

642.6 Capture the Flag



SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SEC642.6

Advanced Web App Penetration Testing, Ethical Hacking,
and Exploitation Techniques

SANS

Capture the Flag

Copyright 2012-2019 Justin Searle and Adrien de Beaupré | All Rights Reserved | Version E01_01

Welcome to Day 6!

Course Roadmap

- Day 1: Advanced Attacks
- Day 2: Web Frameworks
- Day 3: Web Cryptography
- Day 4: Alternative Web Interfaces
- Day 5: WAFs and Filter Bypass
- **Day 6: Capture the Flag**

Network Setup
Exercise Goals
Scope of Work
Rules of Engagement
Start CTF
Four Hours of Game Play
CTF Wrap-Up

This page intentionally left blank.

VPN LAB SETUP

If you use the VPN to connect to the lab, go to Your Labs at

<https://connect.labs.sans.org>

- Instructions to install and configure OpenVPN to access the lab
- Passwords and certificates required to authenticate
- If you encounter any problems, email virtual-labs-support@sans.org

The VPN lab servers reboot periodically



If you take this class remotely, you need to connect via VPN for the exercises.

Remote students include Mentor, self-study, vLive, Simulcast, community, and OnDemand formats. To connect to the lab environment, SANS makes use of OpenVPN software, which can be installed in Windows, *BSD, Linux, and Mac OS X. The instructions also include certificates and passwords as well as the configuration files for the software to authenticate and connect.

Detailed instructions for the VPN installation are at the following URL:

<https://connect.labs.sans.org>

After you connect to the VPN, you can perform the exercises for the class. All the exercises require VPN connectivity.

NETWORK SETUP

Connect to the CTF network:

- Live classrooms use the same connection as the rest of the week
- OnDemand and Simulcast attendees create a VPN to the CTF Network, not the Lab Network

Verify network connectivity:

- Pinging 10.42.6.2
- Surfing to score.sec642.org (don't register yet)

Please do not communicate with any other IPs or hostnames yet!

This page intentionally left blank.

DAY 6 GOALS

We apply the techniques we have learned this week

Instead of one at a time, we use the tools and ideas in combination

This is a fun and educational game:

- Some vulnerabilities are modeled after real penetration tests

You can play to win

You can play for fun

You can play to learn and reinforce the exercises from the week

The three are not mutually exclusive!

Today's goals are to work through our methodology in a full web application pen test. Instead of approaching each item or idea separately as we have this week, we approach them as part of a complete test. This enables us to understand how this all works within a typical, or not so typical, penetration test.

Although the test we perform is an example, some are based on real vulnerabilities and applications in the real world. This example was designed to fit within a single day, which does mean that some of it has to be contrived.

Most important goal: Have fun!

ORGANIZATION OF TODAY

Discuss the rules and scope of the game

Your team can then start the penetration test

Play for approximately four hours, hard stop at 14:00

- Breaks are as-needed and not scheduled
- The first team that finds all the flags wins
- Or the team with the most flags at 14:00 wins

After the CTF is over, we will do a debrief, showing where to find all the remaining flags

Today is broken into three parts. The first is this lecture, which sets up the test and explains your scope. The second part is your team performing the test. Early this afternoon, we wrap up the testing. In the last part, we debrief through the application test. You present some of your findings to the instructor and then the instructor walks through anything that was missed and explains the entire test.

TEAMS

Work in teams of 2-5 people

Each team member must record their own findings and notes

The team maintains a master list of flags found:

- Where the flag was found
- How you got to the flag

Have regular meetings every 20–30 minutes:

- Review what you have found
- Compare notes and swap targets
- Adjust and plan your next steps

The game is based on the lab exercises throughout the week

Work in teams, as we recommend that you do in your regular testing. This enables you to combine skill sets and viewpoints to better assess the test. We recommend at least two people and no more than four. More than four becomes overkill in this environment. People start getting left out.

Have all team members record their findings and steps. After class, these notes can be useful for review.

Make sure you have regular meetings to compare notes and make sure you work together. This is extremely important; too often we see people on a team who have pieces of what is needed, but they don't talk to each other.

PROJECT SCOPE

Social engineering is allowed, but the targets are **EXTREMELY** aware:

- Users may surf URLs you inject

Scope: All web applications on 10.42.6.2-253 (port 80 and 8080)

- Only web applications and web services are in-scope
- Do not attack other services (SSH, DHCP, ARP, DNS, and so on)

Some servers may be accessible only from other servers

642 Inc. operates a DNS server at 10.42.6.2

- You can use this DNS server
- When the exercise begins, try a zone transfer (which isn't an attack)

To determine the risk level of having this information disclosed, 642 Inc. requested a test of all its web applications. This includes all of the web applications in scope. Social engineering is allowed, but the target is security-conscious and aware of the ongoing test. However, any URLs or injected code may be browsed.

Any web application in the network range of 10.42.6.2-253 is within scope of this test. Non-web app services are not. There is a DNS server at 10.42.6.2. This is both the DNS server 642 Inc. uses and the one you should use for the test.

RULES OF ENGAGEMENT

No denial-of-service attacks

No "dangerous" attacks:

- Deleting files or data is not allowed
- No performance-hogging attacks

When you gain access, do not hinder other teams' efforts:

- Do not delete flags, data, or items
- Do not add false flags

Only the web apps on target IP range are in scope:

- Do not attack other students!!!
- XSS attacks may be placed on target web apps IF they ONLY perform XSRF or cookie theft attacks on in-scope websites

You cannot do a few things:

- **No denial-of-service attacks:** We want everyone to reach the systems.
- **No "dangerous" attacks:** We don't want to delete files and data. We also want to recognize that this is a production system, so resource-hogging attacks should not be run.

Do NOT attack other testers!

ADDITIONAL RULES OF ENGAGEMENT

You are allowed to create new accounts:

- Do not change other users' passwords

You are allowed to write to files and install software:

- Do not uninstall software or harden the applications

Remember that this is both a production system and others are testing it

When in doubt, ask

You are allowed to create accounts, but do not change other users' passwords. This may prevent another student from getting through the game.

Installing applications and writing to files is allowed, as long as the applications and files do not cause issues for the production applications. You may want to configure your injected files to answer only to your team.

Keep in mind that this is a production system and that others are also testing the applications.

CAPTURE THE FLAG GOAL

Gather all 42 flags hidden in the environment:

- Flags are a combination of their name and a hash
- Name: key99; Hash: 3228635b89112e2c641f5e5cc44e19fe

Flags can be found if you follow the methodology:

- Hidden in places you should see during mapping
- Hidden in places where you look for vulns in discovery
- Hidden behind vulnerabilities you must exploit
- Hidden deeper in the servers you must map after exploitation

You have a couple goals here. First, find as many vulnerabilities as you can. Keep in mind that not all vulnerabilities can help you retrieve the data, but they are important to your target. Evaluate the risk and explain how you can exploit any that you find.

Gather all the flags. These flags have two pieces of information. The first is a name and the second is a hash.

For example:

Name: key99

Hash: 3228635b89112e2c641f5e5cc44e19fe

This data is scattered throughout the applications and it's your job to find both.

SCORING SERVER

This CTF has a scoring server to track your progress:

- <http://score.sec642.org>
- Choose one person to register for a team
- Only one person can be logged in at a time
- All other members can view scores
- Coordinate keeping track of the flags

As you find flags, enter them here:

- Name
- Hash

During this CTF, there is a scoring server that can keep track of your team's score. As you find flags (the name and hash) you enter them here. You actually need to enter the two fields, and the scoreboard will validate the name and the hash.

ANY QUESTIONS?

If you have any questions, now is the time to ask!

- Ask any question you would like
- But the instructor may not answer because the purpose of the test is for you to answer some of your questions

The instructor will be available throughout the test:

- We will answer questions regarding which tool will perform which technique
- We will not tell you where the flags are
- Any hints or answers to questions will be broadcast for all to hear
- Also, the final referee and judge will declare the winners

Although any questions you have are welcome throughout the day, if you have any, ask them now. If you are wondering something, it is guaranteed that someone else also is.

The instructor will accept all questions but may not answer them because it may reveal too much information. They will be available throughout the day.

THE MANTRA

During any penetration test or CTF, always keep these things in mind:

- Where are you in the methodology
- What do you know
- What is the objective
- Which technique will achieve the goals
- Which tool performs that technique in this application

We have seen too many pen testers and teams miss things, try random tools, or overthink

Some things to think about as you go through the CTF, and later when you are performing penetration testing.

YOU NOW HAVE PERMISSION TO BEGIN

You now have permission to begin the attack against the target applications:

- 10.42.6.2-253

Follow the Rules of Engagement

If and when you win, notify the instructor:

- Don't forget to watch the scoring server

Have fun!



You now have permission to begin the attack against the target applications on 10.42.6.2-253

Follow the Rules of Engagement.

If and when you win, notify the instructor.

Have fun!

COURSE RESOURCES AND CONTACT INFORMATION



AUTHOR CONTACT

Justin Searle
justin@meeas.com
@meeas
Adrien de Beaupré
adriendb@gmail.com
@adriendb



SANS INSTITUTE

11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)



PENT TESTING RESOURCES

pen-testing.sans.org
Twitter: @SANSPenTest



SANS EMAIL

GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

Please use our hashtag #SEC642 and follow us on Twitter!

Index

.AS	1:61, 1:94, 1:102, 1:104-105, 1:107-108, 1:135-136, 2:49, 4:53, 5:15, 5:80
.FLV	4:53
.js	1:160-164, 2:37, 2:49, 2:116, 2:122, 2:174-178, 2:186, 3:63, 3:67, 3:157-162, 4:53
.NET Binary Format for SOAP (NBFS)	4:58
.SWF	4:53, 4:68
/etc/passwd	1:25, 1:28-29, 1:43, 1:45, 1:48, 1:65, 1:69, 2:187, 4:10, 4:12-13, 4:109, 4:111, 4:113, 4:116-118, 4:160-161
/proc	1:54, 1:56-57, 2:25, 4:56
0x00	1:46, 3:94, 3:154, 3:159-160, 3:162, 4:101
3DES	3:25, 3:121, 3:158, 3:163
==	1:51, 1:105-106, 1:118, 1:125, 1:127, 1:131, 1:161, 1:164, 2:22, 2:87, 2:89-93, 2:103, 2:107-108, 2:113, 2:168, 2:170, 3:22, 3:65-67, 4:122, 5:122, 5:137
===	1:105-106, 2:89, 2:92-93, 2:113, 2:168, 3:67
—	
__call()	2:152, 2:156
__callStatic()	2:152
__clone()	2:152
__construct()	2:152
__debugInfo()	2:152
__destruct()	2:152, 2:156
__get()	2:152
__invoke()	2:152
__isset()	2:152
__set()	2:152
__set_state()	2:152
__sleep()	2:152
__toString()	2:152
__unset()	2:152
__wakeup()	2:152, 2:156

A

A5/1 stream cipher	3:25
access_log	1:60
ACID-compliant	1:115
ActionScript	4:53, 4:68
Active Server Pages	2:38
ActiveX	4:2, 4:4, 4:23-24, 4:51-52, 4:59-61
Advanced Metering Infrastructure (AMI)	3:36
AES-128	3:34
AES-256	3:28
AES-ECB	3:31-32
Akamai	5:37
Alert Logic	5:37
Angular.JS	2:37
ANSI SQL	5:113
Apache APR-MD5	3:50
Append	1:46, 1:65, 1:69, 1:89, 1:146, 1:163, 2:48, 2:62, 2:94, 3:37, 3:40, 3:64, 3:66, 3:78, 3:154-155, 4:5-7, 4:9, 4:11-12, 4:20, 5:111, 5:124
APPLET	4:2, 4:54-55
Application context	1:21, 5:115
Arithmetic Mean	3:41-42
ASCII	1:86-88, 1:96, 2:87, 2:166, 3:6, 3:12-13, 3:40-41, 3:91, 3:94, 3:96, 3:102, 3:110, 3:123, 3:126, 3:155, 3:161-162, 3:168, 3:175-176, 5:30, 5:35, 5:64-66
ASP	1:44, 1:46, 1:50, 1:52, 1:61, 1:84, 1:94, 2:11, 2:32, 2:34, 2:36, 2:38, 2:49, 2:66, 2:174, 3:157, 3:171, 5:20, 5:26-28
ASP.Net	1:44, 1:94, 2:11, 2:34, 2:36, 2:38, 2:49, 2:66, 2:174, 3:157, 3:171, 5:26-28
ASP.NET	1:44, 1:94, 2:11, 2:34, 2:36, 2:38, 2:49, 2:66, 2:174, 3:157, 3:171, 5:26-28
ASP.NET MVC	2:38, 2:49, 2:66
Asynchronous JavaScript and XML (AJAX)	1:134, 1:145-146, 2:173, 4:52, 4:121
Atomicity, Consistency, Isolation, and Durability (ACID)	1:115
Auditing	1:112
Auth Bypass	1:34-35, 4:126
Authenticated Encryption with Additional	3:36-38, 3:108

Data (AEAD)

Authentication	1:14, 1:21, 1:25, 1:30, 1:33, 1:35-36, 1:60, 1:112, 1:119, 1:130-132, 2:2, 2:14, 2:33, 2:74, 2:91, 2:96, 2:98-109, 2:111-113, 2:166, 3:6-9, 3:36-38, 3:46, 3:64, 3:115, 4:5, 4:8, 4:11, 4:17, 4:52, 4:56, 4:101, 4:104, 4:121, 4:124, 5:20-21, 5:117-118
----------------	--

B

BackTrack	1:60
Barracuda Networks	5:37
BASE-compliant	1:115
base64	1:37, 1:47-48, 1:51, 1:70-71, 2:170, 3:11-13, 3:19, 3:21-23, 3:30, 3:43, 3:45, 3:88, 3:176, 5:90-92, 5:108-109, 5:124
Basically Available, Soft State, Eventually Consistent (BASE)	1:115, 2:170, 4:122
Big Data	2:33
Binary JSON (BSON)	1:114, 1:117, 1:119, 2:34, 2:173
Binary Search Tree	1:88, 1:100-101
bit-flip	3:139-140, 3:144, 3:152
black box	2:34, 3:54, 3:183, 5:60
Blacklisting	2:49, 5:8-9, 5:36, 5:87-88, 5:100
Blind NoSQL Injection	1:119, 1:127
Blind SQL Injection	1:32, 1:78, 1:80, 1:85, 1:89, 3:56
block cipher	3:25, 3:28-29, 3:33, 3:35-36, 3:38, 3:45-47, 3:54, 3:121, 3:135, 3:146, 3:154, 3:156, 3:158
blog	1:25, 1:39, 1:43, 1:46, 1:48, 1:50-51, 1:54-55, 1:57, 1:59, 1:67, 1:69-73, 1:87, 1:120, 1:151, 1:153, 1:158-165, 2:16, 2:19, 2:21, 2:25, 2:45, 2:49, 2:68, 2:86, 2:111, 2:159, 2:163, 3:62, 4:10, 4:13, 4:111, 5:52, 5:126, 5:130, 5:140
Blowfish	3:25
Bluetooth	1:5, 3:25
Boolean output	1:86, 1:90
Bootstrap	2:37
Brute Force	1:86-87, 2:25, 2:27, 2:81, 2:91, 2:98, 2:100, 3:66, 4:67, 4:70-71
buckets	1:115, 2:12

Buffer Overflow	2:146
Burp	1:9, 1:21, 1:27-31, 1:33, 1:36-37, 1:39, 1:41, 1:57, 1:70-71, 1:73, 1:91, 1:94, 1:102-105, 1:107, 1:110, 1:120, 1:124, 1:128-129, 1:138, 1:143, 1:153, 1:155, 1:157-159, 1:165, 2:25, 2:27, 2:53, 2:60-61, 2:74, 2:98-99, 2:104, 2:134, 2:136-139, 2:142, 2:144, 2:149, 2:158, 2:161-162, 3:13, 3:15, 3:18-19, 3:21, 3:23, 3:43-44, 3:52-53, 3:55, 3:70, 3:80-81, 3:110-113, 3:115-116, 3:118, 3:120-123, 3:126, 3:129-130, 3:139-140, 3:142, 3:146, 3:150-152, 3:173, 3:178, 3:183, 4:10-11, 4:13, 4:15, 4:17, 4:29, 4:32-34, 4:39, 4:41-44, 4:46-47, 4:49, 4:58, 4:60, 4:63, 4:65, 4:67, 4:70-71, 4:86-87, 4:89, 4:91-94, 4:115, 4:127, 5:12, 5:14-15, 5:52, 5:71, 5:73, 5:103, 5:108, 5:126, 5:128
Burp Collaborator	1:21
Burp Comparer	1:33, 3:53, 3:183
Burp Encoder	1:36-37, 3:15
Burp Intruder	1:30-31, 1:33, 1:57, 3:113, 3:115, 3:118, 3:122, 3:129, 3:139, 3:150-152, 3:173, 4:13, 4:67, 4:70, 5:12, 5:71, 5:73, 5:103, 5:108
Burp Proxy	1:29, 1:37, 1:39, 1:41, 1:73, 1:110, 1:159, 1:165, 2:61, 2:138, 2:162, 3:43, 3:80, 4:43, 4:71, 4:92-93
Burp Repeater	1:37, 2:144, 2:158, 3:70, 3:80, 3:110, 3:139, 3:151, 4:39, 4:42-44, 4:47, 4:49, 4:71, 4:89
Burp Sequencer	3:43-44
Burp Suite Pro	1:27, 1:120, 1:138, 2:53
Bypassing Anti-XSRF	1:149

C

C++	1:46, 2:115
CA-cert	4:34
CakePHP	1:60, 2:2, 2:38, 2:49, 2:51, 2:53-63, 2:66
CAPTCHA	3:6, 3:56, 3:165-167, 3:169-170, 3:173, 3:175-179, 3:181
CCM Protocol (CCMP)	3:37
CDATA	5:41, 5:95-96, 5:106

Character sets	5:8, 5:64, 5:66, 5:84
CherryPy	2:38
Chi-square Test	3:42
Cipher Block Chaining (CBC)	3:3, 3:28, 3:33-38, 3:132-135, 3:139-140, 3:142-152, 3:156, 3:158
Cipher Block Chaining Message Authentication Code (CCM)	3:36-38
Citrix	5:37
CloudFlare	5:37
Component Object Model (COM)	4:59-60
CONCAT	1:83-84, 1:98, 3:27, 3:35, 3:37, 3:49, 3:75-78, 3:80, 3:86, 4:8-9, 4:122, 5:124
Content Management System (CMS)	1:14, 1:19, 2:2, 2:5-8, 2:14, 3:61-62
context	1:3, 1:14, 1:20-23, 1:31, 1:56, 1:126, 1:139, 1:142, 2:67, 2:71, 2:125, 2:131-132, 2:150, 2:175, 3:88-89, 3:91-92, 4:28, 4:87, 5:22, 5:26-28, 5:31, 5:64, 5:83-84, 5:93, 5:96, 5:100, 5:113, 5:115
CONVERT	1:47-48, 1:70-71, 1:83-84, 1:86, 1:88, 2:87-91, 2:125, 3:49, 3:63, 4:56, 5:30, 5:116
cookie	1:25, 1:35-37, 1:39-40, 1:58-59, 1:73, 1:137, 1:158, 2:74, 2:154, 3:6, 3:18-19, 3:23, 3:41, 3:46, 3:52, 3:115-116, 3:118, 3:120-122, 3:126, 3:129, 3:142, 3:146, 3:151, 3:157, 3:164, 4:19, 4:21-22, 4:27-28, 4:121, 4:124, 5:22, 5:118, 6:9
cookiecatcher.php	1:25, 1:39-40
Cookies	1:40, 1:59, 1:73, 1:137, 3:6, 3:52, 3:115, 3:142, 3:146, 3:157, 4:27-28, 4:124
Core Rule Set (CRS)	5:39, 5:43
Counter (CTR)	1:5, 1:11, 2:16, 2:63, 2:111, 2:154, 3:6, 3:28, 3:35-38, 3:63, 3:99, 4:52, 4:87, 6:3
Cracking	1:52, 1:86-87, 1:109-110, 3:59-60
Cross Site Request Forgery (CSRF)	1:142, 2:19, 2:35, 2:68, 4:78
Cross Site Request Forgery (XSRF)	1:4, 1:39, 1:141-151, 1:153, 1:155-165, 1:167, 4:76, 4:126, 5:36, 6:9
Cross Site WebSocket Hijacking (CSWSH)	4:124
Cross-Site Scripting (XSS)	1:4, 1:22-23, 1:25, 1:39-40, 1:134-139, 1:142-143, 1:147-151, 1:153, 1:155-165, 1:167, 2:12, 2:14, 2:19, 2:37, 2:68, 2:116, 2:121, 2:146-147, 2:182, 2:184, 3:65, 3:67, 3:170, 4:27-28, 4:76, 4:78, 4:126, 5:2,

	5:12, 5:14-17, 5:19, 5:21-22, 5:24, 5:27-31, 5:36, 5:52, 5:58, 5:62, 5:68, 5:82-83, 5:86-88, 5:91, 5:94-97, 5:99, 5:101, 5:103, 5:105-109, 6:9
CRUD	2:40
crypto	1:14, 2:33, 2:38, 2:91, 3:1-2, 3:4-8, 3:10-11, 3:25, 3:31, 3:36, 3:38, 3:40, 3:52, 3:54-57, 3:60-61, 3:68, 3:82, 3:84, 3:156, 3:182-183, 4:10, 4:13, 4:15, 4:17
CryptOMG	4:10, 4:13, 4:15, 4:17
crystal box	3:54, 3:183
CSLID	4:60

D

Data URI	5:89-92, 5:101, 5:108-109
db.eval	1:117
DBAPPSecurity	5:37
default pages	2:12
Denial-of-Service (DoS)	1:10, 4:126, 4:148, 5:43, 6:9
DenyAll	5:37
DES	3:25, 3:28, 3:47, 3:59-60, 3:82, 3:121, 3:135, 3:158, 3:163
dhclient	1:12
Diffie-Helman Exchange (DHE)	5:69
Directory Traversal	1:28, 1:46, 1:65, 2:187, 4:13, 4:147-148, 4:152, 4:159-161
discovery	1:16-19, 1:25, 1:65, 1:67, 1:77, 1:91-92, 1:94, 1:96-97, 1:99-100, 1:104-106, 1:110, 1:143, 1:153, 2:7, 2:25, 2:51, 2:69, 2:74, 2:76, 2:78, 2:96, 3:170, 4:4, 4:23, 4:27, 4:29-30, 4:33, 4:53, 4:74, 4:76, 4:93, 5:59, 5:111, 6:11
Django	1:60, 2:38, 2:49, 2:66, 3:50, 5:24
Document Object Model (DOM)	1:4, 1:134, 1:136-139, 1:153, 1:155-157, 1:160-162, 1:164, 2:37, 2:179-180, 5:98
Document-Oriented Database	1:114
DOM-Based XSS	1:4, 1:134, 1:136, 1:139, 1:153, 2:37
DOM-based XSS flaw	1:134
Domain Name System (DNS)	1:1, 1:10, 1:12, 1:50, 1:90, 4:30, 4:150, 5:35, 5:47, 6:8

E

EAX	3:36
ECB shuffling	3:2, 3:114, 3:118, 3:120-129
ECMAScript	4:53
EICAR	2:13
Elasticsearch	1:113
Electronic Codebook Mode (ECB)	3:2, 3:28-33, 3:35-36, 3:38, 3:46, 3:108-111, 3:113-116, 3:118, 3:120-130, 3:132-133, 3:135
Elliptic Curve Diffie-Helman Exchange (ECDHE)	5:69
encrypt	1:8, 1:112, 3:2, 3:5-6, 3:8-11, 3:25-38, 3:40-42, 3:44-47, 3:50, 3:52, 3:54, 3:58-59, 3:61-64, 3:66-68, 3:82, 3:84-92, 3:94, 3:96, 3:98-102, 3:105-106, 3:108-110, 3:114-116, 3:118, 3:120-121, 3:126, 3:129-130, 3:132-135, 3:140, 3:146, 3:151-152, 3:157, 3:159-162, 3:164-167, 3:169-171, 3:175-176, 3:179, 3:181, 3:183, 4:29-30, 4:120, 4:124, 4:142, 4:150, 4:157, 5:21, 5:38
Ent	3:41-42
Enterprise Security API (ESAPI)	5:19-22
Entities	1:54, 2:49, 3:8, 4:3, 4:108-111, 4:118
Entropy	3:11, 3:40-43, 3:45, 3:61, 3:63, 3:68, 3:77, 3:82
Ergon Informatik	5:37
error_log	1:60
eval()	2:74, 5:100
event handlers	1:145, 5:75, 5:86, 5:88
EvilCAPTCHA	3:173, 3:175-177
execScript()	5:100
exploitation	1:1-2, 1:8-9, 1:15-19, 1:23, 1:25, 1:31, 1:35, 1:45-46, 1:90, 1:92, 1:100, 1:120, 1:137, 1:139, 1:145, 1:147, 1:149, 1:157, 2:1, 2:7, 2:17-18, 2:22, 2:40, 2:48, 2:74, 2:155, 2:159, 2:171, 3:1, 3:5, 3:55, 3:57, 3:182-183, 4:1, 4:4, 4:23, 4:33, 4:77, 5:1, 5:111, 6:1, 6:11
Express	1:91, 1:105, 2:93, 2:119, 2:174, 2:177, 2:182, 2:184-188, 3:42-43, 3:60, 5:8-9, 5:19, 5:24, 5:29, 5:31, 5:45-46, 5:108

ExpressJS	2:174
External Entity	4:78, 4:111, 4:118
extract()	2:111-112

F

F5	3:30, 3:46, 3:66, 3:88, 3:91, 3:101-102, 3:104, 4:148, 5:37, 6:11
FailPics	3:70-71, 3:73-77, 3:79-80
Fast Data	2:33
Field Programmable Gate Array (FPGA)	3:59-60
File Inclusion	1:25, 1:28, 1:43-52, 1:54-56, 1:58, 1:60-61, 1:63-65, 1:67, 1:69, 1:74, 1:167, 2:187, 3:56, 3:92, 5:76
FileSystemObject	1:61
fingerprinting	5:2, 5:57-58, 5:60-62, 5:71, 5:73-80, 5:119
Flare	4:63, 4:67-68, 4:71, 5:37
Flash Cross Domain policy	4:53
Flask	2:38, 2:66, 2:68, 2:76, 2:78, 2:83
Flex	1:76, 1:78, 2:16, 3:13, 3:48, 3:164, 4:51, 5:38, 5:112
FLOOR	1:83-84, 1:98
fopen	1:40, 1:61
Fortinet	5:37
FTP server	1:55
FuzzDB	1:31, 1:118, 1:120, 5:12, 5:16, 5:71, 5:73, 5:103, 5:108, 5:126, 5:128
Fuzzing	1:118, 1:120, 1:127-128, 2:109, 3:111, 3:120, 3:160, 4:33, 4:85, 4:103-106, 4:129, 4:131, 4:135, 4:137, 4:147-148, 5:12, 5:16, 5:60, 5:63, 5:71, 5:73-79, 5:128
fwrite	1:40, 1:61

G

Galois/Counter Mode (GCM)	3:36
Gentoo	1:60
Github	1:65, 1:91, 1:118, 1:120, 1:122, 2:39, 2:44-48, 2:51, 2:74, 2:87, 2:148-149, 2:162-164, 4:13, 4:15, 4:31
Google Web Toolkit (GWT)	2:38

Gotham Digital Science (GDS)	4:58
gray box	3:54, 3:183
GROUP BY	1:83-84, 1:98
GSM phone calls	3:25

H

Hadoop	2:33-34
Hash Message Authentication Code (HMAC)	3:9, 4:5
HashCalc	3:48-49
Hashed Message Authenticity Check (HMAC)	3:9, 4:5
hashing function	2:91, 3:9, 3:11, 3:38, 3:45, 3:48-50, 3:54, 3:68, 3:82, 4:9
Hbase	1:113, 2:34
Heuristic	1:87, 1:96-97
Hex Editor	2:149, 2:165, 3:101
Hidden field	3:6, 3:52, 3:88
HPACK	4:143
HTML5	4:57, 4:61, 5:83-88, 5:101, 5:103, 5:107
HTTP Pipeline	5:26
HTTP/1.X	4:142-143
HTTP/2	4:3-4, 4:23, 4:61, 4:142-143, 4:145-147, 4:149, 4:152, 4:154-162, 5:69
HttpModule	5:26
HyperText Transfer Protocol (HTTP)	1:10, 1:14, 1:28, 1:32, 1:50, 1:60, 1:64, 1:89-90, 1:101, 1:106, 1:128-129, 1:141, 1:157-158, 1:165, 2:33, 2:43, 2:47, 2:61, 2:113, 2:116, 2:128, 2:149, 2:177, 3:6, 3:12, 3:52, 3:113, 3:157, 3:167, 3:171, 4:3-4, 4:23-25, 4:29, 4:31-33, 4:39, 4:41-44, 4:46-49, 4:53, 4:56, 4:60-61, 4:79-80, 4:120-122, 4:124, 4:127, 4:142-147, 4:149-150, 4:152, 4:154-162, 5:7-8, 5:10, 5:14-16, 5:26, 5:33, 5:35, 5:38, 5:43, 5:45, 5:54, 5:69, 5:71, 5:73-80, 5:105-107, 5:115, 5:128

I

ifconfig	1:12
IHTTPHandler	5:26
IHTTPModule	5:26
Imperva	5:37
include()	1:44, 1:49, 1:51
Initialization Vector (IV)	3:2, 3:27, 3:33-35, 3:37, 3:45, 3:52-53, 3:85-86, 3:90, 3:94, 3:96, 3:98-106, 3:132-140, 3:146-150, 3:152, 3:157-162, 3:164, 3:167, 3:169, 3:171, 3:175
Input sanitization	2:123, 2:146, 2:148
Internet Control Message Protocol (ICMP)	1:90
Internet Server Application Programming Interface (ISAPI)	2:17, 5:26
Isomorphic JavaScript	2:175, 2:180

J

Java applets	4:2, 4:54
Java Decompiler (JAD)	4:56
Java Server Faces (JSF)	2:38, 3:171
JavaScript Object Notation (JSON)	1:114, 1:117, 1:119, 2:33-34, 2:43, 2:147- 148, 2:173, 2:179, 4:25, 4:44, 4:56, 4:79, 4:84
JavaServer Faces (JSF)	2:38, 3:171
Joomla	2:8, 2:154
JSP	1:44, 1:46, 1:52, 1:65, 2:66, 2:116, 2:118, 2:122, 2:186, 3:157-162
JustDecompile	4:58

K

Kerckhoffs' Axiom	3:10
Keystream	3:27, 3:35, 3:37, 3:86-87, 3:90-94, 3:96, 3:100-103, 3:105-106, 3:136, 3:158-163, 3:168-170

L

LAMP	2:174
Laravel	2:38
Laudanum	1:61
LDAP Injection	2:146
Length analysis	3:45
LIMIT	1:82
Local File Inclusion (LFI)	1:3, 1:25, 1:28-29, 1:47-49, 1:54-56, 1:60-61, 1:63-64, 1:67, 1:69-74, 2:96, 2:187, 3:56, 3:92, 4:10, 5:76

M

Magic Methods	2:152-153
Mallory	4:30-32
malware	2:13, 4:59, 5:43
Man-in-the-Middle (MitM)	1:10, 3:9, 4:30, 5:61
mapping	1:16-19, 1:91, 1:102, 1:104, 1:138, 1:143, 1:153, 2:7, 2:35, 2:41, 2:184, 4:29, 4:33, 4:52-54, 4:74-76, 4:127, 5:25, 5:59, 5:67-68, 5:117, 6:11
mapReduce	1:117
MariaDB	1:113, 2:17, 2:34
Marshal	2:148
MD4	4:5
MD5	1:108-109, 2:91, 2:113, 3:9, 3:49-50, 3:61, 3:63, 3:65-68, 3:71, 3:74-81, 4:5-6, 4:19-21
md5sum	3:9, 3:78-80
MEAN	1:112-114, 2:3, 2:174, 2:176, 2:182, 2:184, 5:24
MEAN stack	1:112-114, 2:3, 2:174, 2:176, 2:182, 2:184, 5:24
memcached	1:112
Microsoft SQL	1:82, 1:106, 1:114, 2:34, 5:115
Microsoft SQL Server (MSSQL)	1:78, 1:82-84, 1:88-89, 1:94, 1:106, 1:114, 5:119
Mobile applications	1:7, 2:177, 4:2, 4:4, 4:23, 4:25, 4:27, 4:36, 4:73, 4:164
Model View Controller (MVC)	2:17, 2:35, 2:37-38, 2:40-45, 2:47, 2:49, 2:51, 2:66-67, 2:118, 2:174, 2:177-178,

	2:180
Model-view-view-Model (MVVM)	2:37, 2:179-180
ModSecurity	5:2, 5:12, 5:16, 5:38-39, 5:41-45, 5:47-48, 5:50, 5:52-55, 5:69, 5:71, 5:73-79, 5:103, 5:108-109, 5:124, 5:126, 5:130-131
MongoDB	1:3, 1:113-119, 1:122, 1:124-132, 2:33-34, 2:173-174
Monte Carlo	3:41-42
MSBIN SOAP	4:58
Multipurpose Internet Mail Extensions (MIME)	3:12, 5:78
MySQL	1:25, 1:30-31, 1:33, 1:71, 1:78, 1:82-85, 1:88-89, 1:94, 1:96-98, 1:114, 1:116, 2:17, 2:34, 2:174, 3:49-50, 4:93, 4:161, 5:115-119, 5:122, 5:124, 5:126, 5:128-131

N

National Institute of Standards and Technology (NIST)	3:9, 3:36-37, 3:59, 4:13
Network Intrusion Detection System (NIDS)	5:33
Network Intrusion Prevention System (NIPS)	5:33
NGINX	2:17, 2:34, 5:38
Node.js	2:49, 2:174-177
NodeGoat	2:3, 2:182, 2:184-188
NoSQL	1:3, 1:112-120, 1:122, 1:124-132, 2:33, 2:173-174
NoSQL Exploitation Framework	1:120
NoSQL Injection	1:3, 1:113, 1:117-120, 1:122, 1:124-132
NoSQLMap	1:120, 1:122
NSFOCUS	5:37
Null	1:46, 1:98, 1:116, 1:161, 1:164, 2:90, 2:92, 2:94, 2:96, 2:105, 3:94, 3:154, 4:101, 5:22, 5:30, 5:124, 5:137
null byte	1:46, 3:94

O

obfuscation	2:8, 5:116
-------------	------------

OBJECT	4:54-55, 4:59-60
Object Graph Notation Language (OGNL)	2:66, 2:68, 2:71, 2:119, 2:123, 2:130-131
Object Linking and Embedding (OLE)	4:59-60
oclHashcat+	3:60
onload	1:144, 1:146, 1:151, 5:88, 5:99
openssl	3:9, 3:34
Oracle	1:78, 1:83, 1:114, 2:34, 2:115, 2:117, 2:171, 3:3, 3:50, 3:52, 3:56, 3:155-158, 3:163-165, 3:168-169, 3:171, 3:173, 3:175-181, 5:119
Oracle padding	3:155, 3:157
output encode	2:116, 2:121
OWASP ZAP	1:9, 1:138, 4:127, 4:129, 4:133, 4:140, 4:149

P

padBuster	3:164-168, 3:170, 3:173, 3:176, 3:179-181
padding	3:3, 3:22, 3:28, 3:52, 3:56, 3:154-165, 3:167-169, 3:171, 3:173, 3:175-181, 4:5-9, 4:146
Padrino	2:38
Passlib	3:50
PCAP	4:29, 4:39, 4:41-42, 4:44, 4:49, 4:129, 4:131, 4:134, 4:154, 4:157
Penta Security	5:37
Perfect Forward Security (PFS)	5:69
PHP	1:3, 1:25, 1:28-29, 1:31-32, 1:34-35, 1:37, 1:39-40, 1:43-44, 1:46-52, 1:54, 1:57-61, 1:63-65, 1:67, 1:69-73, 1:84, 1:91, 1:94, 1:96-97, 1:99-102, 1:128-129, 1:142, 1:151, 1:153, 1:155-165, 2:2, 2:17-23, 2:25, 2:27, 2:29, 2:32, 2:34, 2:38-39, 2:49, 2:51, 2:53-63, 2:66, 2:68, 2:85-90, 2:92-94, 2:96, 2:101, 2:106-108, 2:111, 2:113, 2:115, 2:147-156, 2:169, 2:174, 3:18, 3:49-50, 3:65, 3:67, 3:71, 3:74-77, 3:80, 3:134, 3:165-167, 3:170, 3:175-179, 4:15, 4:71, 4:81, 4:89, 4:91-93, 4:101, 4:103-105, 4:111, 4:132, 5:3, 5:16, 5:19-20, 5:43, 5:73-79, 5:105-107, 5:128-129, 5:131, 5:133-136, 5:140, 5:142-147

PHP Class Members	2:150
PHP Comparisons	2:89
PHP Object Injection	2:150, 2:155
PHP Object Orientation	2:150
PHP session files	1:54, 1:58, 1:73
PHPass	3:49-50
phpinfo()	1:49, 1:51, 1:63, 1:72-73, 5:140, 5:142-143
phpinfo.php	1:64
PHPSESSIONID	1:158-159
Pickle()	2:148
PKCS#7	3:3, 3:154-155, 3:159-160, 3:162, 3:167, 3:181
plaintext	1:47, 2:20, 3:8-11, 3:19, 3:21, 3:26-31, 3:33-38, 3:45-46, 3:56, 3:64, 3:85-87, 3:90-94, 3:99-106, 3:108-109, 3:116, 3:132-133, 3:136, 3:138, 3:140, 3:152, 3:154-156, 3:158-163, 3:165-166, 3:168-170, 3:179
Play	1:29, 1:43, 1:47-48, 1:59, 1:63, 1:73, 1:82-85, 1:88, 1:97, 1:101, 1:134, 1:148, 1:161-162, 2:11-12, 2:34, 2:38, 2:49, 2:65, 2:106, 2:182, 2:186, 3:10, 3:48-49, 3:65, 3:71, 3:74, 3:93, 3:112-113, 3:116, 3:124, 3:130, 3:139, 3:144, 3:168, 3:170, 4:11, 4:25, 4:37, 4:42, 4:45, 4:53, 4:63, 4:65, 4:69, 4:71, 4:73, 4:78, 4:92-93, 4:134, 4:140, 5:21-22, 5:66, 5:68, 5:85, 5:88-89, 5:134, 6:5-6
Plugins	1:25, 1:138, 2:5, 2:16, 2:18, 2:20-21, 3:112-113, 3:124, 4:58, 4:87, 5:97
Positive Technologies	5:37
PostgreSQL	1:83, 2:34, 3:50, 5:116, 5:119
Prepend	1:28, 1:46-47, 1:65, 1:69, 2:112, 3:49, 4:9
PreSendRequestContent	5:26
PreSendRequestHeaders	5:26
privilege escalation	1:36, 1:49, 3:134, 3:145, 3:151-152
Process ID (PID)	1:56
Procyon	4:56
properties	1:45, 2:17, 2:20, 2:150, 2:152, 3:90
Pylons	2:38
Pyramid	2:38

Q

Qualys	5:37
Queries Per Letter (QPL)	1:86-89
Quick UDP Internet Connections (QUIC)	4:3, 4:150

R

Rack	1:18, 1:20, 1:25, 1:30, 1:36, 1:52, 1:60, 1:86-87, 1:92, 1:94, 1:108-110, 2:38, 2:41-42, 2:45, 2:94, 3:5-6, 3:43, 3:59-60, 3:115, 3:136, 4:124, 5:36, 5:47, 6:12
Radware	5:37
Rails	1:60, 2:38, 2:40, 2:44-48, 2:51, 2:66, 2:174, 2:180, 5:24
rand()	3:74, 3:76, 3:79
RC4	3:25
readdirSync()	2:182, 2:186-187
readFileSync()	2:182, 2:187
Real-time Block List (RBL)	5:47
reconnaissance	1:16, 1:19, 1:67, 1:105-107, 1:110, 3:70-71, 3:75, 3:81, 4:74
referrer	1:137, 1:145, 1:155
regular expression (regex)	1:91-92, 1:105, 1:128-130, 3:43, 5:8-9, 5:19, 5:24, 5:45-46
Relational DataMase Management System (RDBMS)	5:113, 5:115-116
Remote File Inclusion (RFI)	1:3, 1:45, 1:49-52, 1:54, 1:69, 1:74, 3:56
REpresentational State Transfer (REST)	1:91, 1:119, 2:40, 2:113, 4:2, 4:4, 4:23, 4:25, 4:73, 4:79, 4:84-85
require()	1:44, 1:51
Response.WriteFile()	1:44
RESTful	2:33, 2:40, 2:43, 4:79
RFC 7540	4:142, 4:146
Riak	1:115, 2:34
Ruby on Rails	1:60, 2:40, 2:44-45, 2:66, 2:174

S

Same Origin Policy (SOP)	1:145, 1:147, 1:149, 2:14, 4:53, 4:124
SamuraiWTF	1:1, 1:25, 1:27, 1:39, 1:61, 1:141, 2:106,

	4:20, 4:44, 4:46-47, 5:124
SAMY worm	1:150
Sandbox	2:71, 2:74, 2:117, 2:124-125, 2:131, 4:52, 4:54, 4:59, 4:126, 5:133, 5:147
SCRIPTABLE	4:55
SecDataDir	5:41
SecDefaultAction	5:41, 5:44
SecResponseBodyAccess	5:41
SecRuleEngine	5:41
SecRuleRemoveByID	5:41
Secure authentication	3:8
sed	3:78-79, 3:110
SELECT COUNT	1:83, 1:98, 3:70, 3:80
Serialization	2:3, 2:85-86, 2:130, 2:146, 2:148-156, 2:158, 2:161-162, 2:165, 2:171, 5:133
Server.Execute()	1:44
Session tokens	3:6
sessionid	1:37, 1:158-159
SGML	5:95
SHA1	3:9, 3:49-50, 3:61, 3:68, 4:5, 4:7, 4:11-12
sha1sum	3:9, 4:7, 4:11
SharePoint	1:167, 2:2, 2:6-8, 2:10-14
shotgun approach	1:65
shuffle	3:52, 3:109-111, 3:113-114, 3:118, 3:123, 3:125-126, 3:128, 3:130
Side-Channel	1:90
Silverlight	4:2, 4:4, 4:23-24, 4:51-52, 4:57-58, 4:61
Simple Machine Forum	2:91
Simple Object Access Protocol (SOAP)	4:2, 4:4, 4:23, 4:25, 4:27, 4:58, 4:73, 4:76- 77, 4:79-82, 4:84-85, 4:87, 4:89, 4:91-94, 5:36
Sinatra	2:38, 2:174, 2:177
SMS messages	3:25
SOAPUI	4:85-86, 4:89, 4:92-94
social engineering	1:6, 6:8
Social Security Number (SSN)	5:46
SocketToMe	4:3, 4:129, 4:131-140
Solr	1:113
Sourceforge	1:61, 1:65, 3:59, 5:138
SPDY	4:142
Splunk	1:113
Spring MVC	2:38
SQL injection (SQLi)	1:3, 1:17-18, 1:22-23, 1:25, 1:30, 1:32-34,

	1:36, 1:76-78, 1:80, 1:82, 1:85, 1:89, 1:92, 1:94, 1:96-110, 1:113, 1:117-120, 1:122, 1:124-132, 1:167, 2:12, 2:69, 2:116, 2:146, 2:182, 2:184, 3:6, 3:56, 4:27-28, 4:76, 4:78, 4:86, 4:93, 4:99, 4:126, 5:2, 5:8-9, 5:12, 5:16-17, 5:19, 5:36, 5:111-113, 5:115, 5:119, 5:121, 5:126, 5:128-131
SQLite	4:28, 5:119
Sqlmap	1:18, 1:30-33, 1:41, 1:91-92, 1:94, 1:96-110, 1:120, 1:122, 4:89, 5:116, 5:119-124, 5:126, 5:128-129, 5:131
StackOverflow	2:39, 3:71
stream cipher	3:2, 3:25-28, 3:35, 3:38, 3:45, 3:47, 3:56, 3:84-88, 3:90, 3:94, 3:96, 3:98-106
stream wrapper	1:51-52
strings	1:17, 1:30-31, 1:33, 1:40, 1:46, 1:86, 1:118-120, 2:21, 2:85, 2:87-89, 2:94, 2:154, 3:23, 3:93-94, 4:12-13, 4:86, 4:104-106, 4:110-111, 5:7, 5:9, 5:53, 5:63, 5:80, 5:92, 5:116
Structured Query Language (SQL)	1:3, 1:17-18, 1:22-23, 1:25, 1:30-34, 1:36, 1:76-78, 1:80-82, 1:85-86, 1:88-90, 1:92, 1:94, 1:96-110, 1:112-117, 1:119, 1:167, 2:12, 2:32-34, 2:40, 2:69, 2:116, 2:146, 2:174, 3:6, 3:56, 3:70, 3:74, 3:76, 3:78-81, 4:27-28, 4:76, 4:78, 4:86, 4:93, 4:96, 4:99, 5:2, 5:8-9, 5:19, 5:30, 5:63, 5:85, 5:111-113, 5:115, 5:119, 5:126, 5:128-131
Struts	2:2-3, 2:38, 2:66, 2:68, 2:118-125, 2:127-132, 2:134-144, 5:24
Struts Validation Framework	2:120
Struts2	2:119-124, 2:132
Sucuri	5:37
Supervisory Control And Data Acquisition (SCADA)	3:36
Symfony	2:38

T

tamper scripts	5:121, 5:124, 5:126, 5:129
Teradata	1:113
themes	2:19-23, 2:25

Transport confidentiality	3:8
Transport Layer Security (TLS)	1:112, 3:5, 3:8, 3:25, 3:37, 4:29, 4:124, 4:142, 5:69
Trustwave	5:37-38, 5:126, 5:130
Type Juggling	2:2, 2:87-89, 2:93-94, 2:96, 2:98-109
TYPO3	3:62-68, 3:82

U

uid	1:17, 1:35-39, 1:92, 1:110, 1:127, 1:158-159, 2:49, 2:66, 2:117, 2:141, 2:178, 2:182, 3:109, 3:116, 3:134, 3:137-138, 3:142, 3:144, 3:146-151, 4:79, 4:122, 5:43, 5:55, 5:137
UNC path	1:50, 1:52
UNICODE	1:86, 5:8, 5:30, 5:35, 5:66-68, 5:108, 5:117, 5:124
UNION	1:78, 1:82, 1:94, 1:98, 1:100, 1:109, 1:119, 5:119, 5:124
United Security Providers	5:37
Unserialize()	2:153, 2:156
upload	1:3, 1:45, 1:54-55, 1:63-64, 2:13-14, 2:74, 2:86, 2:128, 2:130, 2:139-141, 2:143, 2:158, 3:67, 3:96, 3:98-100, 3:105, 4:79, 5:43, 5:135-136, 5:138, 5:140, 5:142, 5:145-147
URL Tampering	3:64-65, 3:89
User-Agent	1:32, 1:158, 2:142, 4:46-48, 4:144, 5:16, 5:47, 5:53-54, 5:71, 5:73-79, 5:105-107, 5:126, 5:128-129, 5:131
UTF-16	5:67
UTF-2	5:67
UTF-8	3:12, 4:44, 4:46-47, 4:81-82, 4:97, 4:99, 5:35, 5:64-67, 5:91

V

V8	2:175-176
VBScript	5:97-100
Verizon	5:37
Voldemort	2:34

W

W3AF	1:9
WAITFOR DELAY	1:89, 1:106
Wappalyzer	2:184
Web Application Description Language (WADL)	4:75, 4:84, 4:86
Web Application Firewall (WAF)	1:14, 1:17, 1:96, 1:102, 4:147, 5:1-2, 5:4-5, 5:11-12, 5:14-17, 5:19, 5:33-37, 5:41, 5:43, 5:57-58, 5:60-61, 5:64, 5:69, 5:71, 5:73, 5:77, 5:93-94, 5:96, 5:101, 5:103, 5:105-107, 5:114-115, 5:120, 5:126, 5:128-131
Web Application Firewall Evaluation Criteria (WAFEC)	5:36
Web Application Security Consortium (WASC)	5:36
Web Parts	2:11-12
Web Services Description Language (WSDL)	4:75, 4:83-84, 4:86-87, 4:89, 4:91-93
WEB-INF	2:120, 2:159
WebSockets	4:3-4, 4:23-24, 4:61, 4:120-121, 4:125-127, 4:129, 4:131-140, 4:147-148, 5:69
Whitelisting	2:49, 5:9, 5:36, 5:60
win.ini	1:65
Windows Communication Foundation (WCF)	4:58
Wireshark	2:149, 4:2, 4:29-30, 4:39, 4:41-49, 4:125-126, 4:129, 4:134, 4:140, 4:148-149, 4:152, 4:157-158, 4:162
WISA	2:174
WISC	2:174
WordPress	1:47, 2:2, 2:6, 2:8, 2:16-23, 2:25, 2:27-30, 2:49, 5:140
WPScan	2:25, 2:27
WriteFile()	1:44
WSDLER	4:87

X

XML External Entity (XXE)	2:146, 4:3, 4:111, 4:113, 4:115-118
XMLHttpRequest (XHR)	1:137, 1:145-146, 1:160-161, 1:163-164
XOR	3:27, 3:33-35, 3:37, 3:86-87, 3:90-94,

	3:96, 3:101-104, 3:106, 3:132-133, 3:136, 3:140, 3:152, 3:158-159, 3:161-163, 3:169
xor2files.py	3:93, 3:103
XPath	4:3, 4:78, 4:86, 4:96, 4:98-99, 4:101, 4:103-106
XXD	2:149, 2:166, 3:12, 3:34, 3:96
xxd	2:149, 2:166, 3:12, 3:34, 3:96

Y

Yet Another Markup Language (YAML)	2:33, 4:84
------------------------------------	------------

Z

Zap Fuzzer	4:129, 4:135
Zed Attack Proxy (ZAP)	1:9, 1:138, 3:142, 4:86, 4:127, 4:129, 4:131-133, 4:135, 4:140, 4:149, 5:12, 5:71, 5:103, 5:108
Zend	2:38, 2:85-87
Zero	2:91-92, 2:94, 2:107-108, 4:6, 4:8, 4:146, 5:46, 5:124, 5:138
Zope	2:38