

SANS SEC542 – Web Pen Testing & Ethical Hacking

Topics

Intro & Info Gathering	542.1-1-151
Toolkit	542.1-23-29
Recon	542.1-30-74
Testing	542.1-75-151
Config, Identity & Auth Testing	542.1-1-116
Scanning	542.1-5-38
Spidering	542.1-39-63
Testing	542.1-64-116
Injection	542.1-1-137
Exploitation	542.1-1-137
XXE & XSS	542.1-1-152
Exploitation	542.1-1-152
CSRF, Logic Flaws & Adv Tools	542.1-1-115
Exploitation	542.1-1-104
Reporting	542.1-105-115
Capture the Flag	542.1-1-22



Categories

Labs





AJAX XSS	542.W-4-5
Authentication	542.W-2-6
Authentication Bypass	542.W-3-1
BeEF	542.W-4-4
Bonus Challenges	542.W-5A-1
Burp Intruder Fuzzing	542.W-2-8
Burp VS Snake	542.1-150
Command Injection	542.W-3-2
CSRF	542.W-5-1
Directory Browsing	542.W-2-5
DNS Harvesting	542.W-1-1
Heartbleed Testing & Exploitation	542.W-1-4
HTML Injection	542.W-4-3
HTTP Examination	542.W-1-2
LFI/RFI	542.W-3-3
Metasploit	542.W-5-6
Mobile MITM	542.W-5-2
Python	542.W-5-3
Server Info Gathering	542.W-2-1
Shellshock	542.W-2-2
Snake Challenge Walkthrough	542.W-1-5
SQLi Error-Based	542.W-3-4
SQLmap + ZAP	542.W-3-5
Testing HTTPS	542.W-1-3
Username Harvesting	542.W-2-7
VMware Bridged Mode How-To	542.W-6A-1
W3af	542.W-5-5
Web Spidering	542.W-2-3
When Tools Fail	542.W-5-7
WPScan	542.W-5-4

XXE	542.W-4-1
XSS	542.W-4-2
ZAP + SQLmap	542.W-3-5
ZAP Forced Browse	542.W-2-4

Tools










Acunetix	542.5-65
WVS	542.1-27
App Scanner (Trustwave)	542.1-27
.....	542.5-94
AppScan (IBM)	542.1-27
.....	542.5-65, 94
Aquatone	542.5-3
Aura → SPUD	
BBQSQL	542.3-119
BeEF	542.4-111-119
.....	542.5-46
+ Metasploit	542.5-68-69
BlindShell	542.4-119
Controller	542.4-113, 118-119
Functionalities	542.4-114-117
Hook	542.4-39, 62, 113
Interface	542.4-112
BruteLogic XSS Shell	542.4-86, 92
Burp	542.1-27-28, 84, 106, 109-122, 126
.....	542.5-65, 94
Comparer	542.2-99
Decoder	542.4-51
Filtering	542.1-112
Intruder	542.1-109-110, 118
?	542.2-108-112
.....	542.4-52, 98-102
Proxy	542.1-114-116
Retire.js	542.4-139
Scanner	542.1-109-110
Sequencer	542.3-21
Spider	542.1-117
.....	542.2-51
XSS Payloads	542.4-84
CeWL	542.2-53
Chromium	542.1-29
XSS Auditor ?	542.4-82
DirBuster	542.1-108
.....	542.2-50, 76
DNSRecon	542.1-36-38, 43-44
DOMinator	542.4-64
Echo Mirage	542.1-103
FaaS T	542.1-60
Fiddler 	542.1-104-105
ViewStateViewer	542.1-104
Watcher	542.1-104
X5s	542.1-104
Firefox	542.4-80
Developer Tools	542.4-54
Firesheep	542.3-10
FOCA 	542.1-60-62
FuzzDB	542.2-67
.....	542.4-84

SANS SEC542 – Web Pen Testing & Ethical Hacking


JBroFuzz	542.2–76
.....	542.4–84
Maltego	542.1–32, 64–66
Metasploit	542.1–37–38, 43, 45
.....	542.4–113, 118
.....	542.5–62–76
+ Drupalgeddon	542.5–76
+ Sqlmap	542.5–70
Browser AutoPWN	542.4–118
Database	542.5–64–65, 67
db_import	542.5–65
Integration	542.5–67
RPC	542.5–69
Web Scanning	542.5–66
ModSecurity	542.2–13
.....	542.5–52
Nessus	542.1–27
Netcat	542.1–134
.....	542.2–12–13, 23
.....	542.4–92
Netcraft  ?	542.2–14–15
NetSparker	542.5–65
Nikto ?	542.2–25, 76
.....	542.5–65
Nmap	542.1–37–38, 42, 135
.....	542.2–6–11
Options	542.2–6, 11
Service Probes	542.2–11
SSL Enum Ciphers	542.1–133, 135
OpenSSL	542.1–133–134, 141–142
OpenVPN	542.1–128
Paros Proxy	542.1–106
Qualy SSL Labs 	542.1–133, 136
Qualy WAS 	542.1–27
Recon-ng	542.1–67–74
Session Cookie Sniffer	542.3–10
SHINE	542.1–59
Shodan 	542.1–56–59, 63, 73–74
SPUD	542.1–54
Sqlmap	542.3–120–133
.....	542.4–133
.....	542.5–46
+ Metasploit	542.5–70
Data Exfil	542.3–131–132
Integrations	542.3–121–122
Options	542.3–123–133
Post-Exploitation	542.3–133
SSLDigger	542.1–136
SysInternals	542.1–32
TheHarvester	542.1–63
W3af	542.2–76
.....	542.5–46–58
Plugins	542.5–50–55
Wapiti	542.5–65
Wappalyzer	542.2–46–48
WebInspect (HP)	542.1–27
.....	542.5–94
Whitehat Sentinel	542.1–27

Wireshark	542.1–126
WMAP	542.2–76
.....	542.5–66
WPScan	542.5–41–42
XSScrapy	542.4–96, 107
Injection Payloads ?	542.4–107
XSSer	542.4–84, 96, 105–106
XSSSniper	542.4–96, 103–104
ZAP	542.1–27–28, 84, 106–108, 126
.....	542.5–94
Anti CSRF Test Form	542.5–12
Encode/Decode	542.4–53
Forced Browser	542.2–50
Fuzzer	542.2–68
Spider	542.2–44–45
Technology Detection	542.2–48–49
XSS Payloads	542.4–84
Zenmap	542.2–8

Terminal Commands

curl 	542.4–11–15
dig  	542.1–32, 34, 38, 40–41
.....	542.6–19
nc	542.4–92
nslookup 	542.1–38–39
sort 	542.5–37
tail 	542.5–37
wc	542.W–1–8
wget 	542.2–52
whois  	542.1–32

Security542 VM Toolkit

.....	542.1–15, 25
Chromium	542.4–82
XSS Auditor	542.4–82
Dig	542.W–1–1
DIRB	542.2–76
DirBuster	542.2–76
DNSRecon	542.1–37, 43
.....	542.W–1–1
FuzzDB	542.2–67, 76
Heartbleed 	542.1–144
.....	542.W–1–4
JBroFuzz	542.2–76
Metasploit	542.W–1–1
Mutillidae	542.3–31
Netcat	542.W–1–2
Nmap	542.W–1–1–3
OTG	542.1–15
SecLists	542.2–67, 76
Wireshark	542.W–1–2
WMAP	542.2–76
Wordlists	542.2–109
WPScan	542.5–42
XSSer	542.4–106
XSS Payloads	542.4–106
Zenmap	542.2–8

SANS SEC542 – Web Pen Testing & Ethical Hacking

A

Account Lockout	542.2–83, 86, 92, 98
Active Polling	542.2–14
Active Scan	542.1–108
.....	542.2–6
AJAX	542.1–9
.....	542.4–123–133, 135, 142
Attack Surface	542.4–131
Exploitation	542.4–133
Spider	542.4–132
American Fuzzy Loop	542.1–7
ANSI SQL92	542.3–97
Apache	542.2–24, 72–73
.....	542.3–50
mod_auth_digest	542.2–86
mod_rewrite	542.1–89
mod_security	542.2–13
mod_ssl	542.2–86
API	542.4–135, 138–139
ARPA Address	542.1–40–41
ARPANET	542.1–77
ASLR	542.5–81
Asterisk VoIP	542.4–119
ASVS	542.1–13
Asynchronous Communication	542.4–123
Attack Platform	542.1–25
Attack Surface	542.2–9
Attacker Perspective	542.1–98, 130
.....	542.2–83, 86, 88, 92
.....	542.3–13
Authentication	542.2–80–92
Basic	542.2–81–83
.....	542.5–34, 55
Bypass	542.3–26
Methods	542.3–27
Digest	542.2–84–86
.....	542.5–34
Form-Based	542.2–89–92
.....	542.5–55
Process ?	542.2–90
Methods in Python Requests	542.5–34
Schemes	542.2–80
Token	542.2–87, 92
Windows	542.2–87–88
Automated Attacks	542.5–94
Automated Testing	542.5–92
AutoPWN	542.4–118
AWS	542.5–34
AXFR	542.1–34
Azure SQL	542.3–98

B

Backend Database	542.3–73, 96
Banner Grabbing	542.2–11–13
Base64	542.1–121
.....	542.2–81–82

.....	542.3–15
.....	542.5–33
Baseline	542.2–66
Bash	542.2–29
.....	542.3–38
Basic Auth → Authentication
Battering Ram	542.2–110
.....	542.4–98–99
Bcrypt	542.2–103–104
Binary Search	542.3–119
BIND	542.1–40–41
Version ?	542.1–41
Bing Directives	542.1–51–52
Black Box Testing ?	542.5–89
Blacklist Filters ?	542.4–76–77
Blind Command Injection	542.1–39
Blind Data Exfiltration	542.3–111–112
Blind Injection	542.3–40, 73
Blindness Degrees → SQL Injection
BlindShell	542.4–119
Blog Comment ?	542.4–57
Boolean Testing	542.3–88
Broken Image Injection	542.4–73, 90
Browser	542.1–29
Cache ?	542.1–96
Choice ?	542.1–29
Browser Exploits	542.4–114, 118
Brute Force	542.4–115
Bugtraq	542.1–8

C

CA	542.1–129
CAPTCHA	542.2–74
CDN	542.4–137
CERN	542.1–76
Certificate	542.1–128–129
CGI	542.2–31
Environment Variable	542.2–33
ChaosNet	542.1–41
CHS	542.1–145
Client XSS	542.4–64–65
Clipboard Stealing	542.4–114
CloudFlare Challenge	542.1–143
Cluster Bomb	542.2–112
CMS	542.5–71–72
CNAME	542.1–36, 43
Code Disclosure	542.5–54
Code Execution	542.3–45
Command and Control	542.5–70
Command Injection	542.3–37–40
Comment	542.3–85–87
Delimiters	542.3–86
Commented Code	542.2–58–61
Communications Planning	542.5–104
Concatenation	542.3–85, 87, 96
Concurrency Attack	542.2–108
Confidentiality	542.3–113

SANS SEC542 – Web Pen Testing & Ethical Hacking

Configuration	542.2-21
Default Pages	542.2-24
Flaws	542.2-27-28
CONNECT ?	542.1-94
Connect Scan → TCP Connect Scan	
Content-Security-Policy → HTTP CSP Header	
Cookies	542.3-10, 15-16
.....	542.4-26, 29, 36
HttpOnly Flag ?	542.4-90-91
Scope ?	542.4-37
Secure Flag	542.4-90
Crawling	542.2-41
.....	542.5-64
Critical Finding	542.5-81
Cross-Site Scripting	542.4-35
→ XSS	
Crystal Box Testing	542.5-8, 90
CSP → HTTP CSP Header	
CSRF	542.2-88
.....	542.4-10, 116, 131
.....	542.5-6-12
Difference With XSS	542.5-7
Illustration	542.5-8-11
Prevention Cheat Sheet	542.5-6
Testing	542.1-116
Token	542.5-11
Characteristics	542.5-11
Working	542.5-11
CSS	542.4-28
.....	542.5-7
CVE	542.2-75

D

DAST	542.4-8
Data Attack	542.4-141
Data Exchange	542.4-6
Data Exfiltration	542.3-103, 110-113, 121, 131-132
.....	542.4-8
Database Metadata	542.3-97, 130
DB Columns Determination ?	542.3-108
DB Enumeration	542.3-130
DB Fingerprinting	542.3-96
DB2	542.3-97
Default Pages	542.2-21, 24
Default Vendor Credentials	542.1-58
Denial of Service	542.1-95
.....	542.4-8, 116
Development Process	542.5-90
Digest Auth → Authentication	
Direct Object References	542.2-27
Directory Indexing ?	542.2-73-74, 76
Directory Traversal	542.3-46-49
DjVu	542.5-82, 85
DLL Injection	542.1-130
DNS	542.1-33
Bruteforce Scan	542.1-35, 37, 43
Cache Snoop	542.1-68

Lookup	542.1-32
Nmap Script	542.1-42
Reconnaissance Tools	542.1-38
Reverse Scan	542.1-35-36
Tunnel	542.3-92
Zone Transfers ?	542.1-33-35
DNSSEC	542.1-43
Document Object	542.4-21, 25-26
DOM	542.4-21-22, 36-37
Nodes	542.4-22
Properties	542.4-89
DOM Event Handler Bypass	542.4-78-79
Drupal	542.5-63, 71-72
Drupalgeddon	542.2-28
.....	542.5-71, 73-76
Details	542.5-75
DTD	542.4-9, 12
DTLS	542.1-141

E

EDB → ExploitDB	
EDNS	542.1-33
Egress Filtering	542.3-45
Email Links	542.4-49
EMI	542.2-100
Encoding	542.3-47
ENTITY ?	542.4-12-15
Entropy	542.1-120
Entry Points ? → XSS Payload Delivery	
Error Messages (DB)	542.3-77-84
.....	542.4-146
EV	542.1-129
Eval	542.4-142
Exception Chaining	542.5-25
Executive Summary	542.5-108, 112
EXIF	542.2-53
ExploitDB	542.1-8, 53
External Entity	542.4-9
Externally Sourced Scripts ?	542.4-38-39

F

False Positive	542.2-25
.....	542.5-95
Favicon	542.2-25
Federated Identity Management	542.2-80
Fetch API	542.4-89
File Inclusion	542.3-44-50
Examples	542.3-47-48
Parameters	542.3-50
File Upload	542.3-115
Filter Bypass/Evasion	542.4-76-77, 83, 105
FIPS	542.1-120
Firewall	542.4-58
Forced Browsing	542.1-108
Form-Based Auth → Authentication	

SANS SEC542 – Web Pen Testing & Ethical Hacking

Forum Data	542.4–57
Framework	542.4–136–139
Frequency Search	542.3–119
FTP	542.1–77–78
Full Disclosure	542.1–8
Function Annotations	542.5–25
Fuzzable Values	542.2–108
FuzzDB	542.2–67
.....	542.4–84
Fuzzing	542.1–106, 108
.....	542.2–65–68, 108
Sources	542.2–67
.....	542.4–84

G

GHDB	542.1–53
.....	542.2–74
GML	542.1–76
.....	542.4–6
GnuPG	542.5–104
Google Cache	542.5–51
Google Directives	542.1–51–52
Google Dorks → GHDB	
GPU	542.2–102–103
Gray Box Testing	542.5–91
Grep Payloads	542.4–98, 100

H

Hackers for Charity	542.1–53
Heartbeat	542.1–141
PoC	542.1–144
Heartbleed	542.1–141–145
.....	542.2–28
.....	542.5–71
HFC	542.1–53
Hidden Form Fields → Session Tracking	
Hijacking Attack ? → Session Hijacking	
History Browsing	542.4–114–115
Hooked Browser	542.5–68
Hostname Harvesting	542.1–63
HPACK	542.1–82–83
HTAccess	542.2–81
HTDigest	542.2–86
HTML	542.1–76
.....	542.4–6
Comments	542.2–58
Injection	542.4–29–32, 79
Source	542.3–12
HTTP	542.1–76, 79–83
.....	542.3–6
Authentication → Authentication	
Content-Security-Policy Header	542.4–80
Host Header	542.1–81
.....	542.2–9
Methods Testing	542.2–20

Request	542.1–85
Methods	542.1–91–95
.....	542.2–21–23
Response	542.1–87
Status Codes ?	542.1–96–97, 125
Tunnel	542.1–94
.....	542.2–22
.....	542.3–92
HTTPOnly Cookie → Cookies	
HTTPS	542.1–103, 128–130
Accelerators	542.1–130
Target Support	542.1–133, 137
.....	542.2–9
Weaknesses → SSL Weaknesses	
Hybrid Testing	542.5–95

I

IBM	542.4–6
ICANN	542.1–33
ICMP	542.3–40
ICS	542.1–59
IDS	542.1–130
.....	542.2–6
.....	542.4–58, 84, 117
IFrame	542.4–118
IIS	542.2–24, 87
.....	542.3–46–47, 50
Indexing → Directory Indexing	
Inexpensive Hash Algorithms	542.2–102
Information Disclosure	542.3–45
.....	542.4–145–146
Information Gathering	542.5–91
Information Leakage	542.2–71–76
Types	542.2–72
Information Mapping	542.1–64
Information Schema ?	542.3–97–98, 130
Infracritical	542.1–59
Injection Context	542.4–72–75
Input Filtering → XSS Filtering	
→ Filter Bypass/Evasion	
Input Reflection	542.2–66
INSERT	542.3–69–70, 108
Instant Messaging	542.4–57
.....	542.5–104
Integrated Windows Auth → Authentication	
Integrity Hash	542.2–102
Inter-Protocol Stored XSS → XSS Stored	
Interactive Shell	542.3–115, 133
.....	542.5–70
Interception Proxies	542.1–28, 102–103
.....	542.4–97
Internal System Scanning	542.4–8
Internet Explorer ?	542.4–36
Interprotocol Exploitation	542.4–114, 119
IoT	542.1–56
IPSec	542.1–128
ISC	542.1–40

SANS SEC542 – Web Pen Testing & Ethical Hacking

ISP	542.1–31, 34–35
IWA	542.2–87
IXFR	542.1–34

J

Javascript	542.4–21–26, 32
Compiler	542.4–142
Framework Files	542.4–136
Injection	542.4–114
Objects Methods & Properties	542.4–23–24
Shell	542.4–92
Joomla	542.5–63, 71
JQuery	542.4–137
JSON	542.4–142–147
Exploitation	542.4–145
Format	542.4–144
Injection	542.4–147
Parser	542.4–142
Junyper	542.1–145

K

Kali	542.1–25
Kali-Web	542.1–26
Kerberos	542.1–77
.....	542.2–87
.....	542.5–34
Known Vulnerabilities	542.5–71
Known-Bad Characters	542.4–76–77

L

Large-Scale Script-Based Attack ?	542.4–56
LDAP	542.2–89
LFI ?	542.3–45
Load Balancing	542.1–87
.....	542.2–9
LOAD_FILE ?	542.3–113
Location Method	542.4–89
Log Mechanism	542.4–57
Logic Attack	542.4–136
.....	542.5–16–18
Login Attempt	542.2–83, 86

M

Manual Testing	542.5–92
Mash-Up	542.4–127
Proxy	542.4–129–130
Bypass ?	542.4–130
MDNS	542.1–43
MediaWiki	542.5–82–85
Metadata	542.1–61–62
Meterpreter	542.3–133
.....	542.5–70

MILNET	542.1–77
MITM	542.1–28, 103
.....	542.2–9, 86
MITRE	542.2–75
MooTools	542.4–137
MS SQL	542.3–90, 96–98, 100, 114, 121
.....	542.5–71
Multiplexing	542.1–82
Mutillidae	542.3–31–35
MySQL	542.3–90, 96–98, 100, 114, 121
.....	542.5–71

N

NameChk	542.1–71
NAT	542.1–77
NCP	542.1–31
Neophasis Labs	542.3–119
Network Share	542.1–62
Network Vulnerability Scanner	542.1–27
Nginx	542.2–73
NIDS	542.1–130
Nonce	542.2–84, 86
NoTCP → DNS Zone Transfers	
NSE	542.1–38, 42, 133, 135
DNS	542.1–42
NTLM	542.2–87
.....	542.5–34
Nudge Packet	542.2–11
NULL	542.3–107–109
Null Byte	542.3–49, 60
Null Cipher	542.1–134
NVD	542.1–8

O

OAuth	542.2–80
OAuth1	542.5–34
Off-the-Record → OtR	
OOB Metasploit Shell	542.3–133
OOB SQL Injection → SQL Injection	
OOB Stored XSS → Out-of-Band Stored XSS	
Open Source Info	542.1–49
OpenID	542.2–80
Oracle ?	542.3–96–98, 100, 108, 121
.....	542.5–71
ORDER BY ?	542.3–108
Origin of Trust	542.4–33
OS Command Injection	542.2–30
OS Fingerprinting	542.2–6, 11
OTG	542.1–15–17
Account Enumeration (IDENT-004)	542.2–96
App Architecture (INFO-010)	542.2–40
Command Injection (INPVAL-013)	542.3–37
CSRF (SESS-005)	542.5–6
Entry Points (INFO-006)	542.2–40
Execution Paths (INFO-007)	542.2–40
Framework Fingerprinting (INFO-008) ..	542.2–40

SANS SEC542 – Web Pen Testing & Ethical Hacking

HTML Injection (CLIENT-003)	542.4–29
HTTP Methods/Verbs (CONFIG-006) ..	542.2–20
Information Leakage (INFO-005)	542.2–40
LFI/RFI (INPVAL-012)	542.3–44
SQL Injection (INPVAL-005)	542.1–16
Testing Categories	542.1–17
Unreferenced Files (CONFIG-004)	542.2–70
Weak SSL/TLS Ciphers (CRYPST-001)	542.1–132
Web App Fingerprinting (INFO-009) ..	542.2–40
Web Server Fingerprinting (INFO-002) ..	542.2–19
OtR	542.5–104
OTT	542.2–100
Out-of-Band Channel → SQL Injection	
Out-of-Band Stored XSS	542.4–58
OUTFILE	542.3–113
Output → Tool Output	
OWASP	542.1–13
Cheat Sheet	542.3–116
Resources	542.1–13
Top-10	542.1–14
.....	542.3–32
.....	542.4–8

P

Passive Scan	542.1–108
Password Guessing Attack	542.2–41, 97–98
Password Hash	542.2–102
Patching	542.5–72
Path Disclosure	542.5–54
Payload Delivery ? → XSS Payload Delivery	
PBKDF2	542.2–103
PDO	542.5–75
Pentesting → WebApp Pentesting	
[Black / Crystal (White) / Gray] Box ...	542.5–89
Pentesting Methodology	542.1–12
Server-side VS Client-side	542.1–12
PentestMonkey	542.3–116
Perl	542.3–38
Permission	542.1–58
Memo	542.5–107, 112
Persistent Inpu	542.4–57
PGP	542.5–104
PGP.Rediris	542.1–71
Phishing Attack	542.2–92
PHP Backdoor	542.5–84
PHP Data Objects → PDO	
PHPInfo	542.2–72, 74
PII	542.5–99
Pitchfork	542.2–111
PKI	542.1–128
PMTU	542.1–141
Port Scanner	542.2–6
Port Scanning	542.4–9, 114, 117
Post-Exploitation	542.3–133
.....	542.5–63
PostgreSQL	542.3–121
Pre-engagement Discussion	542.3–114

Prepared Statement	542.5–75
Privilege Escalation	542.3–114
.....	542.5–70, 73
Proxy Detection ?	542.1–93
.....	542.5–51
PTES	542.1–12
PTR	542.1–35–37, 41
Push Promise	542.1–82
PwnedList	542.1–72
Python	542.5–22–37
Data Types & Structures	542.5–29–31
Loops ?	542.5–30
Requests	
SSL/TLS ?	542.5–36
Requests ?	542.5–33–37
Versions	542.5–25
Web Libraries	542.5–32

Q

Quality of Protection	542.2–84
Query Stacking → Stacked Query	
Query String Formats	542.1–89
QUIC	542.1–84

R

Race Condition	542.2–108
Randomness Analysis	542.1–120
Ransomware	542.3–114
RCE	542.4–9
.....	542.5–73, 76
RDBMS	542.3–56, 97
Realm	542.2–81
Reconnaissance	542.1–67–68
.....	542.2–71
Redirection Flaw	542.1–115
Reflection ? → XSS Discovery Reflection Tests	
Regional Registrars	542.1–31
Remote Request Execution	542.4–8
Replay Attack	542.1–116
Reporting ? → WebApp Pentesting Mgt Report	
Request Initiation	542.4–114, 116
Response Splitting	542.5–53
RFC1945	542.1–80
.....	542.1–81
RFC2616	542.1–81
.....	542.4–97
RFC723[0-5]	542.1–81
RFC7540	542.1–82
RFI	542.3–45
.....	542.4–14
Robots	542.2–43
Exclusion Protocol	542.2–43
Reader	542.5–51
Round Trip Time	542.5–34
RPC	542.4–118

SANS SEC542 – Web Pen Testing & Ethical Hacking

.....	542.5–69
Rules of Engagement	542.3–114
→ WebApp Pentesting Mgt RoE	

S

Salt	542.2–84, 102
Same Origin	542.4–127–129
Policy → SOP	
SAML	542.2–80
SAMM	542.1–13
SamuraiWTF	542.1–25
SAST	542.4–8
SCADA	542.1–57, 59
.....	542.5–63
Schema Information → Information Schema	
Scope → WebApp Pentesting Mgt Scope	
Example	542.6–17
Screen Scraping	542.1–54
Script Injection	542.4–32, 79
Search Engines	542.1–50–54
Directives	542.1–51
SEC	542.1–145
SecLists	542.2–67
Secure Cookie → Cookies	
Security Zone	542.4–36
Security542	542.1–25
Server Profiling	542.2–9–15
Server XSS	542.4–65
Service Version	542.2–7
Session	542.3–6
Abuse	542.4–87–92
Fixation	542.3–23–24
Hijacking	542.3–22
.....	542.4–88
.....	542.5–76
Theft Without Redirection	542.4–90
Token	542.4–88
Gathering	542.3–15–22
Predictability	542.3–18
Tracking	542.3–7–13
Cookies	542.3–10
Hidden Form Fields	542.3–12
URI Parameters	542.3–11
Types	542.3–8
SGML	542.1–76
.....	542.4–6
Shell Controller	542.4–92
Shellcode	542.5–70
Shellshock	542.2–28–36, 110
.....	542.5–71
Injection	542.2–32–35
Shunning	542.1–67
.....	542.2–74
.....	542.4–84
Side-Channel Attack ?	542.2–100–104
SIEM	542.4–58
Signatures	542.2–11

Sniffer	542.1–103
Sniper	542.2–109
.....	542.4–98, 102
SO Injection	542.1–130
SOAP	542.1–54, 125
Social Engineering	542.3–24
.....	542.4–56, 63, 88
Social Networks	542.1–55
SOP	542.4–33–40
Bypass	542.4–39–40, 129
Enforcement	542.4–36–37
Requirements ?	542.4–35
Test Cases	542.4–36–39
Source Identifier	542.5–102
Spidering	542.1–108
.....	542.2–40–53
.....	542.3–124
.....	542.4–103, 138
.....	542.5–46, 51, 63–64
Methods	542.2–42
Results	542.2–57–61
Spoofing	542.2–92
SQL	542.3–55–60
Data Types	542.3–59
Injection ?	542.3–54–133
Balancing	542.3–67–70
Blind	542.3–73, 76
Blindness Degrees	542.3–77–84, 89–91
Cheat Sheets	542.3–116
Classes	542.3–74
Example	542.3–61–66
.....	542.5–73
Fromless Select	542.3–106–107
In-Band/Inline	542.3–75, 99
Location	542.3–73
OOB	542.3–91
Out-of-Band Channel	542.3–91
Potential Attacks	542.3–114
Tools	542.3–118
.....	542.5–71
Union-Based	542.3–104–110
Query Modifiers	542.3–58
Special Characters	542.3–60
Verbs	542.3–57
SQL Server → MS SQL	
SQLite	542.3–97, 121
SSL	542.1–94, 128
Labs	542.1–136
Testing	542.1–134
Testing ?	542.1–128, 133–134, 137
Weaknesses	542.1–137
SSO	542.5–100
SSRF	542.4–9–10
Stacked Query	542.3–100–103, 115
Stateless	542.3–6
Stored Procedure	542.3–114
Stored XSS → XSS	
SubStr	542.3–113

SANS SEC542 – Web Pen Testing & Ethical Hacking

SXSS	542.4–45
SYN Scan → TCP SYN Scan	
Synchronizer Token → CSRF Token	

T

TCO	542.2–99
TCP Connect Scan	542.2–6
TCP SYN Scan	542.2–6
Technology Detection	542.2–46–49
Telnet	542.1–77
TEMPEST	542.2–100
Tim Berners-Lee	542.1–76
Timing Attack	542.2–101–104
.....	542.5–37
Timing Inference	542.3–90
TLD	542.1–33
TLS	542.1–128, 141
Versions ?	542.1–133
Token	542.2–87
Tool Output	542.5–112
Ingestion (in Metasploit)	542.5–65
Traffic Identifier	542.5–102
Transparent Proxy	542.5–51
Trust	542.1–129
Trusted Third Party	542.4–39
Type o XSS → XSS DOM-Based	

U

UDP	542.1–33
Unicode	542.3–46
UNION	542.3–69–70, 104–106, 108, 111
Prerequisites	542.3–105
URI	542.1–88
Parameters → Session Tracking	
URL Encoding	542.4–50–54
Encoded Inputs	542.4–55
User-Agent	542.1–85–86
Username Harvesting	542.1–61, 122
.....	542.2–97–99
.....	542.5–37
UXSS	542.4–45

V

Version Scanning	542.2–6, 10–11
Virtual Host	542.1–78, 81
.....	542.2–9
Name-Based	542.2–9
VNC	542.3–133
.....	542.5–70
VoIP	542.1–56
VPN	542.1–128, 145
Vulnerability Scanner	542.5–41–42, 46

W

WAF	542.3–129
.....	542.4–83–84
Weak Hash Algorithms	542.1–137
Weak SSL/TLS Ciphers	542.1–132, 137
Web 2.0	542.1–9
.....	542.4–123, 127
Web Root	542.3–46–47, 50, 115
Web Server Capabilities	542.2–24
Web Shell	542.3–114–115
WebApp Pentesting	542.1–12
Exploits	542.5–71, 81
Hybrid	542.5–95
Management	542.5–98–104
Deliverables	542.5–103
Presentation	542.5–113
Reporting ?	542.5–106–112
Rules of Engagement	542.5–101
Scope	542.5–99–100, 109
Test Traffic Identification	542.5–102
Manual VS Automated	542.5–92–95
Methodology	542.1–16
Preparation	542.5–97
Toolkit	542.1–24–29
Types	542.5–89–91
WebApp Scanner	542.1–27
.....	542.5–46
Webcam	542.1–56
WebDAV	542.1–91, 95
.....	542.2–22
WebSec	542.3–116
WebSocket	542.1–124–126
White Box Testing → Crystal Box Testing	
Whitelist Filters	542.4–76
Whois ?	542.1–31–32
Lookup	542.1–32, 36
Windows OS Authentication	542.2–87
Windows Registry	542.3–114
WordPress	542.5–41–42, 63, 71

X

X-Powered-By	542.2–12
X.509	542.5–36
XML	542.4–6–11, 542.4–142
Parser/Processor	542.4–9
XMLHttpRequest	542.4–123–126, 128, 138
XMPP	542.1–125
XSRF → CSRF	
XSS	542.2–88
.....	542.4–28, 35, 41
Auditor	542.4–82
Backdoor	542.4–92
Classes	542.4–45, 65
Difference With CSRF	542.5–7
Discovery	542.4–42–43, 69
Filter Test	542.4–76
Reflection Test	542.4–71, 98–109
DOM-Based	542.4–63–65

SANS SEC542 – Web Pen Testing & Ethical Hacking

Filtering	542.4-43, 79-80, 83
Fuzzing	542.4-69, 84
Injection Context	542.4-72-75
Injection Points	542.4-70, 99
Non-Persistent → Reflected	
Payload Delivery ?	542.4-49, 57
Persistent → Stored	
PoC Payloads	542.4-69, 84, 86
Reflected	542.4-46-55, 71
Illustration	542.4-47-49
Stored	542.3-114
.....	542.4-56-62, 71
Illustration	542.4-59-60

Inter-Protocol	542.4-61-62
Testing	542.1-104
→ Discovery	
Tools	542.4-96
Xssed	542.1-8
XXE	542.4-8-17
Blind	542.4-16-17
Examples	542.4-12-15, 17

Z

Zombie	542.4-112-114, 116-117
--------------	------------------------