Server-Side Request Forgery (SSRF)

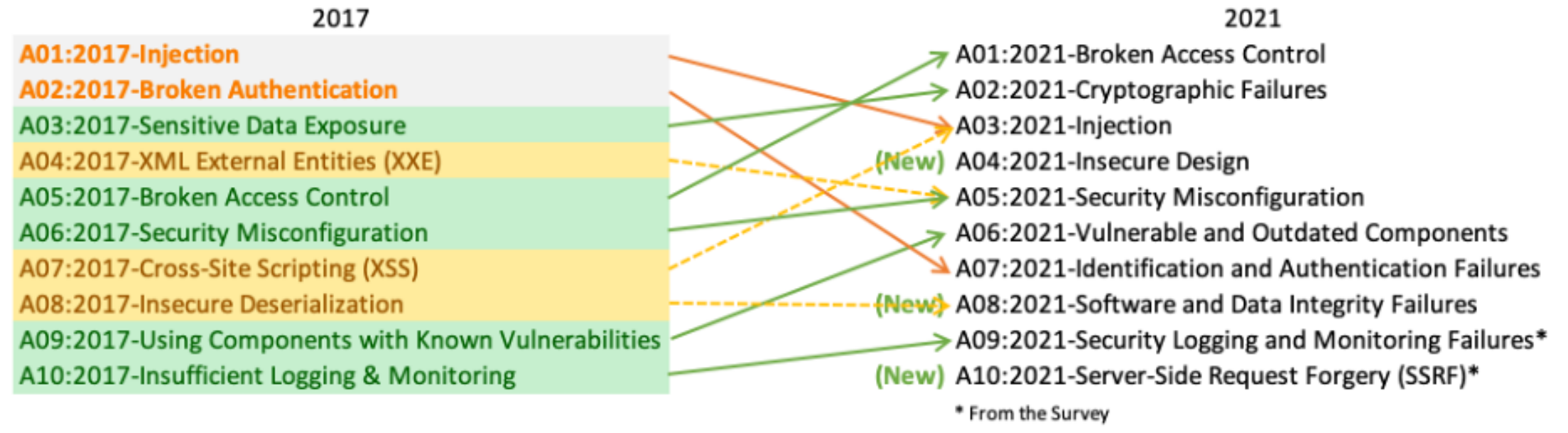
Logan Therrien

13 February 2023

Objectives

- Understand OWASP Top 10
- Understand a SSRF – Server-Side Request Forgery
- Describe Recent SSRF Attacks
- Describe Types of known SSRF Vulnerabilities
- Describe how to prevent SSRF Attacks

OWASP TOP 10



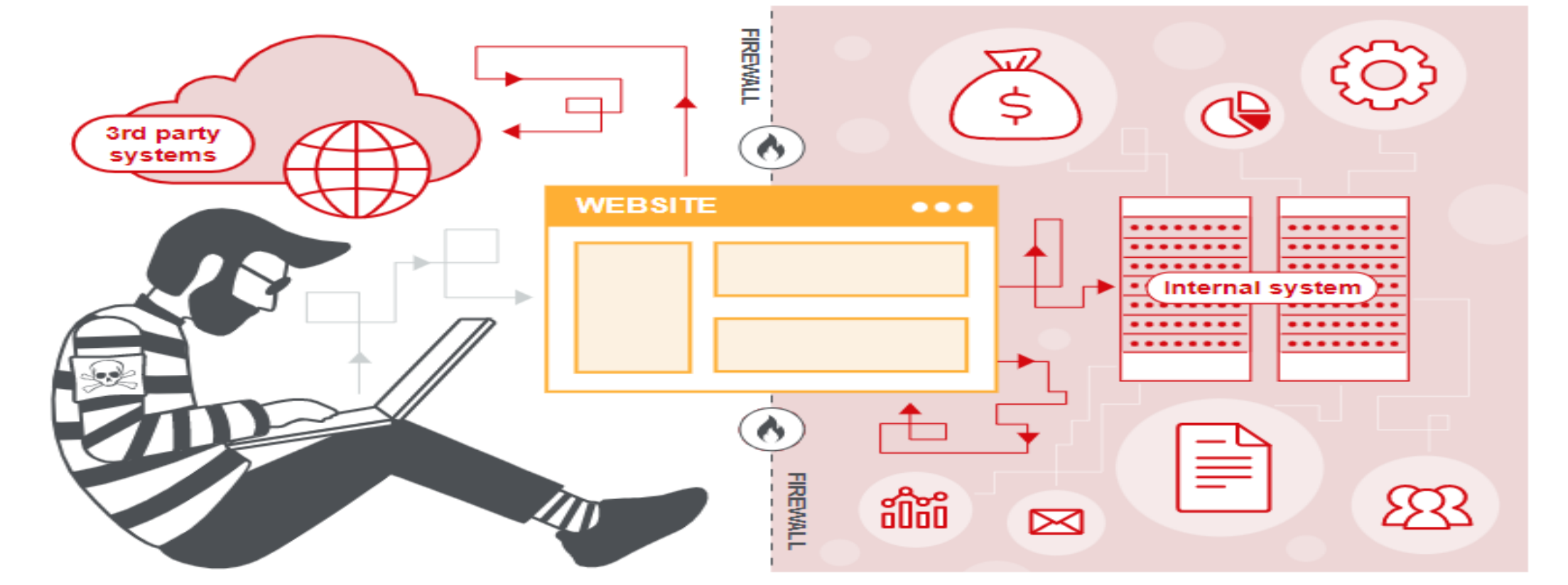
https://owasp.org/Top10/

Notable Breaches

- Capitol One (2019)
  - https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/
  - https://www.capitalone.com/digital/facts2019/

- Microsoft Exchange Server (2021)
  - https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/
  - https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
    - Attacker: China State sponsored group, Hafnium

Example Attacks



Portswigger.net

Example Attacks

Example Attack Scenarios

Attackers can use SSRF to attack systems protected behind web application firewalls, firewalls, or network ACLs, using scenarios such as:

Scenario #1: Port scan internal servers – If the network architecture is unsegmented, attackers can map out internal networks and determine if ports are open or closed on internal servers from connection results or elapsed time to connect or reject SSRF payload connections.

Scenario #2: Sensitive data exposure – Attackers can access local files or internal services to gain sensitive information such as `file:///etc/passwd` and `http://localhost:28017/`.

Scenario #3: Access metadata storage of cloud services – Most cloud providers have metadata storage such as `http://169.254.169.254/`. An attacker can read the metadata to gain sensitive information.

Scenario #4: Compromise internal services – The attacker can abuse internal services to conduct further attacks such as Remote Code Execution (RCE) or Denial of Service (DoS).

Example Attacks

- IT Pro TV
  - https://www.youtube.com/watch?v=-pNYmgK_dWo

A10:2021 Server-Side Request Forgery

- Added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential.
- This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

https://owasp.org/Top10/

FACTORS

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
1	2.72%	2.72%	8.28	6.72	67.72%	67.72%	9,503	385

https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

https://cve.mitre.org/

Overview

- Relatively low incidence rate (relative)
- Above average testing coverage
- Above-average Exploit and Impact potential ratings

HOW TO PREVENT

- From Network Layer
  - Segment remote resource access functionality in separate networks to reduce the impact of SSRF
  - Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.
  - Establish an ownership and a lifecycle for firewall rules based on applications.
    - Log all accepted *and* blocked network flows on firewalls (see A09:2021-Security Logging and Monitoring Failures).

HOW TO PREVENT

- From Application Layer
  - Sanitize and validate all client-supplied input data
  - Enforce the URL schema, port, and destination with a positive allow list
  - Do not send raw responses to clients
  - Disable HTTP redirections

References

- OWASP - Server-Side Request Forgery Prevention Cheat Sheet
- PortSwigger - Server-side request forgery (SSRF)
- Acunetix - What is Server-Side Request Forgery (SSRF)?
- SSRF bible
- A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages!

QUESTIONS