| A | Accept header, fingerprinting and, 250–252 |
| ActionScript, 401 |
| ActiveFax exploitation BeEF bind, 590–592 |
| IPE (Inter-protocol Exploitation), 574–579 |
authentication detection, 436–440
web app attacks, 610
AVM (ActionScript Virtual Machine), 401
avpop( ) function, 215

B
BackFrame, 151–152
background page, extensions, 325
baiting for phishing attacks, 57–58
Base64 encoding, detection evasion, 111–113
BEAST attack, 227–278
BeEF (Browser Exploitation Framework), 46
changeFavicon( ) method, 186
e-mail phishing, 55–56
Get System Info, 517
Metasploit and, 302–304
plugin detection, 380–382
QR code generation, 57–58
Tunneling Proxy, 152
website cloning, 50–51
BeEF bind, 579–580
ActiveFax exploitation, 590–592
IMAP exploitation, 585–590
Linux32 Stage, 584–585
Linux32 Stager, 584–585
TrixBox exploitation, 590–592
as web shell, 596–599
Win32 Stage, 582–584
Win32 Stager, 580–581
BeEF_bind command, 588–589
beef.browser.
  changeFavicon( ) function, 198–199
beef.browser.
  hoodChildFrames( ) function, 196–197
beef.logger.keypress( ) function, 190
beef.logger
  .push_stream( ) function, 191
beef.logger.submit( ) function, 195–196
beef.net.send( ) function, 191
beef.net.send( ) method, 184–185
begin_countdown function, 198–199
BHOs (Browser Helper Objects), 330–331
bind( ) method, 515–516
bind shell communications, IPC and, 554–558
blind XSS detection, 465–468
Blink, 7
blocked plugins, 376–377
blur event, 188–189
Bracket Expansion feature, IPE (Inter-protocol Exploitation), 569
browser APIs, 372
SOP bypassing, 175–178
Browser Autopwn (Metasploit), 300–301
browser bugs, 249
browser events, persistence and, 98–101
browser hacking methodology, 22–28
browser history
SOP and, 133–134
SOP bypassing
  cache timing, 172–175
CSS colors, 170–171
browser hooking, 78–79
browser sandboxing, 15–16
browsers
  attacking, 26
  privileges, 3–4
bug bounties, 248
bugs, fingerprinting and, 258
Burp Suite, 477–480
bypassing Click to Play, 382–388
bypassing cookie protections, 260
attributes
  Expires, 263
  HttpOnly flag, 263–264
  Path, 264–265
  Secure flag, 264–265
cookie jar overflow, 268–270
path attribute restrictions, 265–267
Set-Cookie response header, 261–262
Sidejacking attacks, 271–272
tracking with cookies, 270–271
bypassing CSP, 344–346
bypassing HTTPS certificates fake, 276
validation flaws, 276–227
downgrading to HTTP, 272–276
JavaScript
encryption attacks, 283–286
heap exploitation, 286–293
scheme abuse, 278–279
iOS, 279–281
Samsung Galaxy, 281–283
SSL/TLS layer attack, 227–278
bypassing port banning, 532–537
bypassing sandbox, Java plugins, 395
bypassing SOP
Adobe Flash, 141–142
Adobe Reader, 140–141
browser APIs and, 175–178
browser history and cache timing, 172–175
CSS colors, 170–171
cloud storage, 149–150
exploiting bypasses, 151–178
Firefox, 144–145
Internet Explorer, 142–143
Java, 134–140
Opera, 145–149
proxying requests, 151–153
Safari, 143–144
Silverlight, 142
UI redressing attacks and, 153–154
Clickjacking, 154–160
Cursorjacking, 160–164
drag&drop, 167–170
Filejacking and, 164–167
XCS and, 346–350
security model, 326–330
source code, 322–323
UI pages, 325
Web Store, 328
malicious extensions, 220–221
modeless dialogs and, 205
Web Store, extensions, 328
Chrome Developer Tools window, 322
Chrome:// scheme, 5
Chrome:// zone, 314, 321
_c.killClippy() function, 222
Click to Play, 374–376
bypassing, 382–388
Clickjacking anti-XSRF tokens, 154–157
IFrames, 157–160
clickLink() function, 103
client-server model, 4
Clippy, 221–223
clippy controller, 222–223
cloning websites, 50–51
closures, 81
cloud, SOP, bypassing, 149–150
commands
BeEF_bind, 588–589
netstat, 590
remote execution, 356–359
communication techniques, 79–80
CORS (cross-origin resource sharing), 83–84

C

caching
exploiting, 72
timing, SOP bypass and, 172–175
callee property, 122–124
calling plugins, Click to Play, 374–376
Camera class, 402–403
CAPTCHA, fake windows, 206–208
CBC (Cipher-Block-Chaining) encryption mode, 227–278
CDNs (Content Delivery Networks), 239
CERT/CC (Computer Emergency Response Team Coordination Center), 33
certificates fake, 276
validation flaws, 276–227
changeFavicon() method, 186
checkComplete() function, 463, 522
Chrome
AdBlock extension, 353
Developer mode, 322
extensions, 321–322
background page, 325
content scripts, 324–325
CSP (Content Security Policy), 329–330
fingerprinting, 331–332
Isolated Worlds, 327
manifest.json file, 323–324
match patterns, 327
NPAPI plugins, 326
permissions, 327–328
security boundary, 328–329

C
DNS tunnel communication, 89–95
messaging, 86–89
WebSocket, 84–86
XMLHttpRequest object, polling and, 80–83
compromised web applications, 46
concurrency, web workers and, 11
Connection header, fingerprinting and, 250
console.log( ) call, 460–461
contact harvesting, 54
content defacing, 183–184
retrieving from cross-origin, 136
scripts, Chrome, 324–325
Content-Type header, 373
control encrypted communication, 20–21
retention, 78–79
surrendering, 20
TCP protocol control, 20
converting, variables to strings, 184
cookiejar file, 262
cookies non-cookie session tracking, 230–231
protection bypass, 260
attributes, 263–265
cookie jar overflow, 268–270
path attribute restrictions, 265–267
Set-Cookie response header, 261–262
Sidejacking attacks, 271–272
tracking with cookies, 270–271
secure cookie flag, 13
theft, XSS and, 475
_c.openBubble( ) function, 222
CORS (cross-origin Resource sharing), 9–10, 83–84
SOP and, 131–132
cr-gpg Chrome extension, 360–361
CRIME attack, 227–278
cross-origin requests, web app attacks, 422
enumerating quirks, 422–425
preflight requests, 425
Cross-site Scripting, 6
Reflected Cross-site Scripting, 15
CSP (Content Security Policy), 13, 329–330
bypassing, XCS and, 344–346
CSS (cascading style sheets), 6
colors, SOP bypass and, 170–171
Cursorjacking, 160–164
defacing content, 183–184
default deny, 606
detachApplet( ) function, 530
Detect Tor module, 232–233
detection authentication, 436–440
internal domain name enumeration, 427–429
intranet device IP addresses, web app attacks and, 426–427
Java, 389–391
plugins automatic, 379–380
in BeEF, 380–382
resources, 447
detection evasion encoding Base64, 111–113
non-alphanumeric JavaScript, 115–116
Whitespace, 113–114
obfuscation, 116
callee property, 122–124
JavaScript engine quirks, 124–125
methods, 117–119
mixing content, 121–122
object notation mixing, 119–120
time delays, 120–121
variables, 117–119
Developer mode, Chrome, 322
Diminutive XSS Worm Replication Contest, 42–43
DirBuster, 446
displayPhishingSite( ) function, 212
distributed port scanning, 539–542
<div> elements, invisible, 333
DNS hijack, 493–494
DNS poisoning, 70–71
DNS prefetching, 89–90
DNS requests, forcing, 233
DNS tunnel communication, 89–95
document.domain property, 131
documents, embedding, overlay IFrame, 98
DOM (document object model), 7
event handlers, XCS and, 354–355
fingerprinting and, 249, 253
extensions, 332–335
property existence, 253–257
property values and, 257–258
SOP and, 130–131
DOM XSS, 33, 37–39
domain names, internal, enumeration, 427–429
DoS (Denial-of-Service) attacks
hash collision, 487–488
parseDouble( ) function, 488–489
web app attacks, pinch points, 487–489
drag&drop, SOP bypassing and, 167–170
E
EFF (Electronic Frontier Foundation), 230
e-mail phishing, 48, 54–57
embedded device command execution
firmware replacement, 504–508
pre-authentication RCE, 502–504
embedding documents, overlay IFrame, 98
EM-WebSocket, 85
encoding, detection evasion
Base64 encoding, 111–113
non-alphanumeric JavaScript, 115–116
WhiteSpace, 113–114
encrypted communication, 20–21
encryption, JavaScript attacks, 283–286
endTalkBack field, 556–557
Ettercap, 65–69
HTTP downgrade and, 272–273
event flows
event bubbling, 187–188
event capturing, 187–188
events
attachEvent( ) function, 188
focus, input capture and, 188–189
form events, 195–196
keyboard, input capture and, 190–192
keydown, 190
keypress, 190
keyup, 190
mouse, input capture, 192–195
mousedown, 194
mouseup, 194
onbeforeunload, 99–100
persistence and, 98–101
pointer, input capture, 192–195
Evercookie, 230–231, 271
evolution, 12–13
HTTP headers
CSP (Content Security Policy), 13
HttpOnly flag, 13
secure cookie flag, 13
strict-transport-security, 14
X-content-type-options, 14
X-Frame-Options, 14
execute_commands( ) function, 82–83
exec_wrapper( ), 81
Expires attribute, 263
exploiting
ActiveX, 404–408
caching, 72
Java, plugins, 396–400
media players, 413–415
Metasploit, 293–304
Extended HTML Form attack, 533–534
extension attacks, 26
Chrome, 321–322
background page, 325
content scripts, 324–325
CSP (Content Security Policy), 329–330
Isolated Worlds, 327
manifest.json file, 323–324
match patterns, 327
NPAPI plugins, 326
permissions, 327–328
security boundary, 328–329
security model, 326–330
source code, 322–323
UI pages, 325
Web Store, 328
fingerprinting
DOM and, 332–335
Firebug example, 334–335
HTTP headers and, 331–332
manifest.json file, 335–336
Firefox, 314–315
directory structure, 315–316
source code, 315–317
updates, 316–317
XBL and, 317
XPCOM API, 317–320
XUL and, 317
impersonating, 336–339
OS command
execution, 355–359
OS command injection, 359–364
XCS (Cross-context Scripting), 339–355
extensions, 311
versus add-ons, 313
IE (Internet Explorer), 330–331
versus plugins, 312–313
plugins comparison, 372–373
privileges, 313–314
Internet zone, 314
privileged browser zone, 314
external security perimeter, 22
EXTRACT exploitation,
IPE (Inter-protocol Exploitation), 569
F
Fake Flash Update, 217–221
fake login prompts, 209–210
fake software updates, 213–221
fetch function, 109
fetchonclick function, 109
field testing, 606
FIFO (Fast In First Out), 83
file formats, plugins, 373
file:// scheme, 5
Filejacking, 164–167
filters, evasion, XSS and, 468–469
findClass( ) method, 395
fingerprinting, 248–249
bugs, 258
DOM and, 249, 253
property existence, 253–257
property values and, 257–258
extensions
DOM and, 332–335
Firebug example, 334–335
HTTP headers and, 331–332
manifest.json file, 335–336
HTTP headers and, 249–253
non-HTTP services, 542–544
plugins
detecting in BeEF, 380–382
detecting plugins, 377–379
quirks and, 259–260
web app attacks, 429–436
finish( ) function, 463
fireAppletSSV Validation( ) method, 385–386
Firefox, fingerprinting extensions, 334–335
Firefox
Click to Play bypass, 382–388
extensions, 314–315
directory structure, 315–316
source code, 315–317
updates, 316–317
XBL and, 317
XPCOM API, 317–320
XUL and, 317
Firesheep, 271–272
jemalloc, heap exploitation and, 287–288
JRE (Java Runtime Environment), 375
login manager, 318–320
memory, heap exploitation and, 288–289
remote command execution, 356–359
security model, 320–321
SOP, bypassing, 144–145
UAF vulnerability, 289–293
Firefox Extension Dropper, 219
Firesheep, 271–272
firewalls, WAF
(Web Application Firewalls), 44
Firmware Modification Kit, 506
firmware replacement RCe, 504–508
Flash
Clickjacking, 241
plugins
ActionScript, 401
fuzzing, 403
microphone, 402–403
Shared Objects, 400–401
webcam, 402–403
web app attacks, 482–487
FlexPolicyServer.java class, 484–485
focus( ) method, 188–189
focus event, 188–189
focus events, input capture and, 188–189
forge_request, 471–472
form events, input capturing, 195–196
fullscreen attacks, 199–204
functions
addEventListener( ), 188
anonymous, 83
attachApplet( ), 530
attachEvent( ), 188
avpop( ), 215
beef.browser.
  changeFavicon( ), 198–199
beef.browser.hoodChildFrames( ), 196–197
beef.logger
.keypress( ), 190
beef.logger.push
  _stream( ), 191
beef.logger.submit( ), 195–196
beef.net.send( ), 191
begin_countdown, 198–199
checkComplete( ), 463, 522
_c.killClippy( ), 222
clickLink( ), 103
_c.openBubble( ), 222
decode_whitespace, 114
detachApplet( ), 530
displayPhishingSite( ), 212
DoS (Denial-of-Service) attacks
  parseDouble( ), 488–489
  execute_commands( ), 82–83
fetch, 109
fetchOnclick, 109
finish( ), 463
getAliveHosts( ), 530
getComputedStyle, 230
getFormActions( ), 448–450
getLinks( ), 447–450
grayOut( ), 214
isSameOrigin( ), 447
loadpopunder( ), 206
log( ), 485
logoutGoogle( ), 212
on( ), 188–189
onBeforeSend
  Headers, 332
overriding, JavaScript, 285–286
parseDouble( ), 488–489
parseFromString( ), 449
performComplicatedBackgroundFunction( ), 198–199
poll( ), 81
postMessage( ), 491–492, 527
post_msg( ), 87
receiveMessage( ), 87
redirect_to
  _malware( ), 117
redirect_to_site( ), 117
sendAsBinary( ), 500–501, 553–554
setInterval( ), 111–113, 120–121
setRequestHeader, 332
setTimeout( ), 111–113, 120–121
spawnWorkers( ), 463–465
stopPropagation( ), 100
swfobject
  .embedSWF( ), 236–237
timer( ), 121
whitespace
  _encode( ), 113
  window.stop( ), 522
fuzzing, Flash, 403

G
Gecko, 7, 8
gerolocation, 9
Get Physical Location module, 233–234
Get Stored Credentials module, 236
getAliveHosts( ) function, 530
getAllLogins( ) method, 318
getComputedStyle function, 230
getFormActions( ) function, 448–450
getHostAddress( )
    method, 515–516
getHostName( )
    method, 515–516
getInfo( )
    method, 135
getLinks( )
    function, 447, 448–450
getLocalAddress( )
    method, 515–516
Glassfish, 497–501
Gmail, phishing, 212–213
Golden Hour of Phishing Attacks, 58
Google, Safe Browsing API, 58–59
Google Analytics Opt-out Browser, 313
grayOut( )
    function, 214
Groovy Shell Server exploitation, 568–569

H
handshake, SDP (Session Discovery Protocol) and, 518
hash collision DoS, 487–488
heap exploitation, JavaScript
Firefox example, 289–293
Firefox memory, 288–289
jemalloc (Firefox), 287–288
memory management, 286–287
heap spraying, 289
Hidden Service Protocol, 231
history, SOP and, 133–134
history manipulation, 11
hooked browsers, 32, 78–79
DDoS (Distributed Denial-of-Service) attacks, 489–493
internal IP, network attacks and, 514–519
subnet, network attacks and, 520–523
web app attacks and, 472–474
bypassing HttpOnly, 474–477
HTAs (HTML Applications), tricks, 215–216
HTML (HyperText Markup Language), 5
HTML5, 10
HTTP (Hypertext Transport Protocol), downgrading to, 272–276
HTTP headers, 5
CSP (Content Security Policy), 13
fingerprinting and, 249–253
extensions, 331–332
HttpOnly flag, 13
secure cookie flag, 13
size calculation, IPE and, 565–567
strict-transport-security, 14
X-content-type-options, 14
X-Frame-Options, 14
HttpOnly flag, 13, 263–264
bypassing, 474–477
HTTPS, bypassing certificate validation flaws, 276–277
downgrading to HTTP, 272–276
fake certificates, 276
JavaScript attacks, 283–293
scheme abuse, 278–283
SSL/TLS layer attack, 227–278

I
ICE (Interactive Connectivity Establishment) framework, 518–519
idle_timer variable, 198–199
IE (Internet Explorer), extensions, 330–331<br>iframe tag, 96–98
IFrames
Clickjacking and, 157–160
key logging, 196–197
persistence, 96–98
sandboxing, 16
images, requests, 430–432
IMAP exploitation BeEF bind, 585–590
IPE (Inter-protocol Exploitation), 569–574
IMEI (International Mobile Station Equipment Identity), 281–283
IMG tags, port scanning and, 537–539
Immunity/WinDBG debugger plugin, 577
impersonating extensions, 336–339
InetAddress object, 515–516
initAppletAdapter( )
    method, 385
Initiating Control phase, 31
advertising networks, 46–47
compromised web applications, 46
hooking, 32
MitM (Man-in-the-Middle) attacks, 59–60
ARP spoofing, 64–70
DNS poisoning, 70–71
exploiting caching, 72
MitB (Man-in-the-Browser) attack, 60–61
wireless attacks, 61–64
social engineering attacks, 47–48
phishing attacks, 48–57
XSS (Cross-Site Scripting) attacks, 32–33
control bypassing, 43–45
DOM XSS, 33, 37–39
Reflected XSS, 33, 34–35
Stored (Persistent) XSS, 33, 35–37
Universal XSS, 33, 39–40
viruses, 40–43
innerHTML property, 184
input, capturing, 187–188
focus events and, 188–189
form events, 195–196
IFrame key logging, 196–197
keyboard events, 190–192
mouse events, 192–195
pointer events, 192–195
internal domain name enumeration, 427–429
Internet Explorer
addEventListener( ) function, 188
modeless dialogs and, 205
SOP, bypassing, 142–143
Internet zone, 314
intranets, device IP address detection, 426–427
iOS, scheme abuse, 279–281
IP addresses internal, hooked browsers, 514–519
intranet devices, detection, 426–427
IPC (Inter-protocol Communication), 513
bind shell example, 554–558
data encapsulation and, 553–554
error tolerance, 552
fingerprinting non-HTTP services, 544
IMAP example, 562–564
IRC example, 559
network attacks and, 549–564
printer service example, 559–562
ipc_posix_window, 556
IPE (Inter-protocol Exploitation), 513
HTTP header size calculation, 565–567
network attacks and, 564–565
examples, 567–579
IRC NAT pinning, 545–549
Isolated Worlds (Chrome), 327
isSameOrigin( ) function, 447

J
jar URIs, 138–139
Java
applets, signed, 223–228
cross-origin requests, 134–137
Meterpreter, 399–400
ping sweeping and, 528–531
plugins
applets, 388–389
detecting, 389–391
exploiting, 396–400
reversing applets, 391–395
sandbox bypass, 395
SOP, bypassing, 134–140
Java Applet module, 225–228
Java Payload, 224–225
JavaScript, 6
closures, 81
encryption, attacks, 283–286
heap exploitation
Firefox example, 289–293
Firefox memory, 288–289
jemalloc (Firefox), 287–288
memory management, 286–287
keyboard events, 190–192
non-alphanumeric, detection evasion and, 115–116
obfuscation and engine quirks, 124–125

PDFs
  browser launch, 409–410
  UXSS, 408–409

JBoss, JMX remote command execution, 495–497

JD-GUI, 391

ejemalloc heap (Firefox), 287–288

Jikto, 42

JMX (Java Management Extensions Console), remote command execution, 495–497

JNLP (Java Network Launching Protocol), 386

jQuery, event handling, 188–189

JRE (Java Runtime Environment), 375

JVM (Java Virtual Machine), 389

K

KARMA suite, 64

key values, W3C specifications, 191

keyboard events, input capture and, 190–192

keydown event, 190

keypress event, 190

keyup event, 190

kill bits, ActiveX plugins, 376

L

LastPass password manager, 333–334

impersonating extension, 337–339

layout engines, 7. See also rendering engines; web browser engines

LIFO (Last In First Out), 83

Linux, DNS poisoning, 71

Linux32 Stage, 584–585

Linux32 Stager, 584–585

loadpopunder() function, 206

local storage, 9

log( ) function, 485

login, fake prompts, 209–210

login manager, Firefox, 318–320

logoutGoogle() function, 212

Lucky 13 attack, 227–278

M

m0n0wall, remote command execution, 501–502

MAC address filtering, wireless attacks, 62

makeFile() method, 320

malaRIA framework, 482–487

malicious extensions, 219–221

Malicious.class applet, 375

malware, 16

obfuscation and, 117–119

manifest.json file Chrome extensions, 323–324

fingerprinting extensions, 335–336

markup languages
  HTML (HyperText Markup Language), 5
  SGML (Standard Generalized Markup Language), 5
  XML (eXtensible Markup Language), 6

match patterns, Chrome, 327

MC-WorX ActiveX plugin, 404

media plugins
  media player exploit, 413–415
  resource scanning, VLC and, 410–413

memory management, JavaScript, heap exploitation, 286–287

messaging, 86–89

Metasploit, 293–304

ActiveX, 404–405

media players, 413–415

Meterpreter, 399–400

ActiveX exploit, 405

methodology, browser hacking, 22–28

methods
  beef.net.send(), 184–185
  bind(), 515–516
  changeFavicon(), 385–386
  focus(), 188–189
  getAllLogins(), 318
  getHostAddress(), 515–516
  getHostName(), 515–516
  getInfo(), 135
  getLocalAddress(), 515–516
  initAppletAdapter(), 385
makeFile(), 320
obfuscation and, 117–119
performSSV
Validation(), 386–387
toString(), 184
window.open(), 102
microphone
controlling, 236–242
Flash, 402–403
MitB (Man-in-the-
Browser) attack, 60–61
versus MitM (Man-in-
the-Middle)
attacks, 105
persistence and, 104–110
MitM (Man-in-the-
Middle) attacks, 59–60
ARP spoofing, 64–70
DNS poisoning, 70–71
exploiting caching, 72
MitB (Man-in-the-
Browser) attack, 60–61
versus MitB (Man-
in-the-Browser)
attacks, 105
wireless attacks, 61–64
XCS (Cross-context
Scripting), 339–344
mixed content, 17
MobileESP project,
252–253
modal notifications, user
attacks and, 204–223
modeless dialogs, 204–205
mouse events, input
capture, 192–195
mousedown event, 194
mouseenter event, 194
mouseleave event, 194
mousemove event, 194
mouseout event, 194
mouseover event, 194
mouseup event, 194
MySpace, Samy worm,
41–42

N
NAT Pinning, 545–549
netstat command, 590
NetStream class, 402
network attacks, 27, 513
BeEF bind, 579–580
ActiveFAX
exploitation, 590–592
IMAP exploitation,
585–590
Linux32 Stage,
584–585
Linux32 Stager,
584–585
TrixBox exploitation,
592–596
Win32 Stage, 582–584
Win32 Stager, 580–581
Extended HTML Form
attack, 533–534
IPE (Inter-protocol
Exploitation), 564–565
time delays, 120–121
distributed scanning,
539–542
IMG tags and, 537–539
port banning bypass,
532–537
target identification
internal IP of hooked
browser, 514–519
subnet of hooked
browser, 520–523
non-cookie session
tracking, 230–231
notation, mixing,
obfuscation and, 119–120
NPAPI (Netscape
Plugin Application
Programming
Interface), 372
Chrome extensions
and, 326
nsIFileOutputStream
interface, 319
nsILocalFile
interface, 320
nsILoginManager
interface, 318
nsIProcess
interface, 320

O
Oberheide, Jon, 33
obfuscation
callee property,
122–124
detection evasion, 116
JavaScript engine
quirks, 124–125
methods, random,
117–119
mixing content, 121–122
object notation mixing,
119–120
time delays, 120–121
variables, random, 117–119
on( ) function, 188–189
onBeforeSendHeaders function, 332
onbeforeunload event, 99–100
Opera, SOP, bypassing, 145–149
Oracle, padding attacks, 278
OS, commands
extension attacks, 355–359
injection, 359–364
OS X, DNS poisoning, 71
OSI model, Application Layer, 513
overlay IFrames, 96–98
PacketFu library, 68
padding Oracle attacks, 278
parseDouble( ) function, 488–489
parseFromString( ) function, 449
password manager attacks, 234–236
LastPass, 333–334
impersonating extension, 337–339
passwords, reset, XSRF, 443–444
Path attribute, 264–265
PDF readers, plugins, JavaScript in PDFs, 408–410
perform
Complicated Background Function( ) function, 198–199
performSSVValidation( ) method, 386–387
permissions, Chrome, 327–328
persistence
browser events, 98–101
detection evasion, 110
encoding and, 111–116
obfuscation, 116–125
IFrames, 96–98
MitB (man-in-the-browser) attacks, 104–110
pop-under windows, 101–104
Persistent XSS. See Stored (Persistent) XSS
phishing, 16, 48–57
anti-phishing controls, 58–59
baiting, 57–58
bouncer phishing kit, 59
definition, 47
e-mail phishing, 48, 54–57
Gmail, 212–213
Golden Hour of Phishing Attacks, 58
spear phishing, 47, 48
website phishing, 48, 49–54
whaling, 48
pinch points, web app attacks, 487–489
ping sweeping
Java and, 528–531
XMLHttpRequest and, 523–528
plugin attacks, 27
ActiveX controls, 403
exploiting ActiveX, 404–408
attack surface, 19–20
blocked, 376–377
browser API, 372
calling, Click to Play, 374–376
Click to Play, bypassing, 382–388
detecting, automatic, 379–380
fingerprinting
detecting in BeEF, 380–382
detecting plugins, 377–379
Flash
ActionScript, 401
fuzzing, 403
microphone, 402–403
Shared Objects, 400–401
webcam, 402–403
Java
applets, 388–389
detecting, 389–391
exploiting, 396–400
reversing applets, 391–395
sandbox bypass, 395
kill bits, 376
media
media player exploit, 413–415
resource scanning, VLC and, 410–413
PDF readers, JavaScript in PDFs, 408–410
script API, 372
Plugin2Manager class, 385
PluginDetect framework, 379–380
PDF readers, JavaScript in PDFs, 408–410
script API, 372
Plugin2Manager class, 385
PluginDetect framework, 379–380
plugins, 372
versus extensions, 312–313
extensions comparison, 372–373
file formats, 373
SOP and, 132–133
standard programs
comparison, 374
pointer events, input
capture, 192–195
poll( ) function, 81
polling, 79
XMLHttpRequest
object, 80–83
pop( ) function, 81
populate_global
_vectors( ) function, 454–455
pop-under windows,
101–104, 205–206
port banning, bypassing,
532–537
Port Scanner module, 540
port scanning, 531–532
distributed, 539–542
IMG tags and, 537–539
port banning bypass,
532–537
Postel's Law, 21
postMessage( )
function, 491–492, 527
post_msg( ) function, 87
pre-authentication RCE,
503–504
preflight requests, web
app attacks, 425
Presto, 8
Pretty Theft, 210–211
privacy attacks, 228–230
anonymization bypass,
231–234
microphone control,
236–242
non-cookie session
tracking, 230–231
password managers,
234–236
webcam control,
236–242
private browsing, 229
privileges, 313–314
browsers, 3–4
Internet zone, 314
privileged browser
zone, 314
properties, DOM,
fingerprinting and,
253–258
proxies
HttpOnly bypass,
475–477
SOP bypassing and,
151–153
PsyBot, 504
Q
QR (Quick Response)
codes, 57–58
quirks
erenumerating, web
app attacks and,
422–425
fingerprinting and,
259–260
R
ranges array, 521
RAW server, 574–576
raw TCP data, 553–554
RCE (Remote Command
Execution), 493
embedded device
firmware replacement,
504–508
pre-authentication
RCE, 503–504
Glassfish, 497–501
JMX (Java Management
Extensions
Console), 495–497
m0n0wall, 501–502
receiveMessage( )
function, 87
redirect_to_malware( )
function, 117
redirect_to_site( )
function, 117
Reflected Cross-site
Scripting, 15
Reflected XSS, 33,
34–35, 465
remote command
execution, Firefox
example, 356–359
rendering engines, 7.
See also layout engines;
web browser engines
Blink, 7, 8
Gecko, 7, 8
Presto, 8
Trident, 7, 8
WebKit, 7
Replace HREFS (HTTPS)
folder, 275
requests
images, 430–432
pages, 433–436
resource detection,
445–450
web app attacks, 447
RESTful API, 398–399
Retaining Control phase
control retention, 78–79
Retaining
Communication, 77
communication
techniques, 79–95
Retaining Persistence, 77
browser events,
98–101
detection evasion,
110–125
IFrames, 96–98
MitB (man-in-the-browser) attacks, 104–110
pop-under windows, 101–104
Robustness Principle, 21
rogue access points, 64
RTCPeerConnection, 518

S
Safari, SOP, bypassing, 143–144
Samsung Galaxy, scheme abuse, 281–283
Samy Worm, 41–42
sandbox bypass, 15
Java plugins, 395
sandboxing, 15
browser sandboxing, 15–16
IFrame sandboxing, 16
schemes, abuse, 278–279
iOS, 279–281
Samsung Galaxy, 281–283
script APIs, 372
scripting
Cross-site Scripting, 6
JavaScript, 6
VBScript, 6–7
scripts, Chrome, 324–325
SDP (Session Discovery Protocol), handshake and, 518
secure cookie flag, 13
Secure flag, 264–265, 272
security
CSP (Content Security Policy), 329–330
SOP (Same Origin Policy), 4–5
security mode, Firefox, 320–321
security model, Chrome extensions, 326–330
security software, 2–3
sendAsBinary( ) function, 500–501, 553–554
session storage, 9
SET (Social-Engineer Toolkit), 52
setTimeout( ) function, 111–113, 120–121
setRequestHeader function, 332
TabNabbing, 198–199
UI expectations
Clippy, 221–223
fake login prompts, 209–210
fake software updates, 213–221
Gmail phishing, 212–213
modeless dialogs, 204–209
Pretty Theft, 210–211
SOE (Standard Operating Environment), 2
software
security software, 2–3
updates, fake, 213–221
SOP (Same Origin Policy), 4–5, 21
baiting, 57–58
e-mail phishing, 48, 54–57
spear phishing, 48
website phishing, 48, 49–54
whaling, 48
SET (Social-Engineer Toolkit), 52
signed Java applets, 223–228
SignedObjects, 400–401
Shellcode, BeEF bind, 579–585
Shellcoder's Handbook, 12
Sidejacking attacks, cookies, 271–272
signed Java applets, 223–228
signedAppletCmdExec class, 392–393
Silverlight, SOP, bypassing, 142
Skype, iOS scheme, 279–280
SmartScreen Filter, 208–209
social engineering attacks, 47–48, 197–198
fullscreen attacks, 199–204
phishing attacks
anti-phishing controls, 58–59
phishing attacks
anti-phishing controls, 58–59
phishing attacks
anti-phishing controls, 58–59
Java, 134–140
Opera, 145–149
proxying requests, 151–153
Safari, 143–144
Silverlight, 142
UI redressing attacks and, 153–170
XCS and, 346–350
CORS and, 131–132
DOM and, 130–131
local storage, 9
overview, 130
plugins and, 132–133
purpose, 129
UI redressing and, 133
violation error, 138
SPAM, definition, 47
Spam Cookies button, 269–270
spawnWorkers( ) function, 463–465
sp_configure( ) stored procedure, 456
spear phishing, 47
spearhead phishing, 48
SPF (Sender Policy Framework), 52
Spider (Burp Suite), 478–479
spoofing, ARP Spoofing, 272–273
SQLi (SQL injection vulnerabilities), 450–465
Sqlmap, 480–482
SSID (service set identifier), wireless attacks, 61
SSL (Secure Socket Layer), 227
sslstrip tool, 68
SSL/TLS layer attacks, 227–278
static IP filtering, wireless attacks, 62
stopPropagation( ) function, 100
storage, 9
local storage, 9
session storage, 9
Stored (Persistent) XSS, 33, 35–37, 465
strict-transport-security, 14
strings, variables, converting, 184
STUN (Session Traversal Utilities for NAT), 518
SWF files, 236–237
swfobject.embedSWF( ) function, 236–237
syscall (Linux), 584–585
TabNabbing, 198–199
TCP protocol, control, 20
tel: handler, 279
time delays, obfuscation and, 120–121
timer( ) function, 121
TLS (Transport Layer Security), 227
tokens, anti-XSRF, 444–445
Tor network anonymization bypass, 231–234
DeepSearch, 231–232
Evercookie, 230–231
toString( ) method, 184
Trident, 7, 8
TrixBox exploitation, BeEF bind, 590–592
Tunneling Proxy, 152
web app attacks and, 469–472
TURN (Traversal Using Relays around NAT), 518
UA header, 249
UAF (Use After Free) vulnerability, Firefox, 289–293
UI pages, Chrome, 325
UI redressing SOP and, 133
SOP bypassing and, 153–154
Clickjacking, 154–160
Cursorjacking, 160–164
drag&drop, 167–170
Filejacking and, 164–167
Universal XSS, 33, 39–40
Unix, DNS poisoning, 71
updateKey parameter, 316–317
updates, software, fake, 213–221
updateURL parameter, 316–317
URLs, obfuscation, 34–35
user attacks, 26
input capturing, 187–188
focus events and, 188–189
form events, 195–196
IFrame key logging, 196–197
keyboard events, 190–192
mouse events, 192–195
pointer events, 192–195
privacy attacks, 228–230
anonymization bypass, 231–234
microphone control, 236–242
non-cookie session tracking, 230–231
password managers, 234–236
webcam control, 236–242
social engineering lure, 197–198
fullscreen attacks, 199–204
signed Java Applets, 223–228
TabNabbing, 198–199
UI expectations, 204–223
User-Agent header, fingerprinting and, 250
DOM property values, 257–258
USSD (Unstructured Supplementary Service Data), 281–283
UXSS (Universal XSS), JavaScript in PDFs, 408–409

V
validation, certificates, 276–227
variables converting to strings, 184
obfuscation and, 117–119
VBScript, 6–7
viruses, XSS, 40–41

Diminutive XSS Worm Replication Contest, 42–43
Jikto, 42
Samy Worm, 41–42
VLC (ActiveX), media plugin attacks, 410–413
VLC MMS Stream Handling Buffer Overflow, 413–415
vulnerabilities, 11–12 detection
SQLi (SQL injection vulnerabilities), 450–465
XSS (cross-site scripting), 465–469
RCE (Remote Command Execution), 493

W
WAF (Web Application Firewalls), 44
web app attacks, 413–415
authentication detection, 436–440
Burp Suite, 477–480
cross-origin requests, 422
eumerating quirks, 422–425
preflight requests, 425
detection
internal domain name enumeration, 427–429
intranet device IP addresses, 426–427

DoS attacks
DDoS (Distributed Denial-of-Service) attack, 489–493
parseDouble( ) function, 488–489
pinch points, 487–489
exploit launching
DNS hijack, 493–494
embedded device command execution, 502–508
Glassfish remote command execution, 497–501
JBoss JMX remote command execution, 495–497
m0n0wall remote command execution, 501–502
fingerprinting, 429
requesting known resources, 430–436
Flash, 482–487
hooked browser and, 472–474
bypassing HttpURLConnection, 474–477
resource detection, 445–450
Sqlmap, 480–482
Tunneling Proxy and, 469–472
vulnerability detection
SQLi (SQL injection vulnerabilities), 450–465
XSS (cross-site scripting), 465–469
XSRF (Cross-site Request Forgery) and, 440–443
password reset attack, 443–444
tokens, 444–445
Web Application Hacker’s Handbook, 4
web applications attacking, 27
compromised, 46
web browser, client-server model, 4
web browser engines, 7.
See also layout engines; rendering engines
web server, application and, 4
web shell, BeEF bind as, 596–599
web workers, 11
webcam controlling, 236–242
Flash, 402–403
Webcam module, 238–242
Webcam Permission Check module, 236–237
WebKit, 7
WebRTC, 11
peer-to-peer connections, 517–518
WebRTC (Web Real Time Communications), 239
website phishing, 48, 49–54
websites, cloning, 50–51
WebSocket, 10, 84–86
WebWorker controller, 458–465
ping sweeping and, 525–527
WEP, wireless attacks, 62
whaling, 48
WhiteSpace encoding, 113–114
whitespace_encode( ) function, 113
Win32 Stage, 582–584
Win32 Stager, 580–581
window.open() method, 102
Windows, DNS poisoning, 70–71
windows, pop-under, 101–104
window.stop( ) function, 522
wireless attacks, 61–64
MAC address filtering, 62
rogue access points, 64
SSID hiding, 61
static IP filtering, 62
WEP, 62
WPA/WPA2, 63
WPA/WPA2, wireless attacks, 63
XYS
XBL (XML Binding Language), Firefox, extensions, 317
XCS (Cross-context Scripting), 339
CSP bypass, 344–346
DOM event handlers, 354–355
MitM attacks, 339–344
SOP bypass, 346–350
XSRF (Cross-site Request Forgery), 352–354
XSS, universal, 350–352
X-Frame-Options, 14
XML (eXtensible Markup Language), 6
XMLHttpRequest, 10
CORS headers, 83–84
ping sweeping and, 523–528
sendAsBinary( ) method, 553–554
XMLHttpRequest object, polling and, 80–83
xp_cmdshell( ) stored procedure, 456
XPCOM (Cross Platform Component Object Model) API, Firefox, 317–318
login manager, 318
operating system command execution, 320
reading from filesystem, 319
security model, 320–321
writing to filesystem, 319–320
XSRF (Cross-site Request Forgery), 352–354
web app attacks, 440–443
password reset attack, 443–444
tokens, 444–445
XSS (Cross-Site Scripting) attacks, 32–33
control bypassing, 43–45
cookie theft, 475
| DOM XSS, 33, 37–39 | viruses, 40–43 |
| Reflected XSS, 33, 34–35 | vulnerability detection |
| Stored (Persistent) XSS, 33, 35–37 | blind, 465–468 |
| universal, XCS and, 350–352 | filter evasion, 468–469 |
| Universal XSS, 33, 39–40 | XSS Tunnel, 152 |
| XssRays, 465–467 | XUL (XML User Interface Language), Firefox, extensions, 317 |
| XXE (XML External Entity), 140–141 |