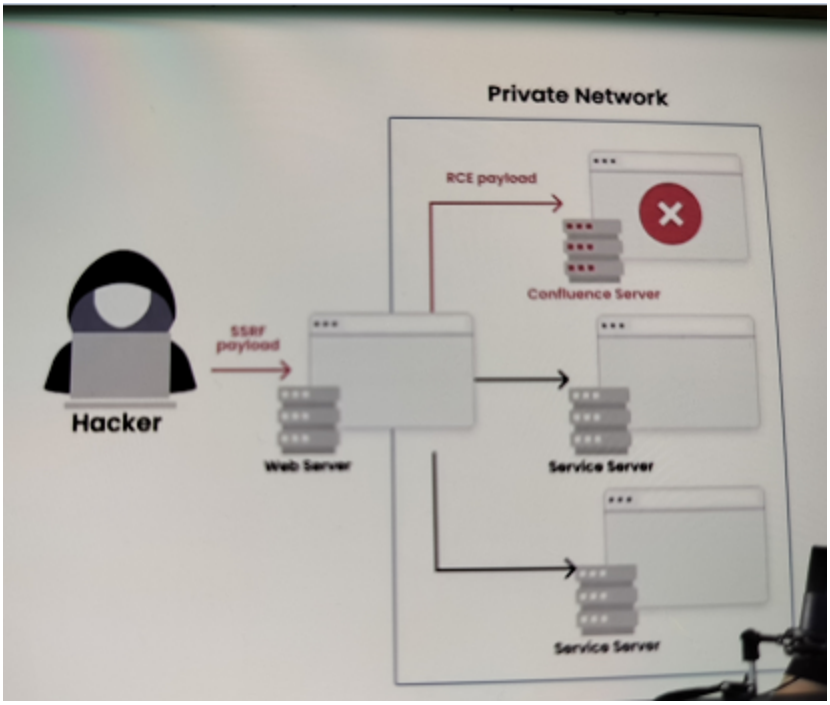
Server-side Request Forgery(SSRF)

Server-side request forgery is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location.

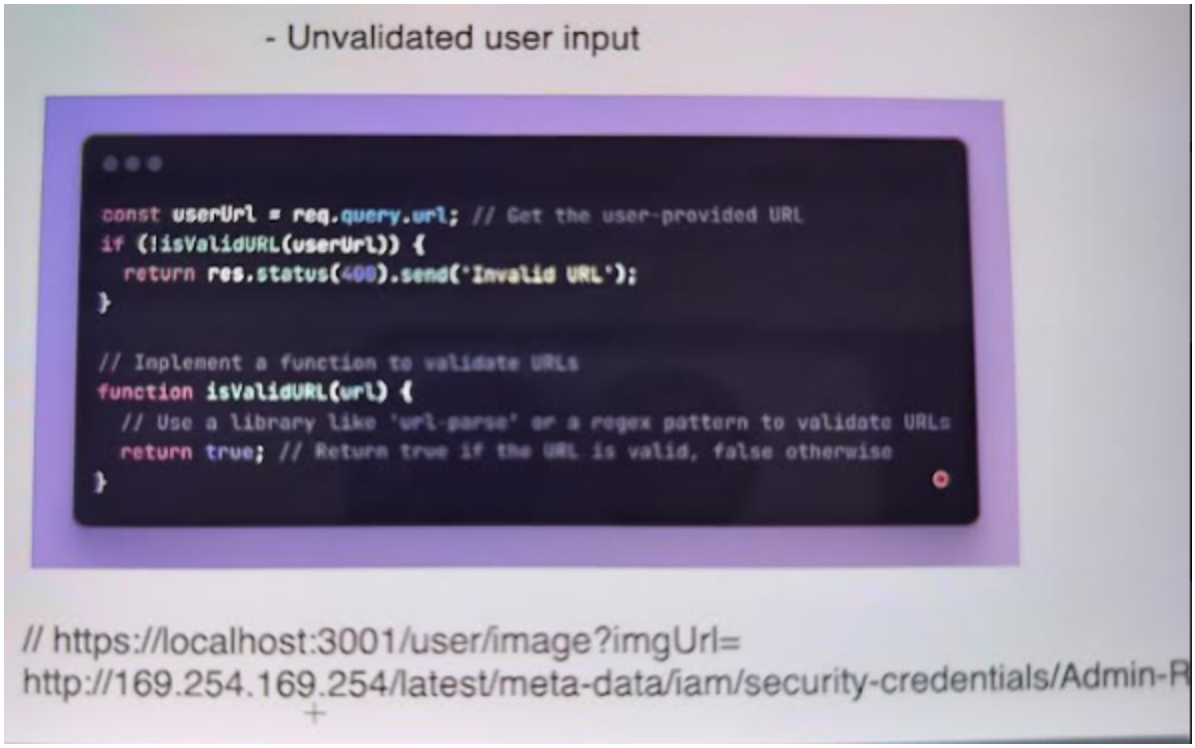
In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems. This could leak sensitive data, such as authorization credentials.



Reasons for this -

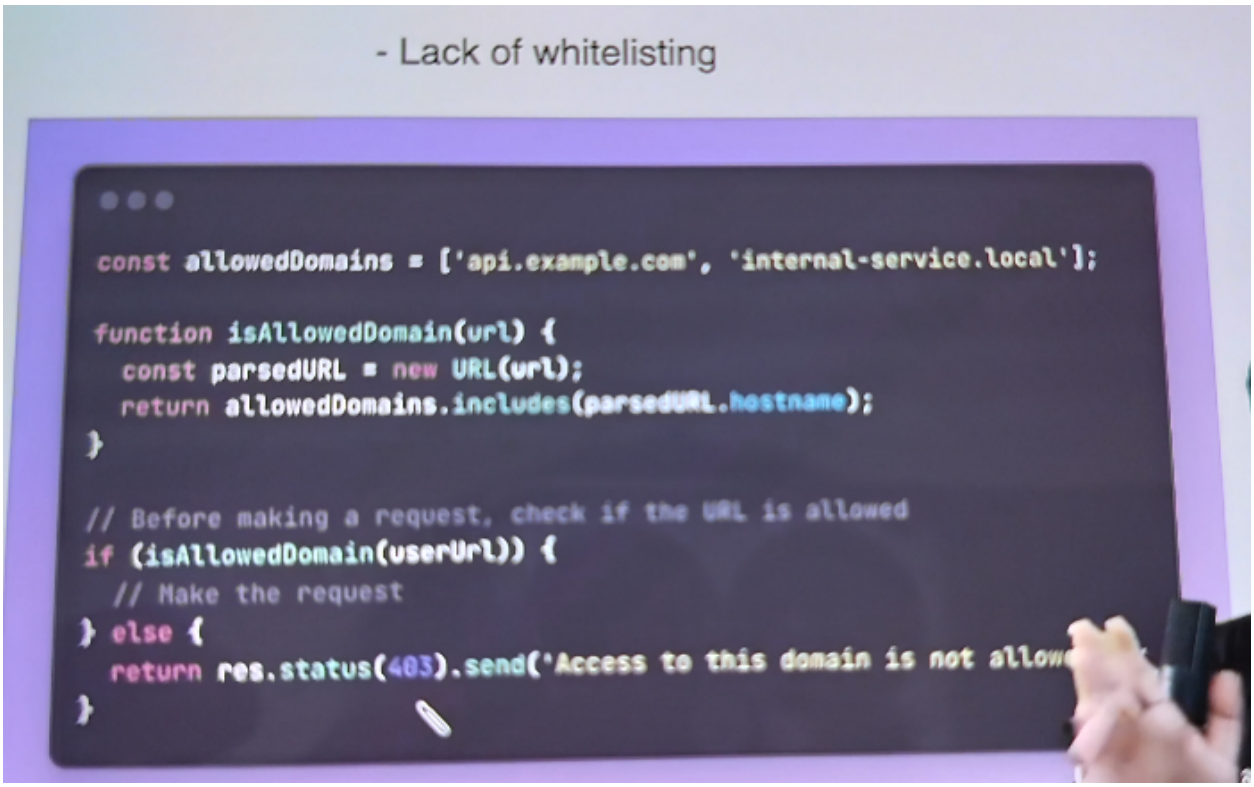
Unvalidated user input

You must always ensure that you validate user input



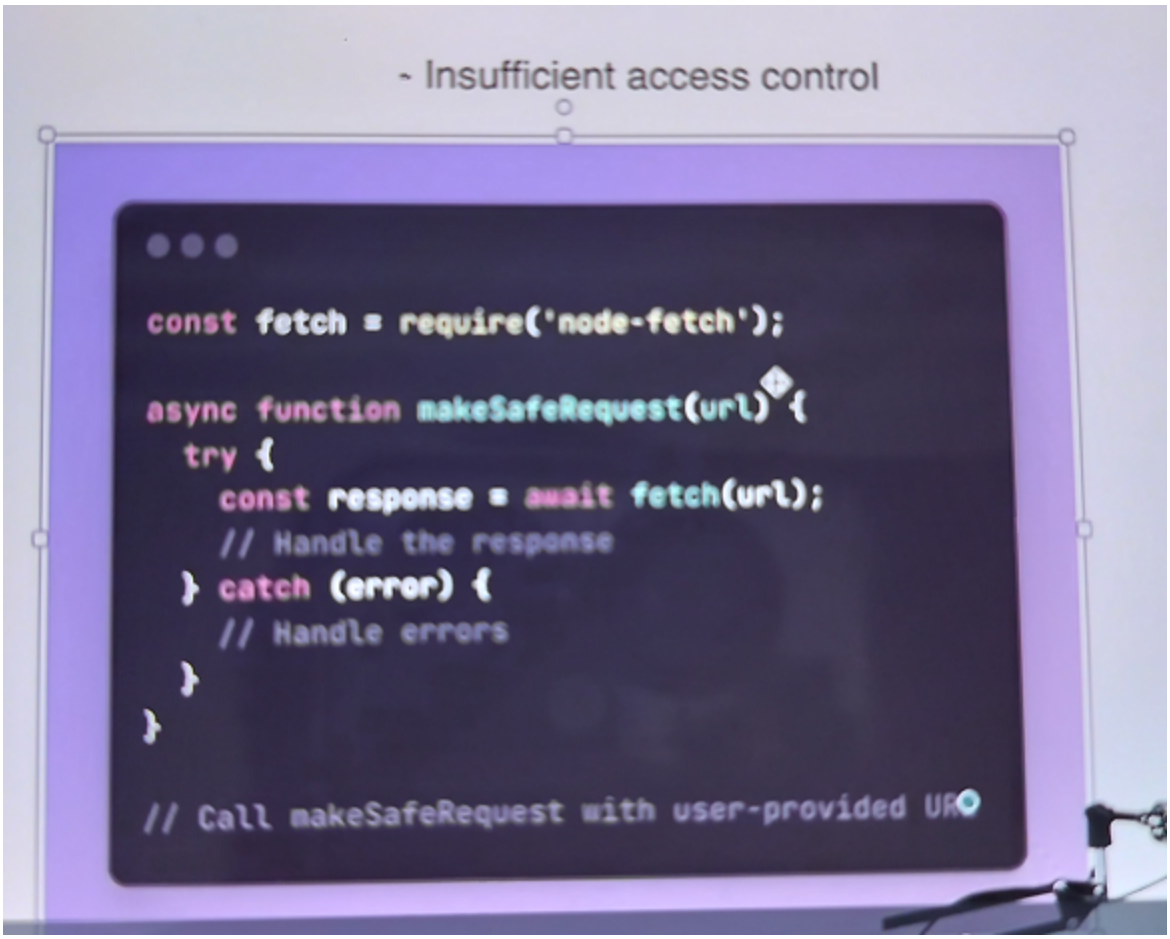
Lack of whitelisting

example of whitelisting



Insufficient access control

Did you create policies around what all can be accessed from file system, operating system, database, network layer,



Using popular libraries like node-fetch and axios can provide us first layer of protection again SSRF

XML External entity attack(XXE)

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

In this case, payload or user input (xml) is sent and our parser or serialization/deserialization technique is not able to distinguish between xml and html/input data, so you end up executing that xml and leaking our internal server data.

html, svg, pdf can look like xml