Server-Side Request Forgery (SSRF)

Alexander Tushinsky

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com

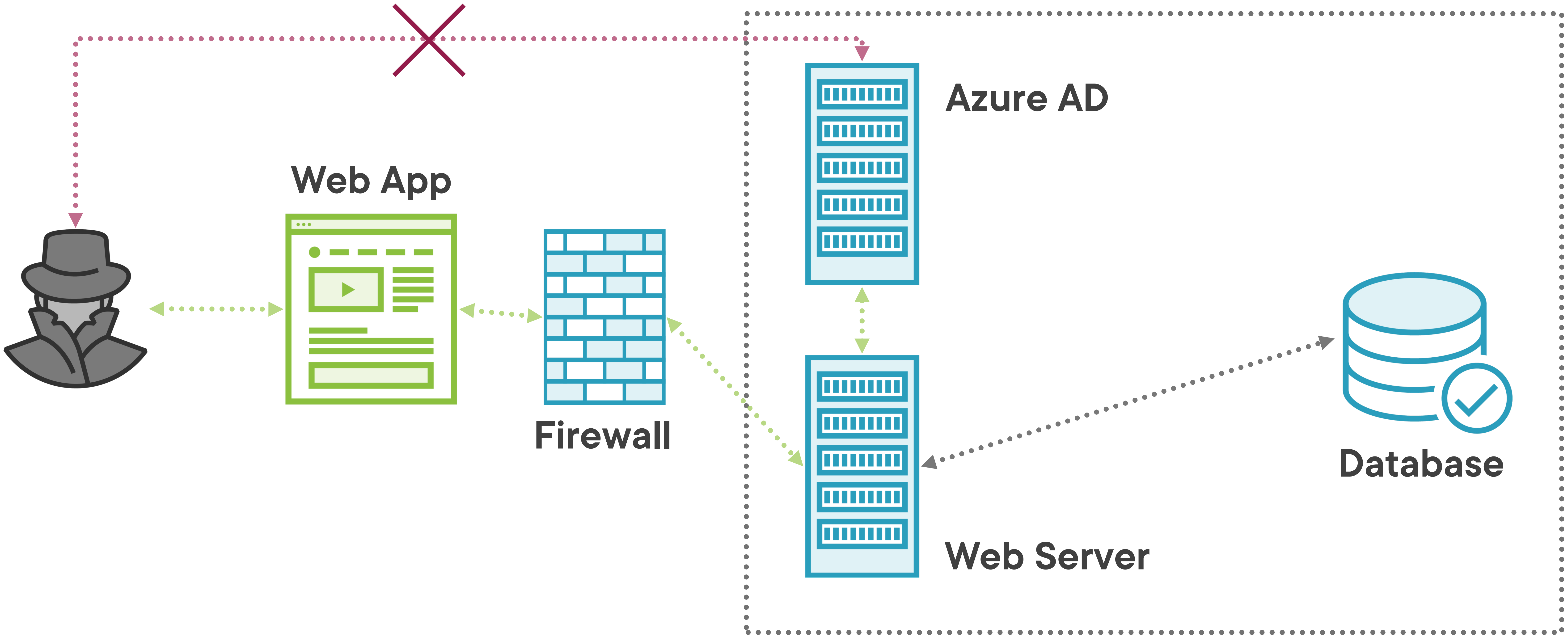
Overview

- What is the SSRF attack?
- Example
- OWASP Recommendation

Server-Side Request Forgery (SSRF)

- Occurs when a web application works with a remote resource without any validation
- Allows an attacker to bypass security defenses
- Can be part of other attacks

SSRF Example



Demo

Server-Side Request Forgery

- Examples of SSRF attacks

OWASP Recommendations

Network Level

- Segment your network
- Least privilege firewall rules
- Log all blocked traffic and monitor via a SIEM

Application Level

- Sanitize and validate all client supplied input
- Use allow lists
- Process response before sending to the client
- Disable HTTP redirects

Demo

Remediation

- Implement an allow list
- Validate user input

Summary

Server-Side Request Forgery (SSRF)

- Looked at the SSRF vulnerability
- OWASP Recommendations