

찾아보기

ㄱ

가상 키보드	226
가짜 CAPTCHA	243
가짜 로그인 프롬프트	245
가짜 소프트웨어 갱신	250
가짜 인증서	323
가짜 캡차	197
개인정보 공격	267
객체 표기법	138
검출 피하기	127
난독화	134
부호화	128
격리된 세계	383
견고성 원리	26
고래잡이	57
공격면	21
공백 부호화	130
공유 객체	468
공유기	509, 578
패스워드 재설정	519, 578
과부하 지점	570
광고	54
교차 기원	
요청	494, 644
원격 명령 실행	579
웹 응용 프로그램 지문 인식	503
웹 응용 프로그램 취약점 검출	527
웹 응용 프로그램 탐색	498
인증 여부 판정	510
자원 검출	521
DNS 하이재킹	578
XMLHttpRequest	12
교차 기원 자원 공유	11, 96, 176
헤더	497

SOP	154
교차 문맥 스크립팅	397
교차 사이트 스크립팅	☞ XSS
교차 사이트 요청 위조	181, 413, 515
방지 토큰	184, 520, 583
교차 영역 스크립팅	397
국제단말기식별번호	329
기본 게이트웨이 IP 주소 구간	611
끌어다 놓기	196
공격	416

ㄴ

난독화	134
내부 도메인 이름 탐색	500
내용 보안 정책	16, 386
우회	403
내용 스크립트	379
널 문자 악용	324
네트워크 공격	33
네트워크 프린터	654

ㄷ

단일 요인 패스워드 기반 인증	245
단편 식별자	44
단합	93
도메인 이름	104
도청	121
동급간 연결	606
동시적 실행	13
동일 기원 정책	5, 25, 151
우회	☞ SOP 우회
동치 부분문자열 공격	571
드로퍼	265

ㄹ

레드 팀 평가 257
 렌더링 엔진 8
 Blink 10
 Google 9
 Presto 10
 Trident 9
 WebKit 9
 링크 수집 524

ㄴ

마우스 포인터 사건 225
 마이크
 악용 470
 제어 276
 마크업 언어 6
 매체 재생 플러그인 480
 맹목 SQL 주입 527, 533, 617
 맹목 교차 기원 XSS 검출 544
 메모리
 관리자 336
 할당자 336
 메타 모듈 353
 명령 모듈 94
 모달 대화상자 239
 모듈리스 대화상자 239
 모래상자 462
 우회 19
 적용 18
 sandbox 특성 170
 무선 보안 제어 수단 71
 무선 통신 도청 71
 문서 객체 모형 DOM 66
 물리적 미끼 66

ㄷ

바운서 피싱 키트 68
 바인드 방식 셸 349, 648
 반사된 XSS 18, 40
 발신자 정책 프레임워크 61
 배열 객체 134

배치 엔진 8
 버그 현상금 289
 버퍼 넘침 660, 671
 변이 기반 XSS 51
 보안 소프트웨어 2
 보편 XSS 46, 410
 복호화 128
 봇넷 570
 부가 기능 365
 부트스트랩된 확장 기능 257
 부호화 128
 분산 DoS 573
 분산 포트 탐지 631
 불량 AP 73
 뷰포트 좌표계 226
 브라우저
 내부 IP 602
 내부 네트워크 609
 도우미 개체 388
 엔진 렌더링 엔진
 모래상자 18
 스레드 13
 영역 367
 진화 15
 캐시 83
 특권 4
 프록시 549
 플러그인 플러그인
 확장 기능 확장 기능
 후킹 91
 API 434
 브라우저 공격 32
 공격면 21
 내부자 공격 69, 121
 브라우저 이력 13, 200
 SOP 156
 브라우저 지문 인식 99, 291
 기벽 303
 소프트웨어 버그 302
 DOM 속성 296
 HTTP 헤더 292

브라우저 해킹 방법론	27
비HTTP 서비스 공격	637
지문 인식	634
비쿠키 세션 추적	269
비공개 브라우징 모드	267
비영수문자	
부호화	132
JavaScript	132



사건

마우스 포인터	225
부상	115, 220
양식	229
지속성 확보	114
초점	221
키보드	222
포획	220
흐름	220
blur	221
focus	221
keypress	223
onbeforeunload	114
사용 후 해제	339
사용자 계정 컨트롤	244
사용자 공격	31
사용자 입력 가로채기	220
사용자 추적 쿠키	316
사이드재킹 공격	317
사회공학	232
새미 월	48
생 TCP 소켓	647
서명되지 않은 Java 애플릿	159
서명된 Java 애플릿	160, 261
서버 쪽 코드 다형성	135
서비스 거부 공격	78, 570
세션	
저장소	11
추적	269
쿠키	308
SDP	607

STUN	606
셸코드	661, 677
소형 XSS 웹 복제 대회	50
숨겨진 IFrame	113
스크립트 API	434
스킵	5
스테이지	668, 677
Linux32용	682
Win32용	677
스테이지	677
Linux32용	682
Win32용	679
스팸	56
시간 지연	139



악성 QR 코드	66
암호화된 통신	25
애플릿	Java 애플릿
양식 사건	229
양식 수집	524
역 방식 셸	350, 667
영속적 XSS	42
영속적 쿠키	308
예비 요청	497
오라클 채움 공격	326
오류 기반 SQL 주입	527
외부 보안 경계선	26
요청 가로채기	122, 124
요청 대리 전달	178
우회	
동일 기원 정책	31
모래상자	19
쿠키 보호	304
클릭해서 실행	447, 463
HttpOnly 제약	555
HTTPS	318
Java 모래상자	462
SOP	49, 151, 405
XSS 억제 수단	51
XSS 필터	51, 548

운영체제 명령	
실행	417, 533
주입	421
원격 명령 실행	417
원형 재정의	122
웹 브라우저	☞ 브라우저
웹 셸	696
웹 실시간 통신	14, 279
웹 응용 프로그램	493
공격	33
공격 사례	577
과부하 지점	570
방화벽	52, 180
통계 착수	54
웹 저장소	11
웹사이트	
복제	59
피싱	57
웹캠	
악용	470
제어	276
이력 조작	13
이메일	
대량 발송기	64
주소 수집	63
피싱	56
Gmail	43, 248
인증 전 원격 명령 실행	589
인증 후 반사된 XSS	557
인증서	
공격	323
유효성 점검 취약성	324
인터넷 영역	367
인트라넷 IP 주소 탐색	498

ㄱ

자동 배경 갱신	22
자원 탐색	480
저장된 XSS	42
전이중 통신	12
전체화면 공격	233

정규표현식 기반 필터	128
정적 IP 필터링	71
정찰	602
제어교환	103
중간자 공격	69, 121
중첩 IFrame	112
지리 위치 API	10
지문 인식	
교차 기원 웹 응용 프로그램	503
데이터베이스	504
매니페스트	393
브라우저	99, 291
비HTTP 서비스	634
플러그인	440
확장 기능	388
HTTP 헤더	389
지속성 확보	
브라우저 내부자 공격	120
브라우저 사건	114
통신	111
팝언더 창	117
IFrame	111
지역 저장소	11

ㄴ

창 피싱	56
초점 관련 사건	221
취약성, 취약점	14

ㄷ

캐시	
악용	83
타이밍	201
캠재킹	282
커서재킹	188
쿠키	269, 304, 555
보호 우회	304
사용자 추적	316
세션	308
세션 추적	269
영속적	308

파괴 불가	269
Domain 특성	310
Expires 특성	307
Flash	468
HttpOnly 플래그	308
Path 특성	310
Secure 플래그	309, 318
쿠키 향아리	305
넘침	313
클라이언트 영역 좌표계	226
클라이언트 쪽 XSS	44, 46
클라이언트-서버 모형	4
클리피	259
클릭재킹	17, 181
클릭해서 실행	160, 437, 602
우회	447, 463
Java 애플릿	450
키 값 정의	224
키보드 사건	222
킬비트	439

ㄷ

탭 뉘아채기	232
통신	
기밀성	69
무결성	69
익명화	270
지속성 확보	89
통신 채널 확보	89
메시지 통신	100
CORS	96
DNS 터널 통신	103
WebSocket	97
XMLHttpRequest 폴링	92
통제 유지	30, 89
통제 착수	29, 37
광고 네트워크	54
사회공학 공격	55
오염된 웹 응용 프로그램	54
중간자 공격	69
XSS 공격	39

통제권 이양	24
트위터 로그인	511
특권 없는 문맥	367

ㄹ

파괴 불가 쿠키	269
파비콘	218
파이프	680
파일재킹	192
팝언더 창	117, 240
팝업 창	117
패스워드 관리자	391
공격	273
퍼징	561
펌웨어 대체	591
페이지	
내용 변조	215
전체 프레임 중첩	111
좌표계	226
포스텔의 법칙	26
포트	
번호	5
차단	623
탐지	622
IMG 요소	629
폴링	97
표준 운영 환경	2
프로토콜	
구현 오류 내구성	643, 646
자료 캡슐화	647
프로토콜 간 악용	660
프로토콜 간 통신	637, 643
IMAP	657, 683
SMTP	646
WebSocket	12, 97, 552
플러그인	23
검출	440
검출 프레임워크	443
공격	32, 446
매체 재생	480
브라우저	23, 433

지문 인식	440
차단	439
확장 기능과의 차이	435
Adobe Flash	155
Adobe PDF Reader	155, 477
Flash	468
Mona	674
NPAPI	423
QuickTime	480
SOP	155
VLC	480, 483
피싱	20, 56
방어 수단	67
웹사이트	57
이메일	56
창	56
황금시간	68
핑 쏘기	613
Java	618
ㅎ	
하이퍼텍스트 마크업 언어	6
해시 충돌 DoS	571
해시 테이블	571
헤더	☞ HTTP 헤더
현재 브라우저 창 위치	119
호스트 이름	5
혼합 내용 취약점	20
화면 좌표계	226
확장 기능	23, 363
공격	32, 395
부가 기능과의 차이	365
부트스트랩된	257
악성	258
위장	395
지문 인식	388
특권	366
플러그인과의 차이	364
Chrome	376
Firefox	368
Google Chrome	376
Internet Explorer	388
확장 명령 포인터	660
후킹	38
후킹된 브라우저	91
힙 뿌리기	338
A	
AAencode	134
Accept 헤더	293
Accept-Encoding 헤더	78, 293
Accept-Language 헤더	293
Access-Control-Allow-Origin 헤더	177, 680
Acrobat	☞ Adobe
ActionScript	469
ActiveFax	670, 688
ActiveX 컨트롤	434, 472
AdBlock	414
add-on	☞ 부가 기능
Address Resolution Protocol, ARP	74
Adobe	
Flash	☞ Flash
PDF Reader 보편 XSS	478
PDF Reader 플러그인	155, 477
Aircrack-ng	71
airdump-ng	72
AJAX(Asynchronous JavaScript and XML)	120
ALLOW-Access-From-Origin 헤더	696
alpha_mixed 부호화	671
Amazon IButton App	400
anti-XSRF token	184, 520
app.launchURL	479
arguments.callee	142
ARP(Address Resolution Protocol)	74
속이기	74, 319
중독	74
Asmax AR	804 589
Asynchronous JavaScript and XML, AJAX	120
attack surface	21
AttackAPI	629
autocomplete 특성	273
Avant	205

B

Base64 부호화	128
BEAST 공격	325
BeEF	
이메일 대량 발송 기능	64
웹 복제 기능	59
터널링 프록시	178
플러그인 검출	445
beef.browser.changeFavicon()	233
beef.browser.hookChildFrames()	231
beef.dom.attachApplet()	264
beef.logger.keypress()	223
beef.logger.push_stream()	224
beef.logger.submit()	229
beef.net.requester.send()	551
beef.net.send()	217
BeEF_bind 모듈	686
beef_bind_shell 모듈	689
Bind	676
Clickjacking 모듈	186
Clippy 모듈	260
Create Foreground IFrame 모듈	235
Detect Tor 모듈	271
Fake AV 모듈	254
Fake Flash Update 모듈	254
Fake Notification Bar (IE) 모듈	266
Firefox Extension Dropper 모듈	257
Get Internal IP 모듈	606
Get Page HTML 모듈	216
Get Physical Location 모듈	272
Get Stored Credentials 모듈	276
Get System Info 모듈	605
Gmail Phishing 모듈	248
internal_network_fingerprinter	505
Java Payload 모듈	262
Metasploit 연동	354
Port Scanner 모듈	631
Pretty Theft 모듈	246
QR Code Generator 모듈	67
Replace Component (Deface) 모듈	218
Replace Content (Deface) 모듈	218

Replace HREFS (HTTPS) 모듈	322
Signed Applet Dropper 모듈	265
TabNabbing 모듈	233
Webcam Permission Check 모듈	276
Webcam 모듈	278
Belkin N1 Vision	639
BHO(Browser Helper Objects)	388
bind shell	648
BlackHole	135
blind SQLi	527
blur 사건	221
bootstrapped extension	257
botnet	570
bouncer phishing kit	68
browser	☞ 브라우저
Browser Helper Objects, BHO	388
buffer overflow	660
bug bounty	289
Burp Suite	559
BusyBox	589

C

callee 속성	142
CamJacking	282
cancelBubble 속성	115
Cascading style sheets, CSS	7
CDN(Content Delivery Network)	278
Chrome 확장 기능	376
내용 스크립트	379
매니페스트 파일	378
악성 확장 기능	258
chrome-extension:// 스킵	382
chrome://extensions 페이지	377
chrome:// 스킵	5
chrome:// 영역	375
ClearClick	192
click to play, CtP	☞ 클릭해서 실행
clickjacking	17
client-server model	4
clientaccess-policy.xml 파일	166
Clippy	259

closure	93
CMS-Explorer	507
command module	94
Comtrend CT-5367	578
confidentiality	69
Connection 헤더	293
Content Delivery Network, CDN	278
content script	379
Content-Type 헤더	435
cookie	☞ 쿠키
CORS(Cross-origin Resource Sharing)	
	☞ 교차 기원 자원 공유
covert channel	104
cr-gpg	422
CRIME 공격	325
Cross-context Scripting, XCS	397
cross-origin	☞ 교차 기원
Cross-site Request Forgery, XSRF	181, 413, 515
Cross-site Scripting, XSS	☞ XSS
Cross-zone Scripting	397
crossdomain.xml 파일	155, 166
CSP(Content Security Policy)	16, 386
우회	403
CSRF	☞ 교차 사이트 요청 위조
CSS(Cascading style sheets)	7
visited 선택자	200
CTP(click to play)	☞ 클릭해서 실행
cursorjacking	188
D	
Damn Vulnerable Web App DVWA	556
DCC(Direct Client-to-Client)	641
DDoS(Distributed Denial-of-Service)	573
decoding	128
DeepSearch	270
denial of service, DoS	78, 570
Diminutive XSS Worm Replication Contest	50
Direct Client-to-Client, DCC	641
Distributed Denial-of-Service, DDoS	573
DJBX33A 알고리즘	571
DNS(Domain Name System)	81
사전 조회	104
은폐 채널	104
중독	81
환원 오류	106
DNSSpoof	81
document 객체	
domain 속성	153
ReadURL.readFile 속성	373
DOM(Document Object Model)	8
사건 처리부 공격	416
속성 존재 여부	296
저장소	11
지문 인식	390
SOP	153
XSS	44
Domain Name System, DNS	81
DoS(denial of service)	☞ 78, 570
parseFloat()	572
drag & drop	196
Dropbox	175
dropper	265
Drupal 로그인	513
dsniff	75
E	
eavesdropping	121
eBay	44
echo 명령	649
EIP(Extended Instruction Pointer)	660
EM-WebSocket	98
encoding	128
equivalent substring	571
error tolerance	643
error-based SQL	527
ettercap	75, 319
Eudora	659
Eudora WorldMail	666
event	☞ 사건
EventMachine	98
Evercookie 프로젝트	269, 317
execute_commands()	95

Exim	646
Extended Instruction Pointer, EIP	660
eXtensible Markup Language, XML	7
extension	☞ 확장 기능
EXTRACT 시스템	665
ezLinkPreview	409

F

fake Captcha	197
favicon	218
file:// 스킵	5, 373
filejacking	192
findClass()	463
fingerprinting	☞ 지문 인식
Firefox	297, 392
로그인 관리자	372
확장 기능	368
SOP 우회	169
FirePHP	389
Firesheep	317
Firmware Modification Kit	592
Flash	
공유 객체	468
바이트코드	469
설정 관리자	185
쿠키	468
퍼징	471
프록시	564
플러그인	468
focus 사건	221
<form> 요소	229
Fullscreen API	237
fuzzing	471, 561

G

g0tBeEF	80
Geolocation API	10
getAllLogins()	372
getHostName()	603
getLocalAddress()	603

Glassfish	583
Gmail	43, 248
Golden Hour of Phishing Attacks	68
Google	
+1 버튼	46
드라이브	175
셰이프 브라우징 API	67
Chart API	67
Chrome 확장 기능	☞ Chrome 확장 기능
Glass	283
Groovy Shell 서버	663

H

handshake	103
heap spraying	338
history	13
hooked browser	91
hooking	38
HostMonster	41
hosts 파일	81
HTA(HTML Application)	252
HTML(HyperText Markup Language)	6
HTML5	12
보안 커닝 페이퍼	53
전체화면 API	237
HTMLUnknownElement 객체	342
HTTP 요청	292
HTTP 프록시	178
HTTP 헤더	6, 15
브라우저 지문 인식	292
크기	661
확장 기능 지문 인식	389
Accept	293
Accept-Encoding	78, 293
Accept-Language	293
Access-Control-Allow-Origin	177, 680
Allow-Access-From-Origin	696
Connection	293
Content-Type	435
CORS	497
Set-Cookie	305

Strict-Transport-Security	17	모래상자 우회	462
User-Agent	293	역컴파일러	458
X-Content-Security-Policy	403	JMX	579
X-Content-Type-Options	16	JNLP	451
X-Frame-Options	17, 114	JRE	438
HttpOnly 쿠키 플래그	16	JSP	580
제약 우회	555	Reflection API	462
HTTPS		Java 애플릿	454
등급 내리기	319	서명되지 않은	159
우회	318	서명된	160, 261
httpsdatalist.dat 파일	400	역공학	457
HyperText Markup Language, HTML	6	클릭해서 실행	450
I		JavaScript 공격	331
ICE(Interactive Connectivity Establishment)	606	암호화	332
IFrame		엔진 기벽 활용	144
끌어다 놓기	199	엔진 에뮬레이션	139
숨겨진	113	코드 압축 최소화	129
중첩	112	함수 재정의	334
지속성 확보	111	힙 악용	335
키 기록	230	JBoss	579
<iframe> 태그	111	JD-GUI	458
IMAP 프로토콜	657, 683	jemalloc	336
IMEI(International Mobile Station Equipment		Jikto	49
Identity)	329	JJencode	132
Info.plist 파일	327	JMX(Java Management Extensions)	579
Initiating Control	통제 착수	JNLP(Java Network Launching Protocol)	451
integrity	69	서술자	451, 467
Internet Explorer 확장 기능	388	jQuery \$.popunder()	119
Internet zone	367	JRE(Java Runtime Environment)	438
IPC(Inter-protocol Communication)	637	jsLanScanner	510
IPE(Inter-protocol Exploitation)	660	JSP(Java Sever Pages)	580
iptables	625	역 방식 셸	580
IRC(Internet Relay Chat)	653	JVM(Java Virtual Machine)	454
isolated world	383	K	
J		KARMA 도구모음	73
jar: 스킴	162	keypress 사건	223
Java		kill bit	439
가상 기계	454		
검출	455		

L

LastPass	391, 396
layout engine	⇔ 렌더링 엔진
LinkedIn	396
Linksys	591
Linux32용 스테이지	682
Linux32용 스테이지	682
local storag	11
Lucky 13 공격	326

M

m0n0wall	586
MAC 주소 필터링	71
MalaRI	564
Man-in-the-Browser, MitB	69, 121
Man-in-the-Middle, MitM	69, 121
manifest.json 파일	378
markup language	6
mass-mailer	64
Maxthon	206
MediaStream API	279
Metasploit	344, 463
유틸리티	473
Browser Autopwn 모듈	353
meterpreter	349
PacketFu 라이브러리	79
Microsoft	
Excel	56
.NET 프레임워크	52
Office 길잡이	259
MitB(Man-in-the-Browser)	69, 121
MitM(Man-in-the-Middle)	69, 121
Mitsubishi MC-WorX	472
mixed content	20
MobileESP 프로젝트	295
Mona 플러그인	674
Mozilla 플러그인 검사기	444
MozWebSocket 객체	100
msfconsole 명령	345
MSHTML	9
MSSQL	533

mutation-based XSS	51
MySpace 프로파일 감염	48

N

NAT	
순회	638
핀 꽃기	638
IRC 공격 사례	639
navigator 객체	
mimeTypees 객체	442
plugin 객체	441
Netcom NB5	589
NoScript	188
NPAPI(Netscape Plugin Application Programming Interface)	382, 434
플러그인	423
nsIFileOutputStream8	373
nsIProcess	374

O

obfuscation	41
Office Assistant	259
onbeforeunload 사건	114
OpenWRT	639

P

Packages 객체	161
padding oracle attack	326
parseFloat()	572
password manager	273
PDF	
플러그인	477
JavaScript 코드	478
persistent cookie	308
persistent XSS	42
phishing	⇔ 피싱
PHP	572
셀	587
pinch point	570
ping sweeping	613
pinning	638

pipe	680	sandbox 특성	170
plugin	☞ 플러그인	ScribeFire	417
PluginDetect	443	SDP(Session Discovery Protocol)	607
pop-under	117	secure 쿠키 플래그	16
pop-up	117	sendAsBinary()	586, 647
port	☞ 포트	Sender Policy Framework, SPF	61
POST	686	session	☞ 세션
post-authenticated Reflected XSS	557	Session Discovery Protocol, SDP	607
post-authentication XSS	180	Session Traversal Utilities for NAT, STUN	606
Postel's Law	26	SET(Social-Engineer Toolkit)	61
Postfix	646	Set-Cookie 헤더	305
postMessage()	617	SGML(Standard Generalized Markup Language)	6
PostScript	656	Shank	79
prefetching	104	Shared Objec	468
preflight request	497	silent background update	22
prompt()	245	single-factor, password-based authentication	245
PsyBot	589	Skype	327
Q		SmartScreen 필터	244
QR 코드	66	SMTP 프로토콜	646
QuickTime 플러그인	480	social engineering	55, 232
R		Social-Engineer Toolkit, SET	61
Radamsa	471	SOE(Standard Operating Environment)	2
Recon-ng	63	SOP(Same Origin Policy)	5, 25, 151
reconnaissance	602	SOP 우회	49, 151, 405
red team assessment	257	클라우드 저장소	175
Reflected XSS	18	Adobe Flash	166
rendering engine	☞ 렌더링 엔진	Adobe Reader	164
Robustness Principle	26	CORS	176
rogue AP	73	Firefox	169
Routerpwn 프로젝트	594	Internet Explorer	167
RSA Security사	56	Java	157
RTCPeerConnection	607	Opera	171
Runtime.getRuntime().exec()	463	Safari	167
S		Silverlight	166
Sagemcom F@ST 2504	509	Sophos Anti-Virus	483
Same Origin Policy, SOP	5, 25, 151	SPAM	56
Samy Worm	48	spear phishing	56
sandbox	☞ 모래상자	SPF(Sender Policy Framework)	61
		SpiderMonkey	144, 341
		SQL 주입	527
		Sqlmap	534, 561

SSID 숨기기	71
SSL/TLS 공격	325
sslstrip	79, 319
stage	677
Standard Generalized Markup Language, SGML	6
Standard Operating Environment, SOE	2
stopPropagation()	115
stored XSS	42
Strict-Transport-Security 헤더	17
STUN(Session Traversal Utilities for NAT)	606
SuperHub	519

T

tabnabbing	233
TCP Socket API	647
TCP 프로토콜 제어	25
tel: 처리부	327
The Shellcoder's Handbook	14
theHarvester	64
TightVNC	635
Tor 프로젝트	268
Traversal Using Relays around NAT, TURN	607
Trident	144
TrixBot	691
TURN(Traversal Using Relays around NAT)	607

U

UAC(User Account Control)	244
UAF(Use After Free)	339
UI 재치장	180
UltraVNC	635
universal XSS	46
unprivileged context	367
Unstructured Supplementary Service Data, USSD	329
URI, URL	
난독화	41
단축 서비스	46
약용	326
URLCrazy	61
USB 드라이브	66

Use After Free, UAF	339
User Account Control, UAC	244
User-Agent 헤더	293
USSD(Unstructured Supplementary Service Data)	329

V

VBScript	8
Virata-EmWeb	654
virtual keyboard	226
VLC 플러그인	480, 483
vulnerability	14

W

WAF(Web Application Firewall)	52, 180
WAR(Web Application Archive)	580
web shell	696
Web Storage	11
WebRTC(Web Real Time Communication)	14, 279, 606
WebSocket 프로토콜	12, 97, 552
브라우저 지원	98
WebWorker API	13, 535, 574, 613
WEP(Wired Equivalent Privacy)	71
whaling	57
whitespace encoding	130
Win32용 스테이지	677
Win32용 스테이지	679
window 객체	
crypto.getRandomValues()	299
devicePixelRatio 속성	297
open()	117
postMessage()	152
postMessage() 브라우저 지원	103
stop()	611
Wired Equivalent Privacy, WEP	71
Wireshark 도구	75
WPA/WPA2	72

X

X-Content-Security-Policy 헤더	403
X-Content-Type-Options 헤더	16
X-Frame-Options 헤더	17, 114
XBL(XML Binding Language)	370
XCS(Cross-context Scripting)	397
중간자 공격	398
XML(eXtensible Markup Language)	7
외부 개체(XXE)	164
XML Binding Language, XBL	370
XML User Interface Language, XUL	370
XMLHttpRequest 객체	12, 92, 96, 154
XMLSerializer 객체	339
xp_cmdshell()	534
XPCOM(Cross Platform Component Object Model)	
API	371
XSRF(Cross-site Request Forgery)	
☞ 교차 사이트 요청 위조	
XSS(Cross-site Scripting)	38
맹목 교차 기원 XSS 검출	544
바이러스	47
반사된	18, 40
변이 기반	51
보편	46, 410
억제 수단 우회	51
영속적	42
인증 후 XSS 취약점	180, 557
지장된	42
취약점 검출	544
쿠키 훔치기	555
클라이언트	44, 46
터널	178
통제 착수	39
필터 우회	51, 548
Acrobat Reader	478
DOM	44
XSS Cheat Sheet	53
XSS ChEF	394
XssAuditor	548
XSSed	42
XssRays	544

XUL(XML User Interface Language)	370
XXE(XML external entity)	164
주입 공격	165

Y

Yahoo	46
-------	----