Chapter 11

Secure Protocols and Applications

Episode 11.01

Episode title: **DNS Security**

Objective: **3.1 Given a scenario, implement secure protocols.**

Common Secure Protocols

- DNS
  - TCP/UDP port 53
  - Domain hijacking
  - URL redirection
  - Cache poisoning
  - Domain Name System Security Extensions (DNSSEC)
    - All DNS zones have certificates
- Simple Network Management Protocol (SNMP)
  - UDP port 161/162
  - Version 1, 2, 3

Common Secure Protocols

- Secure Shell (SSH)
  - TCP 22
- Secured File Transfer Protocol/FTP over SSL (FTPS)
  - TCP port 990
- SSH FTP (SFTP)
  - TCP port 22
- Secure Real-Time Transport Protocol (SRTP)
  - UDP port 5004

Quick Review

- DNS runs on TCP/UDP port 53 and is secured with DNSSEC
- SNMP runs on UDP port 161/162 and version 3 is the most secure implementation
- SSH runs on TCP port 22, FTPS runs on TCP port 990, SFTP runs on TCP port 22, and SRTP runs on UDP port 5004

Episode 11.02

Episode title: **FTP Packet Capture**

Objective: **3.1 Given a scenario, implement secure protocols.**

Quick Review

- FTP is the file transfer protocol and works on Windows, Linux, and macOS
- Unsecured FTP is easily hacked, be sure to use secure protocols like SFTP or FTPS
- Secure your network by limiting access, using secure protocols, or enabling IPSec

Episode 11.03

Episode title: **Secure Web and E-mail**

Objective: **3.1 Given a scenario, implement secure protocols.**

Securing Web Apps

- Can be accessible internally or externally
- Hide true Web server IP address
  - Load balancing
  - Reverse proxying
  - Network Address Translation (NAT)

Securing Web Apps

- HTTPS
  - Enabled on the Web server
  - Requires a server PKI certificate
  - Uses TCP port 443 instead of 80
  - TLS
    - Use version 1.2 or higher

Web App User Authentication

- Lightweight Directory Access Protocol Over SSL (LDAPS)
  - Directory service access protocol
  - Supported by Microsoft Active Directory
  - Requires a server PKI certificate
  - Uses TCP port 636 instead of 389
- On-premises and cloud

Simple Mail Transfer Protocol (SMTP)

- Domain reputation
  - Determines if mail will be received by other SMTP hosts
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Encrypt and sign e-mail messages
  - Requires a client PKI certificate

E-Mail Protocols

- SMTP
  - E-mail transfer protocol
- Post Office Protocol (POP)
  - Client e-mail retrieval protocol
- Internet Message Access Protocol (IMAP)
  - Client e-mail retrieval protocol
- Each can be secured with a server PKI certificate

Quick Review

- Public Web servers should be placed behind a load balancer, reverse proxy, or NAT
- HTTPS requires a server PKI certificate
- S/MIME can encrypt and sign individual e-mail messages
- SMTP, POP, and IMAP can be secured with a PKI certificate

Episode 11.04

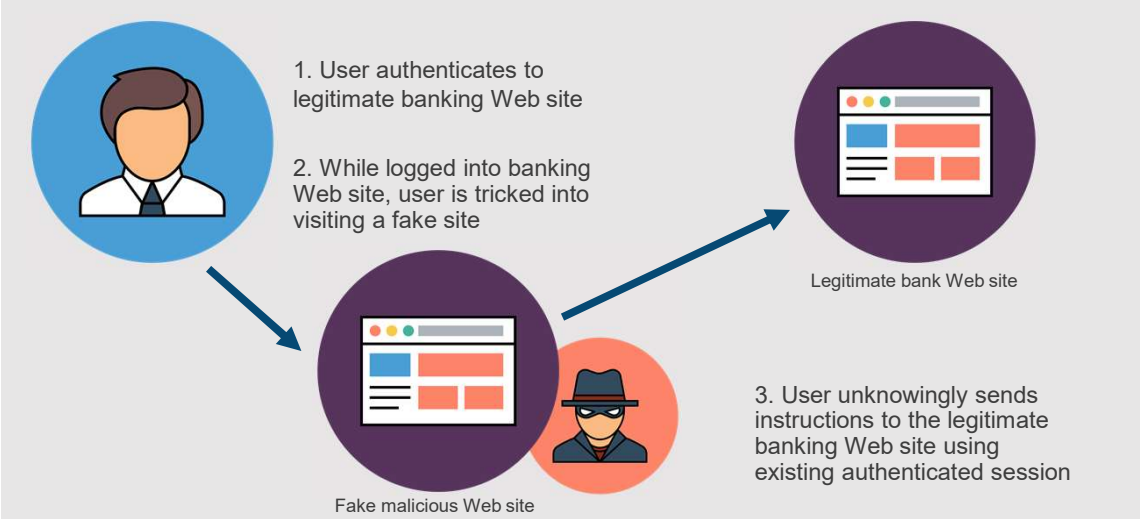
Episode title: **Request Forgery Attacks**

Objective: **1.3 Given a scenario, analyze potential indicators associated with application attacks.**

Request Forgeries

- Cross-site request forgery (CSRF)
  - Targets users and unchanging session tokens
  - Designed to hijack authenticated sessions between a client and a server
- Server-side request forgery (SSRF)
  - Targets Web servers
  - Designed to have server make HTTP requests to other services

Cross-Site Request Forgery



Request Forgeries

- Mitigation
  - Harden client devices
  - Use Web application firewall (WAF)

Quick Review

- Request forgeries involve hijacking existing sessions to run malicious user commands
- Cross-site request forgeries (CSRFs) attack victims that already have authenticated sessions
- Server-side request forgeries (SSRFs) attack server sessions to other hosts such as backend databases
- Mitigate Web app attacks by hardening client devices and using a WAF

Episode 11.05

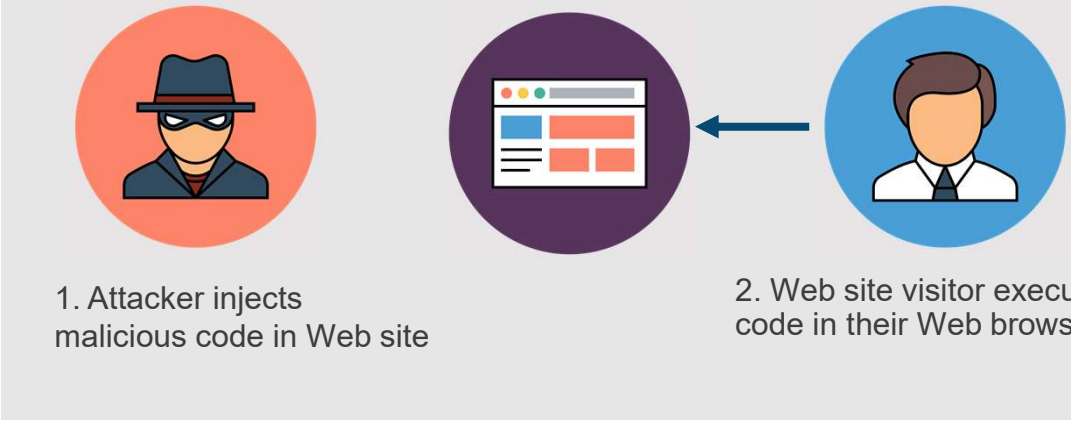
Episode title: **Cross-Site Scripting Attacks**

Objective: **1.3 Given a scenario, analyze potential indicators associated with application attacks.**

Cross-Site Scripting (XSS) Attack

- Starts with a Web app that doesn't properly validate or sanitize input
  - All user input must be untrusted
- Attacker injects malicious code into vulnerable Web site
  - JavaScript is commonly used
- Web site visitors unknowingly execute malicious code

Cross-Site Scripting (XSS) Attack



Quick Review

- All user input in an app must be considered untrusted
- A cross-site scripting (XSS) attack results from improper Web app input validation
- In an XSS attack, attackers inject malicious code into a Web app, then victims visit the Web app and malicious code executes on their device in the Web browser

Episode 11.06

Episode title: **Web Application Security**

Objective:

1.3 Given a scenario, analyze potential indicators associated with application attacks.

2.3 Summarize secure application development, deployment, and automation concepts.

3.2 Given a scenario, implement host or application security solutions.

Web App Security

- For Web server admins and Web app developers
- Harden public-facing and private Web apps

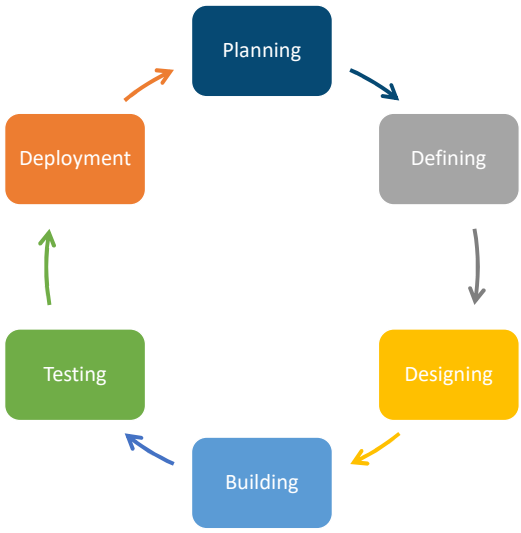
Injection Attacks

- Malicious user input is accepted by the Web app
- Types
  - Structured Query Language (SQL)
  - Lightweight Directory Access Protocol (LDAP)
  - Extensible Markup Language (XML)
- Mitigation
  - Sanitize all user input

Secure Coding

- Software development security best practices
  - Input validation
  - Secure Web browser cookies
  - HTTP headers
  - Code signing
  - Use trusted components and APIs

Software Development Life Cycle



Continuous Integration and Continuous Delivery (CI/CD)

- Automate developer code changes
- Test for quality assurance
- Send update notifications to users for code version control
- Security issues
  - Attackers could make changes and inject into the update

Infrastructure As Code

- VM templates
- Cloud templates
- Rapid and consistent provisioning/ deprovisioning
  - Useful for sandbox testing
- Security issues
  - Attackers could modify templates

Software Testing

- Static testing
  - Code review
  - Manually scanning code
- Dynamic testing
  - Observe runtime behavior
- Fuzzing
  - Provide app with unexpected data

Quick Review

- The OWASP Top 10 lists the most common Web application attacks
- CI/CD combines software development and management activities
- Adherence to secure coding and testing practices is required

Episode 11.07

Episode title: **Web App Vulnerability Scanning**

Objective: **1.7 Summarize the techniques used in security assessments.**