سرفصل دوره آموزش SANS SEC642

SEC642.1: Advanced Attacks

- Review of the testing methodology
- Using Burp Suite in a web penetration test
- Exploiting local and remote file inclusions
- Exploring advanced discovery techniques for SQL injection and other server-based flaws
- Exploring advanced exploitation of XSS and XSRF in a combined attack
- Learning advanced exploitation techniques

SEC642.2: Web Frameworks

- Mass assignment in CakePHP
- Authentication bypass in PHP
- MEAN stack attack
- SharePoint
- WordPress

SEC642.3: Web Cryptography

- Identifying the cryptography used in the web application
- Analyzing and attacking the encryption keys
- Exploiting stream cipher IV collisions
- Exploiting Electronic Codebook (ECB) Mode Ciphers with block shuffling
- Exploiting Cipher Block Chaining (CBC) Mode with bit flipping
- Vulnerabilities in PKCS#7 padding implementations

SEC642.4: Alternative Web Interfaces

- Intercepting traffic to web services and from mobile applications
- Flash, Java, ActiveX, and Silverlight vulnerabilities
- SOAP and REST web services
- Penetration testing of web services
- WebSocket protocol issues and vulnerabilities

- New HTTP/2 protocol issues and penetration testing

SEC642.5: Web Application Firewall and Filter Bypass

- Understanding of Web Application Firewalling and filtering techniques
- Determining the rule sets protecting the application
- Fingerprinting the defense techniques used
- Learning how HTML5 injections work
- Using UNICODE, CTYPEs, and Data URIs to bypass restrictions
- Bypassing a Web Application Firewall's best-defended vulnerabilities, XSS and SQLi