Introduction to Information and Computer Security (CS-5340)

Group Members

Divya Sri Mullapudi

R11910418

Jahnavi Gurrala

R11876605

Vivekkumar Pawankumer Thakur

R11903119

Anthony Humphreys

R11625346

Project Topic

Exploring Server-Side Request Forgery

Project Background and Challenges

Server-Side Request Forgery (SSRF) is a web security vulnerability that allows an attacker to make a server-side application to make HTTP requests to arbitrary domains. This type of vulnerability comes to surface when an application takes untrusted user input and uses it to construct a request to another server without the proper validation.

The primary challenge with SSRF vulnerabilities is their ability to bypass network restrictions, and security by exploiting the server's inherent trust in its internal network. Which can lead to unauthorized access, expose sensitive data, and worst case scenario a full system compromise by attacking other vulnerabilities.

Some of the common challenges in detecting and mitigating SSRF include:

- **Preventing SSRF in applications.**
- **Identifying SSRF vulnerabilities in complex systems.**
- **Keeping up with evolving SSRF attack trends.**
- **Implementing and maintaining effective SSRF protection techniques.**

Proposed Solution

To address the challenges posed by SSRF vulnerabilities, we propose a comprehensive approach by creating our own application tackling these challenges:

We will develop a Django application that demonstrates common SSRF vulnerabilities and uses modern techniques to patch these vulnerabilities. As for now we will keep our server as a local host, as we can still implement the security measures below. If expanding on our topic more becomes necessary, we can add more features, but for now our solution will focus on:

- Implementing strict input validation to ensure that user-provided URLs are safe.
- Blocking access to internal IP ranges and sensitive cloud metadata endpoints.
- Logging and monitoring outgoing requests to detect potential SSRF attempts.
- Incorporating role-based access control to allow legitimate actions while protecting sensitive internal resources.

By combining detection and mitigation strategies, this project aims to provide practical solutions for addressing SSRF vulnerabilities in real-world web applications.