SEC542 – Web App Penetration Testing and Ethical Hacking

Topics

Introduction and Information Gathering
- Introduction and Information Gathering 1–3-13
- Defensible Network Architecture 1–14-53
- Protocols and Packet Analysis 1–54-107
- Virtualization and Cloud Essentials 1–108-165
- Securing Wireless Networks 1–166-235

Defense-in-Depth
- Defense-in-Depth 2–3-45
- Identity Access Managemnet 2–46-76
- Authentication and Password Secuirty 2–77-112
- Security Frameworks 2–113-141
- Data Loss Prevention 2–142-181
- Mobile Device Security 2–182-205

Vulnerability Management and Response
- Vulnerability Assessments 3–3-32
- Penetration Testing 3–33-76
- Attacks and Malicious Software 3–77-128
- Web Application Security 3–129-162
- Security Operations and Log Management 3–162-200
- Digital Forensics and Incident Response 3–201-239

Data Security Technologies
- Cryptography 4–3-52
- Cryptography Algroithms and Deployment 4–53-80
- Applying Cryptography 4–81-129
- Network Security Devices 4–130-184
- Endpoint Security 4–185-220

Windows and Azure Security
- Windows Security Infrastructure 5–3-43
- Windows as a Service 5–44-70
- Windows Access Controls 5–71-119
- Enforcing Security Policy 5–120-193
- Microsoft Cloud Computing 5–194-247
- Automation, Logging, and Auditing 5–248-296

Linux, AWS, and Mac Security
- Linux Fundamentals 5–3-66
- Linux Security Enhancements and Infrastructure 5–67-121
- Containerized Security 5–122-143
- AWS Fundamentals 5–144-161
- AWS Security Controls 5–162-178
- AWS Hardening 5–179-200
- macOS Security 5–201-215

Workbook
- tcpdump 5–26-37
- Wireshark 5–38-50
- Aircrack-ng 5–51-57
- Hashcat 5–58-69
- Cain and Abel 5–70-94
- AppLocker 5–95-123
- Nmap 5–124-139
- Malicious Software 5–140-147
- Command Injection 5–148-153
- hping3 5–154-163
- Image Steganography 5–164-184
- GNU Privacy Guard (GPG) 5–184-203
- Snort 5–204-227
- Process Hacker 5–228-244
- NTFS Permissions Reporter 5–245-258
- SECEDIT.EXE 5–259-266

A

- access control problems 1–15
- Acunetix Vulnerability Scanner 1–35
- American Fuzzy Lop 1–9
- Application Security
  - Dynamic Application Security Testing (DAST) 1–13, 1–17-18
  - Interactive Application Security Testing (IAST) 1–13
  - Out-of-Band Application Security Testing (OAST) 1–13
  - Static Application Security Testing (SAST) 1–13, 1–16
  - Testing
    - Full Knowledge 1–13
    - Zero-Knowledge 1–13
- Arachni Scanner 1–35
- ARPANET 1–92
- Assessments
  - Automated 1–20
  - Frameworks 1–22
    - OWASP Web Security Testing Guide 1–22
    - Penetration Testing Execution Standard (PTES) 1–22
  - Full-Knowledge 1–13, 1–21
  - Manual 1–20
  - Methodology 1–22
  - Testing Techniques 1–22
  - Zero-Knowledge 1–13, 1–21
- Attack Platform 1–33-34
- Attack platform 1–32
- Auditing 1–54
- Authentication (ATHN) 1–28
- Authorization (ATHZ) 1–28
- Automated Scanning 1–20

B

- backdoors 1–15
- BApp Store 1–53
- Best 1–20
- Bing 1–65
- Browser 1–32
- Browsers 1–36
- Bugtraq 1–10
- BuprSuite Pro Active/Live Scan 1–35

- Burp Suite
  - Infiltrator 1–13
- Burp Suite Professional 1–38, 1–42
  - BApp Store 1–53
  - Comparer 1–52
  - Crawling/Auditing 1–54
  - Dashboard 1–43
  - Decoder 1–51
  - Engagement Tools 1–55
    - Cenerage CSRF PoC 1–55
    - Content Discovery 1–55
    - Find Commment / Find Scripts 1–55
    - Search 1–55
    - Simulate Manual Testing 1–55
    - Target Analyzer 1–55
  - Extender 1–53
  - Heads-Up Dispaly 1–43
  - Intruder 1–48
  - Proxy 1–47
  - Repeater 1–49
    - Inspector 1–49
  - Sequencer 1–50
  - Target
    - Scope 1–44
    - Site Map 1–45
    - Site Map - Filter 1–46
- business functionality testing 1–10
- Business Logic (BUSL) 1–28

C

- CERN 1–91
- Certificate Authorities 1–87
- Certificate Transparency 1–87
- CHAOSNET 1–81
- Checklist 1–29
- Client Side (CLNT) 1–28
- Code review 1–13
- Command
  - HTTP/0.9 1–95
- Commands
  - dig (many) 1–81
  - dig domain lookup 1–80
  - DNSRecon 1–83-84
  - full (AXFR) zone transfer 1–75
  - reverse DNS 1–76
- Common Name 1–87
- concurrency problems 1–15
- Configuration and Deployment Management (CONF) 1–28
- cryptographic weaknesses 1–15
- Cryptography (CRYP) 1–28

D

- Decoding 1–51
- Dig 1–74
- dig 1–80
  - Syntax 1–81
- DNSRecon 1–77, 1–83-84
- Documentation 1–19
- Domain Name System (DNS) 1–74
  - Brute Force Scans 1–77
  - EDNS 1–74
  - PTR 1–76
  - Querying Directly 1–75
  - Recon Tools 1–78
    - dig 1–80-81
    - DNSRecon 1–83-84
    - Nmap 1–82
    - nslookup 1–79
  - Repositories 1–85-86
    - Dnsdumpster.com 1–85
    - Farsight Security's DNSDB 1–85
  - Reverse 1–75
  - Zone Transfer 1–74
- Dorking 1–67
- Dorks 1–66
- DuckDuckGo 1–65
- Dynamic Application Security Testing (DAST) 1–13, 1–17-18, 1–35
  - Scanners 1–35
  - Tools 1–17-18
- Dynamic web application security scanners 1–32

E

- Easter eggs 1–15
- EDNS 1–74
- Encoding 1–51
- Error Handling (ERRH) 1–28
- Exploit Database (EDB) 1–10

F

- filter bubble 1–64
- flawed business logic 1–15
- Fortify WebInspect 1–35
- forward proxy 1–38
- Full-Knowledge 1–13, 1–21

G

- Generalized Markup Language (GML) 1–91
- Google 1–65-66
- Google Dorks 1–66
- Google Hacking Database (GHDB) 1–66-67
  - GHDB-ID 4804 1–67
- Grep 1–48

H

- Hashing 1–51
- HCL AppScan 1–35
- HTTPS Certificates 1–87

SEC542 – Web App Penetration Testing and Ethical Hacking

Hypertext Transfer Protocol (HTTP)
- 0.9 . . . 1–95
- 1.0 . . . 1–95
- History . . . 1–9, 1–91
  - 0.9 . . . 1–9
- QUIC . . . 1–93
- Semantics . . . 1–93
- Syntax . . . 1–93

I

Identity Management (IDNT) . . . 1–28
Information Gathering . . . 1–59
Information Gathering (INFO) . . . 1–28
Interactive Application Security Testing (IAST) . 1–13
Interception Proxies . . . 1–38
- Configuring . . . 1–57
- Zed Attack Proxy (ZAP) . . . 1–39

Interception proxies . . . 1–32
Internet . . . 1–91-92
Invicti (formerly Netsparker) . . . 1–35

K

Kali . . . 1–33-34
- metapackages . . . 1–34
- Update Command . . . 1–34

Kerberos . . . 1–92

L

LinkedIn Open Networkers (LIONs) . . . 1–68
logic bombs . . . 1–15

M

Mailing Lists . . . 1–10
- Bugtraq . . . 1–10
- Full Disclosure . . . 1–10

Man-in-the-middle (MITM) . . . 1–38
Manual Assessments . . . 1–20
Manual Inspection and Reviews . . . 1–19
Methodology . . . 1–22
Micah Hoffman's OSINT MindMap . . . 1–61
Michal Zalewski . . . 1–9
Morris Worm . . . 1–92

N

Network Vulnerability Scanner . . . 1–35
Nikto . . . 1–35
NIST
- 800-30
  - Appendix D . . . 1–14

NIST National Vulnerability Database . . . 1–10
Nmap
- DNS NSE Scripts . . . 1–82

nslookup . . . 1–79

O

Offensive Security . . . 1–10
Open-Source Intelligence (OSINT) . . . 1–60
- For Web Application Testers . . . 1–62
- Micah Hoffman's OSINT MindMap . . . 1–61
- Search Engines . . . 1–64
  - Dorking . . . 1–67
  - Google Dorks . . . 1–66
  - Key Search Operators . . . 1–65
- Social Media . . . 1–68
  - LinkedIn . . . 1–68
- SpiderFoot . . . 1–71
- Suites . . . 1–70

Operational Security (OPSEC) . . . 1–71
Out-of-Band Application Secuirty Testing . . . 1–13
OWASP . . . 1–24
- Top 10 . . . 1–25-26
- Web Application Penetration Testing Methodology . . . 1–27
- Web Security Testing Guide (WSTG) . 1–19, 1–22, 1–29
  - Information Gathering . . . 1–59
  - Testing Categories . . . 1–27
  - Web Application Penetration Testing Methodology . . . 1–27

P

p0f . . . 1–9
Paros Proxy . . . 1–39
Penetration Testing . . . 1–17
Penetration Testing Execution Standard (PTES) . 1–22
Post-exploitation . . . 1–22
Push Button Pen Testing . . . 1–18

Q

Qualys WAS . . . 1–35

R

Rapid7 AppSpider . . . 1–35
Reconaissance . . . 1–22
Reporting . . . 1–22
Reverse DNS . . . 1–76
RFC
- 1918 . . . 1–92
- 1945 . . . 1–94-95

Runtime Application Self-Protection (RASP) . . . 1–13

S

Scanning . . . 1–22

SEC542 – Web App Penetration Testing and Ethical Hacking

- Security Posture ... 1–14
- Semantics ... 1–93
- Session Analysis ... 1–50
- Session Management (SESS) ... 1–28
- SOCMINT ... 1–68
- Software Development Lifecycle (SDLC) ... 1–17, 1–19
- Software Engineering Institute (SEI) ... 1–14
- Source Code Review ... 1–15
  - Advantages ... 1–15
  - Disadvantages ... 1–15
- SpiderFoot ... 1–71
- Static Application Security Testing (SAST) 1–13, 1–16
- Syntax ... 1–93

T

- Testing Techniques ... 1–22
- The Tangled Web ... 1–9
- Threat Modeling
  - Advantages ... 1–14
  - Disadvantages ... 1–14
  - NIST 800-30 ... 1–14
- Threat modeling ... 1–13
- Tim Berners-Lee ... 1–9, 1–91
- time bombs ... 1–15
- Tookkit ... 1–32
- Trojans ... 1–15

V

- Virtual Host Discovery ... 1–73
  - DNS ... 1–74-75
  - HTTPS Certificate ... 1–87
- Vulnerability assessment ... 1–22
- vulnerability mailing lists ... 1–10

W

- Web Application PenTester's Toolkit ... 1–32
- Web Applications ... 1–8
- Whitehat Sentinel ... 1–35
- World Wide Web ... 1–91
- World Wide Web (W3) ... 1–94

Z

- ZAP Active Scan ... 1–35
- Zed Attack Proxy (ZAP) ... 1–38, 39
  - Attack Menu ... 1–41
  - Functions
    - Active Scan ... 1–41
    - Forced browsing ... 1–41
    - Fuzzing ... 1–41
    - Spider and AJAX spider ... 1–41
  - Interface ... 1–40
- Zero-Knowledge ... 1–13, 1–21
- Zone Transfer ... 1–74-75