

Índice

Introducción	13
1. Un mundo de nuevas APIs.....	13
2. El peso de un escudo.....	14
3. De qué trata este libro	15
4. La aplicación	16
5. El escenario	17
6. Junto a la aplicación.....	18
7. A partir de aquí.....	20
Capítulo I	
Los orígenes	21
1. Pioneros	21
2. La era de los excesos y la inocencia.....	21
3. Poniendo parches.....	22
4. Origen	23
5. CORS.....	24
6. Especial protección.....	25
7. Contexto seguro	28
8. Haciendo sitio.....	33
9. Restringiendo el acceso a la cookie	34
10. Evolucionando el concepto de sitio	38
11. No mezclar.....	41
12. Conclusiones	42

Capítulo II

Robando peticiones	43
1. Introducción.....	43
2. Un escenario de ataque	46
3. Cuestión de valores (por defecto).....	47
4. Disclaimer.....	48
5. Samesite=Lax.....	49
6. POST.....	50
7. Diccionario	52
Introducción	52
La segunda vulnerabilidad	53
El ataque.....	54
8. Contras de una contramedida.....	57
9. Jugando duro	57
10. Tomando el control.....	60
11. Protecciones.....	66
12. Conclusiones	68

Capítulo III

Robando entradas	71
1. Tocando fondo.....	71
2. Llegando al fondo	73
3. Poniendo nombres	73
4. El disfraz	74
5. Lo contrario	79
6. Previendo	81
Algunas condiciones	81
Evitando la encerrona con scripting.....	82
De cabecera	85
Olvidando la sesión.....	88
Pedir permiso	90
7. En un contexto principal.....	91
Jugar con fuego	91

8. Dos consejos útiles	98
9. Conclusiones	99

Capítulo IV

Robando espacio.....	101
1. Rellenando huecos	101
2. Más efectividad. Mayor efecto.	102
3. Sin necesidad de enviar	105
4. Protección.....	108
5. ¿Resuelto?	110
6. Para probar	111
7. Especificando	112
8. Demostrando quién es quién	117
9. Inocentes elementos.....	122
10. Defensas.....	124
11. Las migas de pan marcan el camino	124
12. La doble inyección	126
13. La perspectiva de la víctima	131
14. Encadenando el enlace	134
15. El triángulo	135
XSS	135
CSRF	136
Clickjacking	138
16. Cuestión de imagen	139
17. Lo que la aplicación puede controlar.....	142
18. Ninguna tecnología es inocente	143
Volviendo a girar la tuerca	143
Selectores, atributos y valores.....	144
Blind CSS Injection.....	146
Blind CSS Injection.....	148
La protección.....	152
19. CSP.....	152
20. Conclusiones	153

Capítulo V

Más allá del espejo	155
1. Malas elecciones.....	155
2. Donde se almacenan los ataques	157
3. De espaldas al servidor.....	160
4. Regalando una sesión (de forma interesada)	162
5. Escondiendo las galletas.....	164
6. El resquicio.....	166
7. Buscando la oportunidad.....	167
8. Las otras tres condiciones	169
9. Cuando todo es favorable	170
10. Cuando abrir no es una opción	173
11. Jugando a adivinar	174
12. El olor de los ficheros	178
13. Sin que el servidor lo sepa	180
14. Prevención y Detección	183
15. Las armas del futuro	188
16. El mundo al revés	195
17. De forma más explícita.....	197
18. Otra cabecera más.....	198
19. Conclusiones	200

Capítulo VI

Pescando en aguas revueltas	203
1. Preocupaciones de un phisher	203
2. Nombres DNS y de host	205
3. Al atacante le basta con una oportunidad	207
4. Las circunstancias	209
5. Misdirection	210
6. El segundo truco	212
7. A lo Crusoe	215

8. Recursos adicionales.....	217
9. No hay dos sin tres.....	218
10. Open significa abrir.....	221
11. Cuando las cosas no funcionan.....	222
12. Ver es creer.....	223
En lo que la víctima no se fijó.....	223
13. Algo parecido a la magia.....	225
14. Autophishing.....	228
15. Conclusiones.....	232
 Capítulo VII	
Descubrir el paisaje.....	233
1. Protegiendo lo propio.....	233
2. Una vez infiltrado.....	233
3. La infiltración.....	238
4. Reconociendo el barco.....	243
5. Historia de un ataque que dejó de funcionar.....	246
6. ¿Estás ahí?.....	247
7. Por partes.....	249
8. Routers.....	250
9. Mirarse en el espejo.....	252
10. Analizando el rango.....	256
11. Llegando a buen puerto.....	258
12. Conclusiones.....	262
 Índice de imágenes.....	263
 Índice alfabético.....	269
 Otros libros publicados.....	271

