Introduction to Server-Side Attacks

As mentioned in this module's summary, Server-Side Attacks leverage the below in an attempt to issue requests on behalf of the hosting application server, leak sensitive data, or have the hosting application server execute attacker-supplied commands:

1. The trust between the final application server and intermediate machines/components or itself
2. User input-handling inefficiencies, such as differences regarding interpretation or poor validation

Types of Server-Side Attacks

This module will cover different types of Server-Side attacks and how to exploit them. These are:

- `Abusing Intermediary Applications`: Accessing internal applications not accessible from our network by leveraging specific exposed binary protocols.
- `Server-Side Request Forgery (SSRF)`: Making the hosting application server issue requests to arbitrary external domains or internal resources in an attempt to identify sensitive data.
- `Server-Side Includes Injection (SSI)`: Injecting a payload so that ill-intended Server-Side Include directives are parsed to achieve remote code execution or leak sensitive data. This vulnerability occurs when poorly validated user input manages to become part of a response that is parsed for Server-Side Include directives.
- `Edge-Side Includes Injection`: Edge Side Includes (ESI) is an XML-based markup language used to tackle performance issues by temporarily storing dynamic web content that the regular web caching protocols do not save. Edge-Side Include Injection occurs when an attacker manages to reflect ill-intended ESI tags in the HTTP Response. The root cause of this vulnerability is that HTTP surrogates cannot validate the ESI tag origin. They will gladly parse and evaluate legitimate ESI tags by the upstream server and malicious ESI tags supplied by an attacker.
- `Server-Side Template Injection (SSTI)`: Template Engines facilitate dynamic data presentation through web pages or emails. Server-Side Template Injection is essentially injecting ill-intended template directives (payload) inside a template, leveraging Template Engines that insecurely mix user input with a given template.
- `Extensible Stylesheet Language Transformations Server-Side Injection`: Extensible Stylesheet Language Transformations (XSLT) is an XML-based language usually used when transforming XML documents into HTML, another XML document, or PDF. Extensible Stylesheet Language Transformations Server-Side Injection can occur when arbitrary XSLT file upload is possible or when an application generates the XSL Transformation's XML document dynamically using unvalidated input from the user.

Let's now dive into each attack in detail.

Next ➔   ✓ Mark Complete & Next

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left