Stands for Server-Side Request Forgery. It's a vulnerability that allows a malicious user to cause the webserver to make an additional or edited HTTP request to the resource of the attacker's choosing.

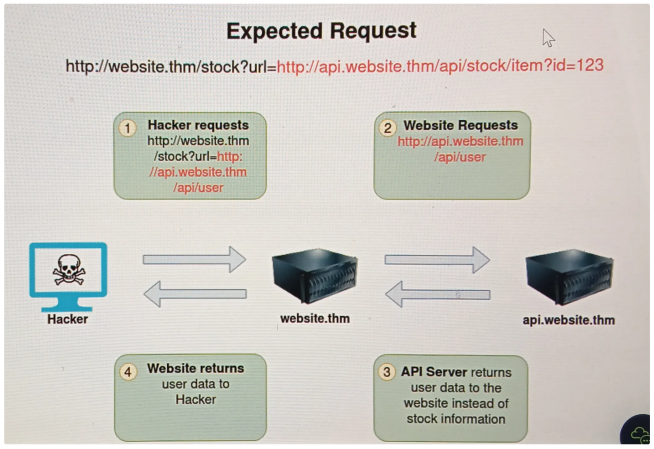
Two types of SSRF

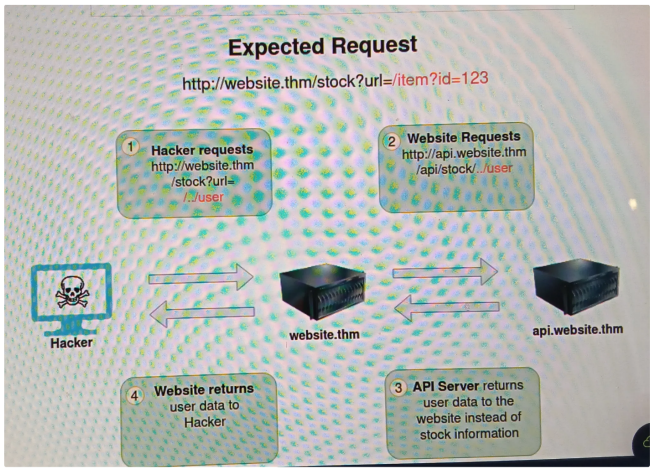
1. Regular SSRF where data is returned to the attacker's screen.
2. Blind SSRF vulnerability where an SSRF occurs, but no information is returned to the attacker's screen

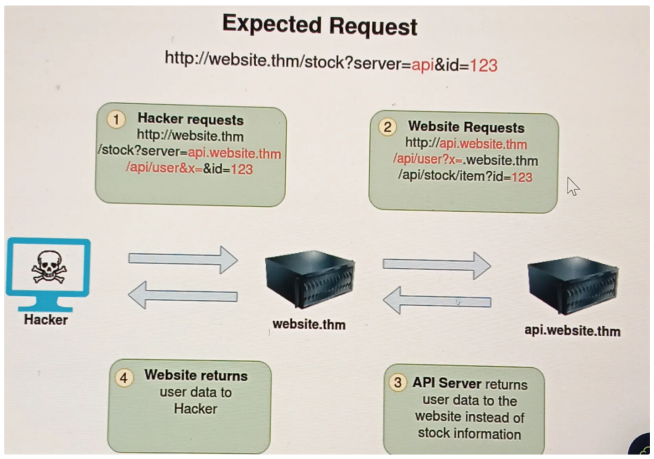
Successful SSRF attack can result in any of the following:

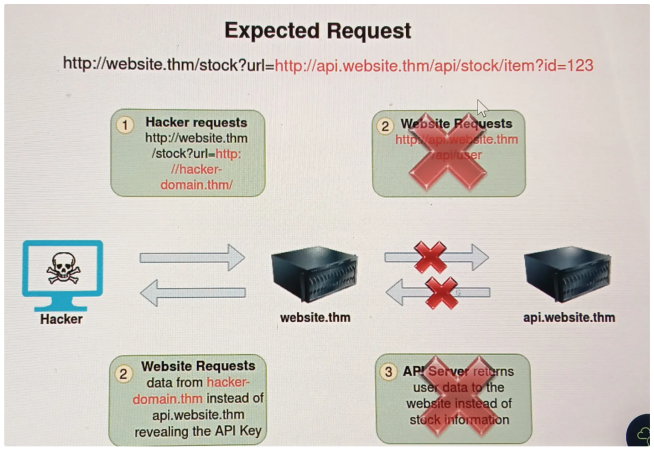
1. Access to unauthorized areas.
2. Access to customer/organizational data.
3. Ability to scale internal networks
4. Reveal authentication tokens/credentials my

Below example shows how the attacker can have complete control over the page requested by the web server. The expected request is what the website.thm server is expecting to receive, with the section in red being the URL that the website will fetch for the information. The attacker can modify the area in red to an URL of their choice.









Potential SSRF vulnerabilities can be spotted in web applications in many different ways. Here is an example of four common places to look:

When a full URL used in parameter in the address bar:

```
<form method="post" action="/form">
    <input type="hidden" name="server" value="http://server.website.thm/store">
    <div>Your Name:</div>
    <div><input name="client_name"></div>
    <div>Your Email:</div>
    <div><input name="client_email"></div>
    <div>Your Message:</div>
    <div><textarea name="client_message"></textarea></div>
</form>
```

Partial URL such as just the hostname.

Or perhaps only path of the URL.

requestbin.com can be used to catch HTTP request from a server.

More security-savvy developers aware of the risks of SSRF vulnaribilities may implement checks in their applications to make sure the requested resource meets specific rules. There are usually two approaches to this, either deny list or an allow list.

Deny List

A deny list is where all requests are accepted apart from resources specified in a list or matching a particular pattern. Attackers can bypass a Deny List by using alternative localhost references such as 0,0.0.0.0, 0000, 127.1, 127.*.*.*, 2130706433, 017700000001 or subdomains that have a DNS record which resolves to the IP Address 127.0.0.1 such as 127.0.0.1.nip.io.

Also, in a cloud environment, it would be beneficial to block access to IP address 169.254.169.254, which contains metadata for the deployed cloud server, including possibly sensitive information.

Allow List

A allow list is where all requests get denied unless they appear on a list or match a particular pattern, the rule checks only the beginning of the URL but doesn't verify if the entire URL belongs to the trusted domain.This loophole let's attackers sneak in their own URLs.