# 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
- Administrative Pages 1–152
- AJAX
  - Spidering 2–21
- Algorithms 1–131
  - Assymetric 1–131
    - DH 1–131
    - DSA 1–131
    - ECDH 1–131
    - ECDSA 1–131
    - RSA 1–131
  - Hashing
    - MD5 1–131
    - SHA 1–131
    - SHA256 1–131
    - SHA384 1–131
  - Symmetric
    - AES 1–131
    - DES 1–131
    - TDES/3DES 1–131
- American Fuzzy Lop 1–9
- Application Frameworks 1–151
- Application Information Gathering
  - Spidering 2–13
- Application Infrastructure 1–150
- Application Security 1–10
  - Assessing 1–12-13
  - Dynamic Application Security Testing (DAST) 1–13, 1–17-18
  - Improving 1–12
  - 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
- Assymetric 1–131
- Attack Platform 1–33-34
- Attack platform 1–32
- Attack strings 2–36
- Auditing 1–54
- Authentication 2–50, 1–130
  - Basic 2–52-53
    - Illustrated 2–54
    - Issues 2–55
  - Bearer 2–72
  - Bypass 2–119
    - Parameter Tampering and Direct Page Access 2–120
    - SQLi 2–121
  - Digest 2–56
    - Illustrated 2–57
    - Issues 2–58
  - Form-based 2–63-64
    - Illustrated 2–65
    - Issues 2–66
  - Integrated Windows 2–59
    - Illustrated 2–60
    - Issues 2–61
  - OAuth 2–68-71
  - Openid/Oauth/SAML Authentication 2–67
  - Schemes 2–50
- Authentication (ATHN) 1–28
- Authorization
  - Attacks 2–123
  - Bypass 2–122
  - Role Enforcement 2–124
- Authorization (ATHZ) 1–28
- Automated Scanning 1–20

B

- backdoors 1–15
- BApp Store 1–53
- Bash shell 2–137
- Basic Authentication 2–52-53
  - Illustrated 2–54
  - Issues 2–55
- bcrypt 2–87
- Bearer Authentication 2–72
- Best 1–20
- Bing 1–65
- Browser 1–32
- Browsers 1–36
  - Authentication Schemes
    - Required 2–51
- Bugtraq 1–10
- BuprSuite Pro Active/Live Scan 1–35
- Burp Suite
  - Infiltrator 1–13
  - Request Parameters 1–111
- 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
- BurpSuite
  - AJAX 2–21
  - Authenticating 2–62
  - Discover Content 2–28
  - Intruder 2–92
    - Battering Ram 2–94
    - Cluster Bomb 2–96
    - Pitchfork 2–95
    - Sniper 2–93
  - Sequencer 2–111-112
  - Spidering 2–19
- business functionality testing 1–10
- Business Logic (BUSL) 1–28

C

- Cache-Control 1–124
- CERN 1–91
- Certificate Authorities 1–87, 1–132
- Certificate Transparency 1–87
- CEWL
  - Spidering 2–22
- CGI Scripts 2–139
- CHAOSNET 1–81
- Checklist 1–29
- Cipher Suites 1–130
- Cipher suites
  - Testing 1–134

- Client Side (CLNT) ........ 1–28
- Cloudflare Challenge ........ 1–163
- Code review ........ 1–13
- Command
  - HTTP/0.9 ........ 1–95
  - HTTP/1.0 ........ 1–96
  - HTTP/1.1 ........ 1–97
- Commands
  - Base64 Encode ........ 2–53
  - DELETE request ........ 1–116
  - dig (many) ........ 1–81
  - dig domain lookup ........ 1–80
  - DNSRecon ........ 1–83-84
  - echo prevent CR ........ 2–53
  - Enumerate HTTP methods ........ 1–153-154
  - FuFF ........ 2–30-32
  - full (AXFR) zone transfer ........ 1–75
  - HEAD request ........ 1–113
  - heartbleed.py ........ 1–164
  - nc port scan ........ 1–142
  - nmap https ........ 1–135
  - OPTIONS request ........ 1–116-117
  - reverse DNS ........ 1–76
  - Server strings ........ 1–123-124
  - SHA1 hash of session id ........ 1–104
  - testssl.sh ........ 1–136
  - Wget
    - robots off ........ 2–18
    - set proxy ........ 2–18
- Commmon Vulnerabilities and Exposures (CVE)
  - CVE-2014-6269 ........ 2–138
  - CVE-2014-6271 ........ 2–137
  - CVE-2014-6277 ........ 2–138
  - CVE-2014-6278 ........ 2–138
  - CVE-2014-6286 ........ 2–138
- Common Name ........ 1–87
- Common Vulnerabilities and Exposures (CVE) .. 2–48
- Concurrency attacks ........ 2–92
- concurrency problems ........ 1–15
- Confidentiality ........ 1–130
- Configuration and Deployment Management (CONF) 1–28
- Configuration Files ........ 1–151
- Content Management Systems(CMS) ........ 1–151
- Content-Type ........ 1–109
- Cookie ........ 1–122
- Cookies
  - Protecting ........ 3–8
- Crawling ........ 2–14
- Cross-Site Tracing (XST) ........ 1–114
- CRUD ........ 1–118
- Cryptographic Failures ........ 1–126
- cryptographic weaknesses ........ 1–15
- Cryptography (CRYP) ........ 1–28

## D

- Databases ........ 1–151
- Decoding ........ 1–51
- Default Web Pages ........ 1–151
- DELETE ........ 1–105
- Developer comments ........ 2–23
- Diffie-Helman ........ 1–129
- Dig ........ 1–74
- dig ........ 1–80
  - Syntax ........ 1–81
- Digest Authentication ........ 2–56
  - Illustrated ........ 2–57
  - Issues ........ 2–58
- DirBuster ........ 2–29
- Direct Page Access ........ 2–120, 2–125
- Directory Broswing ........ 2–46
- Directory Browsing
  - Google ........ 2–47
- Directory brute forcing ........ 2–27
- Disabled functionality ........ 2–23
- 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
- Electromagnetic Interference (EMI) ........ 2–84
- Encoding ........ 1–51
- Enrors
  - Information Leakage ........ 2–44
- Entropy ........ 2–112
- Error Handling (ERRH) ........ 1–28
- Exploit Database (EDB) ........ 1–10

## F

- FFuF 2–30-32
  - Custom Filters 2–32
  - HTTP request 2–31
  - Virtual Host Discovery 2–31-32
- filter bubble 1–64
- Fingerprinting 1–141
- flawed business logic 1–15
- Forced Browsing 2–27
  - BurpSuite 2–28
  - FFuF 2–30-32
  - file extensions 2–27
  - ZAP 2–29
- Form-based Authentication 2–63-64
  - Illustrated 2–65
  - Issues 2–66
- Fortify WebInspect 1–35
- forward proxy 1–38
- Full Disclosure 1–10
- Full-Knowledge 1–13, 1–21
- FuzzDB 2–40
- Fuzzing 2–36
  - Examples 2–37
  - Reviewing the Responses 2–38
  - ZAP 2–41

## G

- Generalized Markup Language (GML) 1–91
- GET 1–106-108
  - URI Query Parameters 1–108
- Globally Unique Identifiers (GUID) 2–103
- Google 1–65-66
  - Directory Browsing 2–47
- Google Dorks 1–66
- Google Hacking Database (GHDB) 1–66-67
  - GHDB-ID 4804 1–67
- Grep 1–48

## H

- Hashing 1–51, 1–131
- HCL AppScan 1–35
- HEAD 1–113
- Heartbleed 1–161
  - Effect 1–162
  - Exploit Output 1–164
- Hidden links 2–23
- High-risk functions 2–23
- HMAC
  - JWT Signature Cracking 2–76
- HPACK 1–98-99
- HttpOnly Bypass 1–114
- HTTPS
  - Authentication 1–130
  - Cipher Suites 1–130
  - Confidentiality 1–130
  - Integrity 1–130
  - Public Keys/Certificates and Certificate Authorities 1–132
  - Testing
    - nmap 1–135
    - Version and Cipher Suites 1–134
  - Transmission Security 1–127
- HTTPS Certificates 1–87
- Hypertext Transfer Protocol (HTTP)
  - 0.9 1–95
  - 1.0 1–95-96
  - 1.1 1–97
  - 3 QUIC 1–100
  - 2 1–98-99
  - History 1–9, 1–91
    - 0.9 1–9
  - QUIC 1–93
  - Request
    - Example 1–102
    - Highlights 1–123
    - Methods/Verbs 1–105-116, 1–122
    - Referer 1–121
    - User-Agent 1–120
  - Response
    - Cache-Control 1–123-124
    - Example 1–103-104
    - Server 1–123
    - Set-Cookie 1–123
    - Status Code 1–123
  - Semantics 1–93, 1–101
  - Syntax 1–93
  - Testing
    - Methods 1–153
  - URI Query Parameters 1–108

## I

- idempotent 1–105
- Identifying Web Server Components 1–151
- Identity Management (IDNT) 1–28
- Identity Provider 2–67
- Incident Response 2–11
- Information Gathering 1–59
- Information Gathering (INFO) 1–28
- Information Leakage 2–44
  - CVE search 2–48
  - Flaws 2–48
  - Types 2–45
- Insecure Direct Object Reference (IDOR) 2–125
- Insecure Directo Object Reference (IDOR)
  - AuthZ attacks 2–123
- Integrated Windows Authentication 2–59
  - Illustrated 2–60
  - Issues 2–61
- Integrity 1–130
- Integrity hashes 2–86
- 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

## J

- JSON Web Token (JWT) 2–72-73
  - Issues 2–76
  - Structure 2–74-75

## K

- Kali 1–33-34
  - metapackages 1–34
  - Update Command 1–34
- Kerberos 2–59, 1–92

## L

- Link Depth 2–14
- LinkedIn Open Networkers (LIONs) 1–68
- Logged Events and Sources 2–9
- Logging and Monitoring 2–8
  - Centralized Logs 2–10
  - Sources 2–9
  - Timestamping 2–9
- logic bombs 1–15
- Logic Flaws 2–16

## 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
- MD5 2–87
- META tags 2–15
- Method Interchange 1–112
- Method Tampering 1–112
- Methodology 1–22
- Micah Hoffman's OSINT MindMap 1–61
- Michal Zalewski 1–9
- MITRE 2–48
- Morris Worm 1–92
- Multiplexing 1–98
- Mutillidae 2–127
  - Hints 2–129
  - Reset DB 2–130
  - Security Levels 2–128
- mySQL 1–150

## N

- Netcraft Sitereport 1–149
- 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
- nmap 1–144-145
- nslookup 1–79
- NTML 2–59
- NTP 2–10

## O

- OAuth 2–68
  - Flow 2–69-71
- 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
- OpenID/OAuth/SAML Authentication 2–67
- OpenSSL 1–161
- Operational Controls 2–8
- Operational Security (OPSEC) 1–71
- OPTIONS 1–116
- Other software 1–151
- Out-of-Band Application Secuirty Testing 1–13
- OWASP 1–24
  - Top 10 1–25-26
    - A09:2021-Security Loggin and Monitoring Failures 2–8
    - Cryptographic Failures 1–126
  - 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
- Password hashes 2–86
- PATCH 1–118
- PBKDF2 2–87
- Penetration Testing 1–17

- Penetration Testing Execution Standard (PTES) . 1–22
- Pipelining . 1–98
- Port
  - 3306/tcp . 1–150
- Port Scanning . 1–142, 1–151
  - Tools
    - Netcraft . 1–143
    - Nmap . 1–143
    - Shodan . 1–143
    - Zenmap . 1–143
- POST . 1–109
  - Parameters . 1–110
- Post-exploitation . 1–22
- Private key . 1–132
- Privilege Escalation . 2–123
- Profiling . 1–141
- Pseudo-random number generators (PRNG) . 2–103
- Public key . 1–132
- Push Button Pen Testing . 1–18
- Push Promise . 1–98

## Q

- quality of protection (qop) . 2–56
- Qualys SSL Labs . 1–137
- Qualys WAS . 1–35
- Quick UDP Internet Connection (QUIC) . 1–100

## R

- Rapid7 AppSpider . 1–35
- Realm . 2–52
- Recon and Enum . 1–141
- Reconaissance . 1–22
- Referer . 1–121
- Reporting . 1–22
- Reverse DNS . 1–76
- RFC
  - 2069 Digest OG . 2–56
  - 2617 Digest Auth . 2–56
  - 6749 OAuth . 2–68
  - 6750 Bearer AuthN . 2–72
  - 7231book 1 . 114
  - 1918 . 1–92
  - 1945 . 1–94-95
  - 2246 . 1–127
  - 2616 . 1–97, 1–114
  - 2617 . 2–52
  - 3986 . 1–106, 1–108
  - 5246 . 1–127
  - 5789 . 1–118
  - 6265 . 1–114
  - 6520 . 1–161
  - 7231 . 1–97
  - 7232 . 1–97
  - 7233 . 1–97
  - 7234 . 1–97
  - 7235 . 1–97, 1–114
  - 7540 . 1–98
  - 7541 . 1–99
  - 8446 . 1–127
  - 9114 . 1–100
- Robot Exclusion Protocol . 2–15
- Robots.txt . 1–155
- robots.txt . 2–15
- Role Enforcement . 2–124
- RSA . 1–129
- Runtime Application Self-Protection (RASP) . 1–13

## S

- Scanning . 1–22
- SecLists . 2–40
- Security Information and Event Management (SIEM) 2–10
- Security Posture . 1–14
- Semantics . 1–93
- Server
  - Configuration flaw . 2–8
- Session Analysis . 1–50
- Session Management (SESS) . 1–28
- Sessions
  - Attacks . 2–110
    - Fixation . 2–113
    - Logout and Timeout . 2–114
    - Predictability . 2–111-112
  - Confidential . 2–107
  - Expire . 2–106
  - Identifiers . 2–101
  - Management . 2–100
    - Testing . 2–109
  - Management Principles . 2–102
  - Predicatbility . 2–104
  - Theft . 2–108
  - Unpredictable . 2–103
- Set-Cookie . 1–122-123, 1–124
- Shellshock . 2–137-139
  - fuzzing . 2–94
  - Payloads . 2–140
    - Execution and Impact . 2–143
    - Injection Explained . 2–141-142
  - Visualized . 2–144
- Shodan . 1–146-148
  - for Pentesters . 1–147
  - Port Scanner . 1–148
- Side-Channel Attacks . 2–84
  - Practical . 2–85
  - Timing . 2–86
    - Practical . 2–88
- Single Sign On (SSO)
  - Integrated Windows Authentication . 2–59
- Slow hashing . 2–87
- 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
Spidering 2–14
  AJAX 2–21
  Analyzing Results 2–23
  BurpSuite 2–19
  CEWL 2–22
  Command-Line 2–18
  Manual and Automated 2–17
  Manual vs. Automated 2–16
  ZAP 2–20
SQL Injection (SQLi)
  Auth Bypass 2–121
SSL 1–127
Static Application Security Testing (SAST) 1–13, 1–16
Status Codes 1–123
Symmetric 1–131
Syntax 1–93

T

Target
  Profiling 1–141
Testing Techniques 1–22
testssl.sh 1–136
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
Timing Attacks 2–86
  Practical 2–88
  Slow Hashing 2–87
Timing-based attack 2–38
TLS 1–127
  Handshake 1–128-129
Token Authentiction 2–72
Tookkit 1–32
Tools
  heartbleed.py 1–164
  Netcraft Sitereport 1–149
  nmap 1–144-145
  Shodan 1–146-147
Total cost of ownership (TCO) 2–83
TRACE 1–114
Transmission Security 1–127
Trojans 1–15

U

Unlinked content 2–27
URI Query Parameters 1–108
User-Agent 1–120
Username Enumeration 2–81-82
  Results to look for 2–83
  Side-Channel Attacks 2–84
Username enumeration 2–38
Username Harvesting 2–81-82
  Results to look for 2–83
  Side-Channel Attacks 2–84
UTC 2–10

V

Verb Tampering 1–112
Version Detection 1–151
Virtual Host Discovery 1–73
  DNS 1–74-75
  HTTPS Certificate 1–87
Vulnerability assessment 1–22
vulnerability mailing lists 1–10
Vulnerability Scans 1–151

W

Web Application PenTester's Toolkit 1–32
Web Applications 1–8
web client 1–120
Web Security Testing Guide (WSTG)
  Information Gathering 2–13
  Review Webserver Metafiles for Information Leakage 1–155
  Test HTTP Methods 1–153-154
  Testing for Weak Transport Layer Security 1–132
  WSTG-ATHN-04: Testing for Bypassing Authentication Schema 2–118
  WSTG-CONF-04: Review Unreferenced Files for Sensitive Information 2–43
  WSTG-IDNT-04: Testing for Account Enumeration 2–80
Web Servers 1–151
Wget 2–18
Whitehat Sentinel 1–35
Wordlists 2–36
World Wide Web 1–91
World Wide Web (W3) 1–94
WWW-Authenticate 2–51

Z

ZAP Active Scan 1–35
Zed Attack Proxy (ZAP) 1–38, 39
  AJAX 2–21
  Attack Menu 1–41
  Discover Content 2–29
  Functions
    Active Scan 1–41
    Forced browsing 1–41
    Fuzzing 1–41

# SEC542 – Web App Penetration Testing and Ethical Hacking

    Spider and AJAX spider . . . . . 1–41
Fuzzer . . . . . 2–41
Interface . . . . . 1–40
    Spidering . . . . . 2–20
Zero-Knowledge . . . . . 1–13, 1–21
Zone Transfer . . . . . 1–74-75