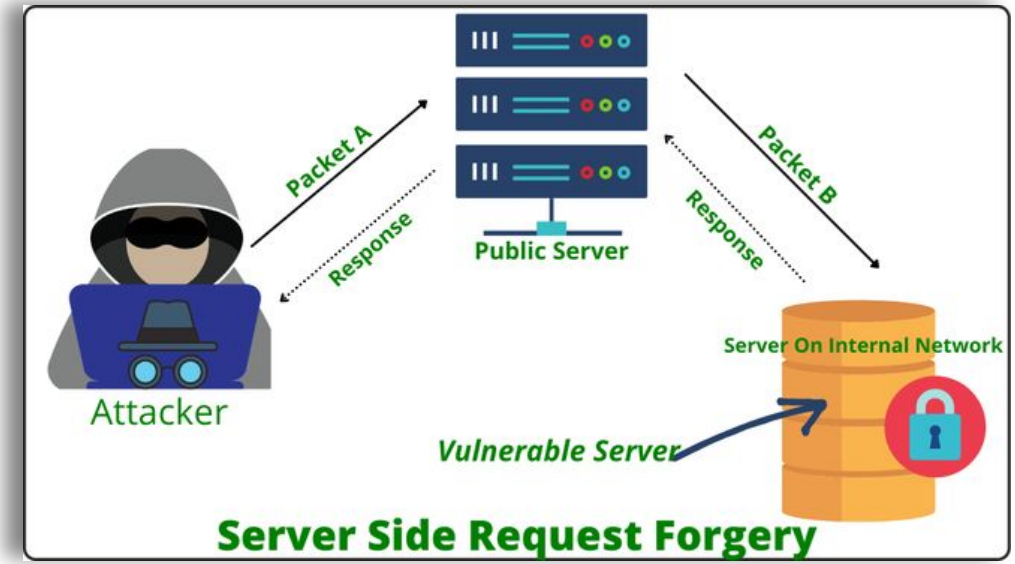
Server-Side Request Forgery

A10:2021-Server-Side Request Forgery

Overview

- A new category added in 2021, the SSRF category.
- Low incidence rate (2.72%) on average.
- Average weighted exploitation 8.28 / 10.
- Average coverage 67.72%.
- Total number of occurrences 9,503.
- Total number of CVEs 385.

Principle


Packet A
Response
Public Server
Packet B
Response
Attacker
Server On Internal Network
Vulnerable Server
Server Side Request Forgery

Principle

A hidden field in a form:

```
<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>
```

A partial URL such as just the hostname:

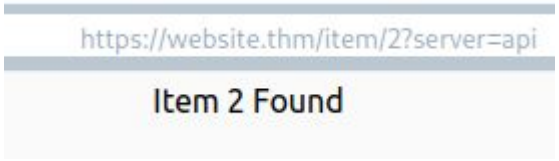
https://website.thm/form?server=api

Types

- Standard SSRF
- Blind SSRF
  - Application can be induced to issue a back-end HTTP request to a supplied URL.

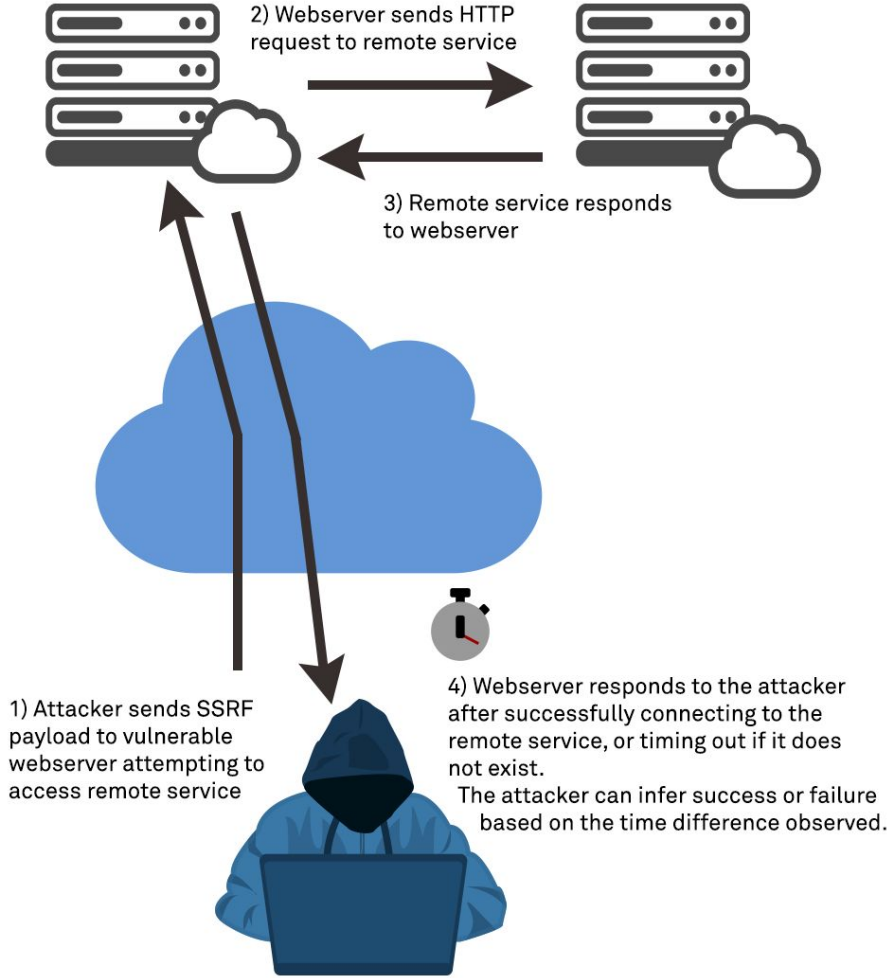
Standard SSRF

- Data are returned to the attacker screen
- Example from :
  https://website.thm/item/2?server=api
  To :
  https://website.thm/item/2?server=server.website.thm/flag?id=9&other=test



Blind SSRF

- Check behaviour in order to determine if it is a success or not
- For example, like in blind SQLi, use **timeout** or similar stuff in order to use **time-difference** observations



Consequences of an SSRF attack

- Private IP addresses
- Internal resources behind firewalls
- Server loopback interfaces, “localhost”, typically accessed through http://127.0.0.1
- Cloud service metadata
- Internal APIs
- Privileged files on vulnerable servers
- Local ports (discovered via port scanning)

Basic demo

- Basic usage of SSRF
  - Some are similar to Local File Inclusion (LFI)
- Docker network
- Access a service that is not accessible from the outside through a vulnerable exposed service

Impact on industry

- 100,000 businesses attacked globally since November 2022
- Ransomware on Microsoft Exchange servers

Microsoft Exchange: ProxyNotShell

ProxyNotShell consists of two security defects in Exchange Server:

- **SSRF**: CVE-2022-41040, with a CVSS score of **8.8**
- **RCE**: CVE-2022-41082, a remote code execution flaw with a CVSS score of **8.0**

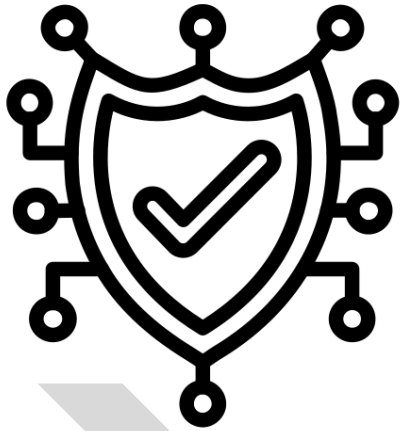
ProxyNotShell consequences

- SSRF to access the Autodiscover endpoint and reach the Exchange backend for arbitrary URLs
- RCE is exploited to execute arbitrary code. In response.

These 2 exploitations of vulnerabilities allow an **elevation of privilege.**

Microsoft deployed a series of URL rewrite mitigations for the Autodiscover endpoint

SSRF Mitigation Techniques



1. Firewalls
2. Application Controls
3. Whitelists and DNS Resolution
4. Authentication on Internal Services
    - Harden Cloud Services
5. Response Handling
6. Disable Unused URL Schemas (file://, ftp://, http://)
7. SSRF Protection with Bright Security DAST

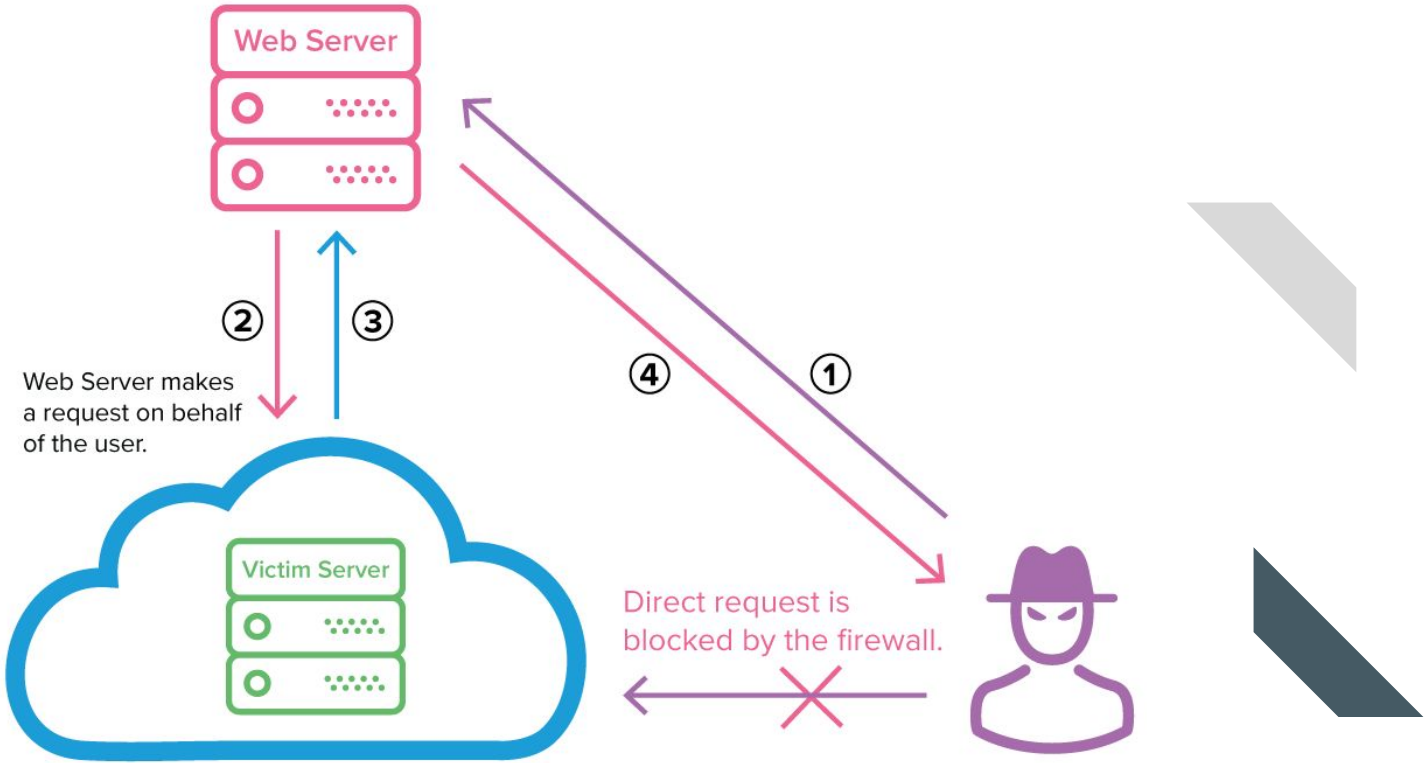
Deny List

- Where all request are accepted except those from a list/pattern
  - Try to bypass the matching pattern : **/allowedDirectory/../private** instead of **/private** which is blocked, like in the demo
  - Register an other domain which to reference this forbidden address

Allow List

- Where all requests get denied unless they appear on a list/pattern
  - Try to register a subdomain matching the pattern

Web Application Firewall



Advanced Demo

- Exercice on **TryHackMe**
- SSRF attack on the update of the avatar account

Conclusion

This vulnerability is likely to escalate in the coming years. Currently, it ranks 10th on the OWASP Top 10, but if we do not take the threat seriously, it will likely grow. It is important to be cautious of client-side crafted requests made to the server. To prevent this, we should always take the following precautions:

- Sanitize
- Analyze
- Block
- Avoid as much back-end logic in client-side as possible
- And never response without sanitizing.

References

- “7 SSRF Mitigation Techniques You Must Know.” *Bright Security*, 17 Jan. 2023, https://brightsec.com/blog/7-ssrf-mitigation-techniques-you-must-know
- A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021. owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_(SSRF).
- *CheatSheet OWASP SSRF*. (2017, January 26). owasp.org. https://cheatsheetseries.owasp.org/assets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet_SSRF_Bible.pdf
- Arghire, I. (2023, January 23). *Ransomware Uses New Exploit to Bypass ProxyNotShell Mitigations*. SecurityWeek. https://www.securityweek.com/ransomware-uses-new-exploit-bypass-proxynotshell-mitigations/
- https://portswigger.net/web-security/ssrf

Questions ?