

# Inhaltsverzeichnis

<b>I</b>	<b>Einleitung und Grundlagen</b>	<b>1</b>
<b>1</b>	<b>Einleitung</b>	<b>3</b>
<b>2</b>	<b>Grundlagen</b>	<b>5</b>
2.1	Hypertext Transfer Protocol	5
2.2	Sprachen	7
2.2.1	Hypertext Markup Language	7
2.2.1.1	Formulare	9
2.2.1.2	Framesets und Frames	11
2.2.1.3	Eingebettete Frames	13
2.2.1.4	HTML5	15
2.2.1.5	Validierung	16
2.2.2	Cascading Style Sheets	18
2.2.2.1	Anwendungsbeispiel	19
2.2.3	JavaScript	21
2.2.3.1	Anwendungsbeispiel	22
2.2.3.2	Document Object Model	23
2.2.4	Extensible Markup Language	26
2.2.4.1	Asynchronous JavaScript and XML	27
2.2.4.2	Scalable Vector Graphics	29
2.3	Anmerkungen und Literaturtipps	32
<b>II</b>	<b>Angriffe und Sicherheitsmechanismen im Webbrowser</b>	<b>35</b>
<b>3</b>	<b>Bekannte Angriffe und Schwachstellen</b>	<b>37</b>
3.1	Social Engineering und Information Disclosure	38
3.2	Logical Flaws	39
3.3	Cross-Site Request Forgery	41
3.4	Cross-Site Scripting	42
3.4.1	Nichtpersistentes XSS	42
3.4.2	Persistentes XSS	44
3.4.3	DOM-basiertes XSS	45
3.5	Session Hijacking	46

<b>4</b>	<b>Sicherheitsmechanismen im Webbrowser</b>	<b>49</b>
4.1	Same-Origin-Policy	50
4.2	HTML5-Angriffe	52
4.2.1	Selbstausslösende Event-Handler mit autofocus	52
4.2.2	XSS via formaction	53
4.3	Opera und SVG	54
<b>III</b>	<b>UI-Redressing und Clickjacking</b>	<b>57</b>
<b>5</b>	<b>Einordnung von UI-Redressing und Clickjacking</b>	<b>59</b>
<b>6</b>	<b>UI-Redressing – Definition und Angriffe</b>	<b>61</b>
6.1	Clickjacking	61
6.1.1	Classic-Clickjacking	63
6.1.2	Likejacking und Sharejacking	71
6.1.3	Ein Mausklick genügt	73
6.1.4	Cursorjacking	74
6.1.5	Filejacking	78
6.1.6	Drag&Drop-Operationen	80
6.1.7	Content extraction	83
6.1.8	Cookiejacking	86
6.1.9	Tabnabbing und Tapjacking	87
6.1.9.1	Ausnutzung von window.open	92
6.1.9.2	Chrome to Phone fernsteuern	95
6.1.10	Kombinationen mit CSRF, XSS und CSS	99
6.1.10.1	Der Twitter-Wurm	99
6.1.10.2	Eventjacking	103
6.1.10.3	Classjacking mit jQuery	105
6.1.10.4	Pointer-Events	107
6.1.10.5	Whole-page Clickjacking	111
6.2	Strokejacking	114
6.2.1	Keylogging ohne die Verwendung von Skriptsprachen	117
6.3	Pop-up-Blocker umgehen & Event-Recycling	120
6.3.1	Double-Clickjacking	123
6.4	SVG-Maskierungen	126
6.5	Clickjacking Tool	128
<b>7</b>	<b>Die Abwehrmaßnahmen: Frame-Busting</b>	<b>129</b>
7.1	JavaScript	130
7.2	X-Frame-Options	131
7.3	Content Security Policy	133
7.4	NoScript	134

<b>8</b>	<b>Angriffe auf Abwehrmaßnahmen: Busting-Frame-Busting</b>	<b>137</b>
8.1	Mobile und nicht mobile Webseiten	137
8.2	Doppeltes Framing	137
8.3	onBeforeUnload-Event-Handler ausnutzen	138
8.3.1	Normales Verhalten	138
8.3.2	Der HTTP-Header 204	140
8.4	XSS-Filter im IE und Chrome	142
8.4.1	Microsoft Internet Explorer	142
8.4.2	Google Chrome	143
8.5	JavaScript deaktivieren	144
8.5.1	Beschränkte Frames im Internet Explorer	144
8.5.2	Das sandbox-Attribut	144
8.5.3	Der Design-Modus	145
8.6	Sicherheitsverletzungen durch das location-Objekt	147
8.6.1	Microsoft Internet Explorer	147
8.6.2	Apple Safari	148
8.7	Ausnahmen beim Referrer benutzen	149
<b>9</b>	<b>Das Katz- und Mausspiel</b>	<b>151</b>
9.1	Der »ultimate« Frame-Busting-Code	151
9.2	Die defineProperty-Funktion	152
<b>IV</b>	<b>Ergänzende Informationen</b>	<b>155</b>
<b>10</b>	<b>Statistiken</b>	<b>157</b>
10.1	Frame-Buster	157
10.2	X-Frame-Options	159
10.3	Transparente Frames und Clickjacking-Angriffe	160
<b>11</b>	<b>Die häufigsten Irrtümer</b>	<b>163</b>
11.1	Clickjacking ist UI-Redressing	163
11.2	Clickjacking benötigt JavaScript-Code	164
11.3	JavaScript sollte deaktiviert werden	164
11.4	X-Frame-Options schützt gegen Clickjacking	164
11.5	Browserinterne XSS-Filter schützen den Benutzer	165
11.6	Sidejacking gehört zu Clickjacking	166
<b>12</b>	<b>Interviews mit bekannten Experten für das Clickjacking</b>	<b>167</b>
12.1	Robert Hansen (USA)	167
12.1.1	Über die Person	167
12.1.2	Interview	167
12.2	Jeremiah Grossman (USA)	170
12.2.1	Über die Person	170

12.2.2 Interview	170
12.3 Paul Stone (England)	172
12.3.1 Über die Person	172
12.3.2 Interview	172
12.4 Krzysztof Kotowicz (Polen)	174
12.4.1 Über die Person	174
12.4.2 Interview	174
12.5 Mario Heiderich (Deutschland)	176
12.5.1 Über die Person	176
12.5.2 Interview	176
<b>13 Hinweise für die jeweiligen Leser</b>	<b>179</b>
13.1 Browserhersteller	179
13.2 Administratoren und Webentwickler	180
13.3 Benutzer eines Webbrowsers	181
<b>14 Zusammenfassung und Ausblick</b>	<b>183</b>
<b>Danksagung und Feedback</b>	<b>185</b>
<b>Referenzen und weiterführende Literatur</b>	<b>187</b>
<b>Index</b>	<b>207</b>