

# Índice

<b>Prólogo .....</b>	<b>13</b>
<b>Capítulo I</b>	
<b>Programas de Bug Bounty .....</b>	<b>15</b>
<b>1. Ámbito .....</b>	<b>15</b>
Origen y evolución .....	15
Perfil del Bug Hunter .....	16
<b>2. Mecánica de los programas .....</b>	<b>19</b>
Plataformas de reporte .....	19
Ficha de programa .....	21
Alcance del programa .....	22
Reporte de vulnerabilidades .....	25
Cobro de recompensas .....	27
Mecánica para las compañías .....	27
<b>3. Tipos de programas .....</b>	<b>28</b>
Programas públicos .....	28
Programas privados .....	29
<b>4. Principales plataformas .....</b>	<b>29</b>
HackerOne .....	29
Bugcrowd .....	33
Intigriti .....	38
YesWeHack .....	41
Programas propios .....	44
<b>5. Escribir un reporte .....</b>	<b>45</b>
Estructura y contenido .....	45
Ejemplos .....	48
Automatización .....	51
<b>6. Gestión psicológica .....</b>	<b>52</b>
Advertencias .....	52
Hábitos saludables .....	53

Fijación de objetivos .....	54
<b>7. Fiscalidad de las recompensas España .....</b>	<b>55</b>
 <b>Capítulo II</b>	
<b>Metodología .....</b>	<b>57</b>
<b>1. Ámbito .....</b>	<b>57</b>
Elegir un programa .....	57
Preparación previa .....	58
Seguimiento y trazabilidad .....	59
Flujo de trabajo .....	60
Automatización .....	61
<b>2. Enumeración .....</b>	<b>61</b>
FOCA .....	62
Censys .....	64
Amass .....	64
Sublist3r .....	66
Shodan .....	67
Certificate Search (crt.sh) .....	69
<b>3. Limpieza .....</b>	<b>70</b>
Massdns .....	70
<b>4. Visualización .....</b>	<b>71</b>
EyeWitness .....	71
<b>5. Análisis .....</b>	<b>72</b>
BurpSuite .....	72
Chrome DevTools .....	78
<b>6. Automatización .....</b>	<b>87</b>
LazyRecon .....	87
Offensive Ai .....	88
 <b>Capítulo III</b>	
<b>Low Hanging Fruit .....</b>	<b>91</b>
<b>1. Ámbito .....</b>	<b>91</b>
<b>2. Fugas de información .....</b>	<b>91</b>
Introducción .....	91
Impacto .....	92
Google Dorking .....	92
GitHub .....	96
Wayback Machine .....	99

Ejemplos.....	101
<b>3. Subdomain Takeover.....</b>	<b>104</b>
Introducción.....	104
Impacto.....	107
Metodología.....	109
Ejemplos.....	110
<b>4. Open Redirect.....</b>	<b>113</b>
Introducción.....	113
Impacto.....	113
Metodología.....	115
Ejemplos.....	119
 <b>Capítulo IV</b>	
<b>High Hanging Fruit.....</b>	<b>123</b>
<b>1. Ámbito.....</b>	<b>123</b>
<b>2. Cross-site Scripting (XSS).....</b>	<b>125</b>
Introducción.....	125
Impacto.....	127
Metodología.....	128
Ejemplos.....	131
<b>3. Broken Authentication.....</b>	<b>135</b>
Introducción.....	135
Impacto.....	135
Metodología.....	137
Ejemplos.....	137
<b>4. Information Disclosure.....</b>	<b>139</b>
Introducción.....	139
Impacto.....	140
Metodología.....	141
Ejemplos.....	142
<b>5. Vertical Privilege Escalation.....</b>	<b>144</b>
Introducción.....	144
Impacto.....	145
Metodología.....	146
Ejemplos.....	146
<b>6. SQL Injection.....</b>	<b>149</b>
Introducción.....	149
Impacto.....	151
Metodología.....	153

Ejemplos.....	156
<b>7. Business logic flaws.....</b>	<b>158</b>
Introducción .....	158
Impacto.....	159
Metodología .....	160
Ejemplos.....	160
<b>8. Insecure Direct Object Reference (IDOR).....</b>	<b>161</b>
Introducción .....	161
Impacto.....	161
Metodología .....	162
Ejemplos.....	165
<b>9. Cross-Site Request Forgery (CSRF).....</b>	<b>167</b>
Introducción .....	167
Impacto.....	168
Metodología .....	169
Ejemplos.....	170
<b>10. Server-Side Request Forgery (SSRF) .....</b>	<b>172</b>
Introducción .....	172
Impacto.....	173
Metodología .....	174
Ejemplos.....	174
<b>11. Remote Code Execution (RCE).....</b>	<b>176</b>
Introducción .....	176
Impacto.....	176
Metodología .....	177
Ejemplos.....	177

## Capítulo V

<b>Bug Bounty en dispositivos móviles.....</b>	<b>181</b>
<b>1. Ámbito.....</b>	<b>181</b>
Tipos de aplicaciones .....	183
Vulnerabilidades comunes .....	183
<b>2. Android.....</b>	<b>184</b>
Introducción .....	184
Herramientas .....	185
Casos reales.....	188
<b>3. iOS .....</b>	<b>193</b>
Introducción .....	193
Herramientas .....	194

Casos reales.....	196
<b>4. IoT.....</b>	<b>198</b>
Introducción.....	198
Vulnerabilidades comunes.....	200
Casos reales - Car Hacking.....	201
<b>Capítulo VI</b>	
<b>Comunidad Bug Bounty.....</b>	<b>205</b>
<b>1. Ámbito.....</b>	<b>205</b>
<b>2. Grandes Bugs &gt;10.000 \$.....</b>	<b>206</b>
iPhone Camera Hack: 75.000\$.....	206
Robo de cuenta de Instagram: 40.000\$.....	207
Leaks de información: 30.000\$.....	209
User Data Disclosure en Facebook: 10.000\$.....	210
IDOR en PayPal: 10.500\$.....	212
<b>3. Bugs Intermedios: 500\$ - 10.000 \$.....</b>	<b>213</b>
XSS en Google Translate: 5.000\$.....	213
IDOR en Airbnb: 3.000\$.....	214
URL Spoofing en Facebook y Messenger: 3.000\$.....	215
Subdomain takeover en Starbucks: 2.000\$.....	216
Ataque de fuerza bruta en Instagram: 1.000\$.....	217
<b>4. Quick wins: 100\$ - 500 \$.....</b>	<b>219</b>
Directory listing: 500\$.....	219
Open redirect: 250\$.....	221
Leak de e-mails vía recuperación de contraseña: 250\$.....	221
Error de lógica de negocio en Reverb: 200\$.....	222
Host header injection en Starbucks: 150\$.....	224
<b>5. Recursos y aprendizaje.....</b>	<b>226</b>
Hacker101.....	226
Bugcrowd University.....	228
Intigriti Hackademy.....	229
YesWeHack Dojo.....	231
PortSwigger Academy.....	234
Influencers.....	236
Conferencias.....	238
<b>Conclusiones.....</b>	<b>241</b>
<b>Índice alfabético.....</b>	<b>243</b>

Índice de imágenes .....	247
Otros libros publicados.....	257