WEB EXPLOITATION: COMMON TECHNIQUES & DEFENSES

WEB & CLOUD SECURITY

CYBERSECURITY DIRECTORATE

Web Exploitation is a BIG topic

A few common techniques

- Access Control Bypass
- Injection
- Server-Side Request Forgery (SSRF)
- Local File Inclusion (LFI)
- Unrestricted File Upload

Access Control Bypass

- Lack of least privilege
- Abusing improper validation

Adapted from OWASP Top 10:2021

Attacking	Defending (*do all of this*)
• Forced browsing • Leaked/hardcoded credentials • Parameter manipulation • Cryptographic token manipulation	• Enforce least privilege • Deny by default • Know thy dependencies; stay current (SBOM) • Employ active defenses • Behavioral analytics • Red Team • Log & audit

Demo Time

Improper Access Control

Injection

- Hostile user-supplied data is directly used
- Non-parameterized calls without context-aware escaping

Adapted from OWASP Top 10:2021

Attacking

- SQL
  - Direct output
  - Blind
- Content
- Command

Defending (*do all of this*)

- Sanitize & validate input
- Use "Safe" APIs (e.g., parameterized)
- Enforce least privilege
- Employ active defenses
- Log & audit

Demo Time

Injection

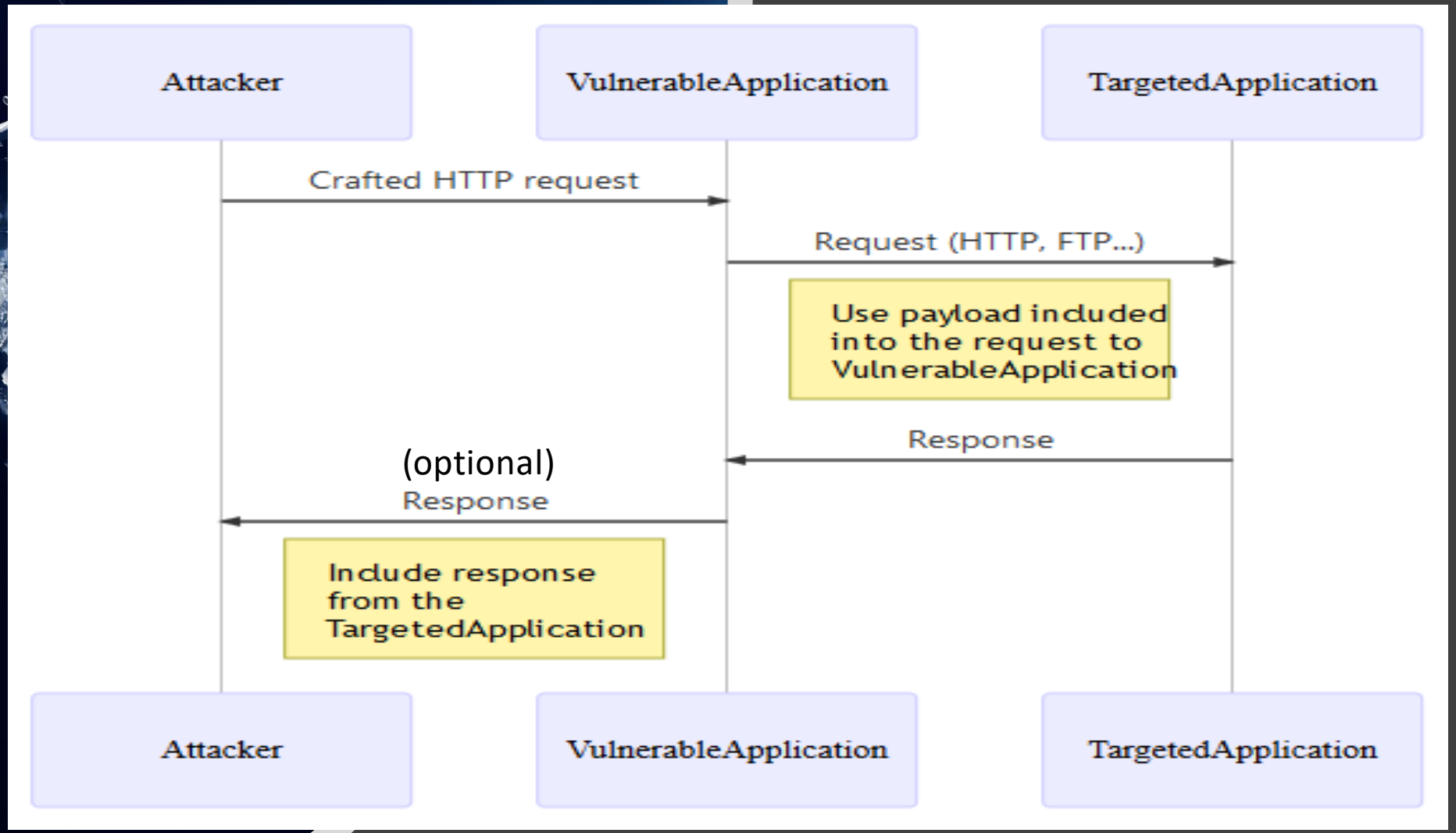
SSRF

- Coercing the server into making a request on the attacker's behalf

Adapted from OWASP Top 10:2021

Attacking	Defending (*do all of this*)
• Abuse trust relationships • Bypass network defenses • Leak sensitive information • Cloud metadata	• Network segmentation • Zero Trust architecture • Sanitize & validate input • Log & audit

SSRF - Visualized



From the OWASP SSRF Cheat Sheet

LFI

- Exploits dynamic file inclusion to view, edit, or execute an unexpected file
- Results in data exposure and possibly remote execution

Adapted from OWASP WSTG v4.2

Attacking

- Filenames passed as parameters or headers
- Dynamically served content less likely to be stored in a database
- Source code review

Defending (*do all of this*)

- Source code review
- Enforce least privilege
- Sanitize & validate input
- Log & audit

Demo Time

LFI sensitive data exposure

Unrestricted File Upload

- Uploaded files present risk to the server/application
- Unrestricted upload could lead to remote code execution or denial of service

Adapted from OWASP WSTG v4.2

Attacking	Defending (*do all of this*)
• Identify file uploads • Source code review • Bypass filtering mechanisms • Observe upload location	• Source code review • Segregate upload storage • Enforce least privilege • System generated filename • Allowlist file extensions • Employ active defenses • Log & audit

Demo Time

Unrestricted file upload

Happy Hunting!