Índice

Capítulo I
Introducción 13
1. Un mundo de nuevas APIs 13
2. La aventura de una API peligrosa 14
3. La amenaza continúa 15
4. De qué (no) trata este libro 16
5. El escenario 17

Capítulo II
En nombre de otros 19
1. Introducción 19
1.1 Hora de cambiar 19
2. Un escenario de ataque 21
3. POST 22
4. Diccionario 24
5. Contras de una contramedida 28
6. Jugando duro 28
7. Tomando el control 31
8. Protecciones 36

Capítulo III
Robando entradas 39
1. El fondo de escritorio 39
2. Poniendo nombres 42
3. Otro admin más 42

4. Lo contrario 46
5. Previniendo 49
6. Sin frames ni iframes 53
7. Proteger… sí. ¿Pero qué? ¿Y cómo? 57

Capítulo IV
Siguiendo indicaciones 61
1. Introducción 61
2. Riesgos evidentes y alguno no tanto 62
3. El estado de la sesión 64
3.1 Planteando el problema 64
3.2 Enfoque 65
3.3 Estudio del comportamiento 66
3.4 Implementación 68
4. Enfoques alternativos 70
5. Algunas conclusiones 73

Capítulo V
Rompiendo los escudos 75
1. Introducción 75
2. Bajo control 77
3. Activando "X-XSS-Protection: 1" 78
4. Un segundo ejemplo 84
5. Sacando partido de XSS Auditor 87
6. X-XSS-Protectcion: 1; mode=block 90
7. Blind XSS Auditor Testing 91
8. Sin redirecciones 94
9. Conclusiones 97

Capítulo VI
Lo que el ojo no ve 99
1. Introducción 99
2. Inyección de cabeceras 101
3. Sólo un punto de inyección 104

4. Anulando cabeceras 106
5. Más allá de las cabeceras 108
6. Cabeceras descontroladas 112

Capítulo VII
Engañando al usuario 117
1. Preocupaciones de un phisher 117
2. Nombres DNS y de host 118
3. Las circunstancias 121
4. El segundo truco 125
4.1 Aquello en lo que la víctima no se fijó 125
4.2 Jugando a ser un navegador 132
4.3 El proxy 133
4.4 Modificando lo existente 136
4.5 Redefiniendo los fundamentos 139
4.6 Conclusiones 141

Capítulo VIII
Caer en tus redes 143
1. El ataque más sencillo 143
2. Breaking the ICE 144
3. Usando la información 148
4. Escaneando equipos 148
5. Escaneando puertos 151

Capítulo IX
Adjunto remito... 159
1. El peligro de los adjuntos 159
2. Simplemente, por estar ahí 160
3. A unos sí. A otros no 162
4. Creando el contexto apropiado 164
5. La historia previa 165
6. Software y configuraciones 167
7. Al otro lado 171

Capítulo X
Sonría, por favor 183
1. Introducción 183
2. Cámara y micro 183
2.1 Primeros pasos 183
2.2 Mira a la cámara 185
3. Un primer engaño 188
4. Ocultando la barra de direcciones 190
5. Conclusiones 195

Capítulo XI
Ninguna tecnología es inofensiva 197
1. De vuelta a los filtros anti-XSS 197
2. Un login.php alternativo 199
3. Selectores, atributos y valores 200
4. Blind CSS injection 201
5. Detalles de implementación 204
6. Firefox 210
7. Conclusiones 211

Capítulo XII
Abriendo las ventanas de par en par 213
1. Introducción 213
2. Estrategias para abrir ventanas 214
2.1 La solución más obvia 214
2.2 El camino del evento 215
2.3 Multiplicidad de eventos 217
3. Resultados 218
3.1 Edge 218
3.2 Internet Explorer 219
3.3 Google Chrome 220
3.4 Firefox 220
4. Un caso práctico 221
5. El foco de atención 225
6. El ataque visto desde el servidor malicioso 227

7. La parte cliente del ataque 229
8. Dicho todo esto… 231

Índice alfabético 233

Índice de imágenes 235