Contents

1 The Relevance of Client-Side Web Security 1
1.1 The Web at a Glance 2
1.2 Client-Side Web Security 6
1.3 Purpose of this Book 8
References 9

2 Traditional Building Blocks of the Web 11
2.1 Traditional Web Technology 11
2.1.1 Loading Web Content 12
2.1.2 Authentication and Authorization 12
2.1.3 Cookies and Session Management 13
2.2 Browser Security Policies 14
2.2.1 Same-Origin Policy 14
2.2.2 Security Model for Third-Party Content Inclusion 15
2.2.3 Context Navigation Policy 17
2.3 Extending the Client-Side Features 18
2.3.1 Plugins for Arbitrary Content 19
2.3.2 Browser Extensions 20
2.4 Enhancing the User's Window on the Web 21
References 23

3 The Browser as a Platform 25
3.1 The Synergy Between Browsers and Devices 25
3.2 From Rendering Engine to Feature-Rich Platform 27
3.2.1 Client-Side Storage 27
3.2.2 Communication Mechanisms 28
3.2.3 Mobile Features 29
3.2.4 Registering Default Applications 29
3.3 Transforming the Browser into an Operating System 29
References 31

4 How Attackers Threaten the Web 33
4.1 Threat Models in Literature 33
4.1.1 Forum Poster 34
4.1.2 Web Attacker 34
4.1.3 Gadget Attacker 34
4.1.4 Related-Domain Attacker 35
4.1.5 Related-Path Attacker 35
4.1.6 Passive Network Attacker 36
4.1.7 Active Network Attacker 36
4.2 Threat Models as Concrete Attacker Capabilities 37
4.2.1 Send Requests to an Application 37
4.2.2 Register Own Domain 37
4.2.3 Host Content Under Own Domain 39
4.2.4 Respond to Requests from Own Domain 39
4.2.5 Register a Valid TLS Certificate for Own Domain 39
4.2.6 Manipulate Target's Domain-based Data 40
4.2.7 Manipulate Target's Client-Side Context 40
4.2.8 Eavesdrop on Network Traffic 40
4.2.9 Generate Network Traffic 40
4.2.10 Intercept and Manipulate Network Traffic 43
4.3 Conclusion 41
References 42

5 Attacks on the Network 43
5.1 Eavesdropping Attacks 43
5.1.1 Description 44
5.1.2 Mitigation Techniques 44
5.1.3 State of Practice 45
5.1.4 Best Practices 46
5.2 Man-in-the-Middle Attacks (MitM) 46
5.2.1 Description 47
5.2.2 Mitigation Techniques 48
5.2.3 State of Practice 49
5.2.4 Best Practices 50
5.3 Protocol-level Attacks on HTTPS 50
5.3.1 Overview of Attacks 51
5.3.2 State of Practice 52
References 53

6 Attacks on the Browser's Requests 57
6.1 Cross-Site Request Forgery 57
6.1.1 Description 58
6.1.2 Mitigation Techniques 60
6.1.3 State of Practice 62
6.1.4 Best Practices 62

6.2 UI Redressing 62
6.2.1 Description 63
6.2.2 Mitigation Techniques 65
6.2.3 State of Practice 66
6.2.4 Best Practices 66
References 66

7 Attacks on the User's Session 69
7.1 Session Hijacking 69
7.1.1 Description 69
7.1.2 Mitigation Techniques 71
7.1.3 State of Practice 73
7.1.4 Best Practices 73
7.2 Session Fixation 73
7.2.1 Description 74
7.2.2 Mitigation Techniques 75
7.2.3 State of Practice 76
7.2.4 Best Practices 76
7.3 Authenticating With Stolen Credentials 76
7.3.1 Description 77
7.3.2 Mitigation Techniques 77
7.3.3 State of Practice 79
7.3.4 Best Practices 79
References 79

8 Attacks on the Client-Side Context 83
8.1 Cross-Site Scripting 83
8.1.1 Description 84
8.1.2 Mitigation Techniques 85
8.1.3 State of Practice 86
8.1.4 Best Practices 87
8.2 Scriptless Injection Attacks 87
8.2.1 Description 87
8.2.2 Mitigation Techniques 88
8.2.3 Best Practices 89
8.3 Compromised Script Inclusions 89
8.3.1 Description 90
8.3.2 Mitigation Techniques 90
8.3.3 State of Practice 91
8.3.4 Best Practices 91
References 92

9 Attacks on the Client Device 95
9.1 Drive-By Downloads 95
9.1.1 Description 96

9.1.2 Mitigation Techniques 97
9.1.3 State of Practice 98
9.1.4 Best Practices 98
9.2 Malicious Browser Extensions 98
9.2.1 Description 99
9.2.2 Mitigation Techniques 99
9.2.3 State of Practice 100
9.2.4 Best Practices 101
References 101

10 Improving Client-Side Web Security 105
10.1 Overview of Best Practices 105
10.1.1 Secure Communication Channel 106
10.1.2 Application-level Techniques 106
10.1.3 Security Policies 107
10.2 Research-driven Security Technology 108
10.3 Conclusion 109
References 109

http://www.springer.com/978-3-319-12225-0

Primer on Client-Side Web Security

De Ryck, P.; Desmet, L.; Piessens, F.; Johns, M.

2014, X, 111 p. 13 illus., 12 illus. in color., Softcover
ISBN: 978-3-319-12225-0