Sécurité informatique sur le Web

Apprenez à sécuriser vos applications (management, cybersécurité, développement et opérationnel)

Introduction à la sécurité des applications web

1. Quelques chiffres sur le Web et la sécurité **9**

2. À qui s'adresse ce livre ? **11**

3. Anatomie d'une application web **11**

4. Frameworks et CMS **15**

5. Méthodes classiques et méthodes agiles **17**

6. Sécurité des systèmes d'information **19**

7. Les différents axes de sécurisation d'une application web **21**

8. DevSecOps **22**

Panorama de la sécurité web

1. Introduction **25**

2. Les normes et référentiels **25**

2.1 ISO/IEC 27034 25

2.2 PCI-DSS et PA-DSS 28
2.3 HIPAA 31
2.4 CNIL (commission nationale de l'informatique et des libertés) 32
2.5 GDPR (General Data Protection Regulation) 34

3. Les bibliothèques, projets et recommandations 35

3.1 MITRE CWE 35
3.2 BSIMM 37
3.3 OpenSAMM 40
3.4 SDL de Microsoft 43
3.5 Cigital touchpoint 44
3.6 OWASP CLASP 45
3.7 Note technique de l’ANSSI 46
3.8 Recommandations du CLUSIF 47
3.9 NIST 48

4. Les guides et bonnes pratiques 48

4.1 OWASP TOP 10 48
4.2 OWASP testing guide 50
4.3 OWASP ASVS 52
4.4 OWASP code review guide 54

5. Les technologies liées à la sécurité web **57**

5.1 Analyse de code statique (SAST) 57

5.2 Analyse de code dynamique (DAST) 59

5.3 Tests interactifs de la sécurité des applications (IAST) 60

5.4 Autoprotection des applications (RASP) 61

5.5 Pare-feu applicatif (WAF) 61

5.6 Outil de suivi de bugs (issue tracking system) 63

6. La sécurité des navigateurs et serveurs web **64**

6.1 SOP, CORS 64

6.2 HSTS 68

6.3 X-frame-options, x-content-type-options, x-xss-protection 70

6.4 Content Security Policy 73

6.5 FLAG SECURE, HTTPONLY COOKIE 74

6.6 Authentification HTTP 77

Top 10 des risques et vulnérabilités liés au Web

1. Le top 10 des menaces du Web **81**

2. Comprendre les risques selon l'OWASP **82**

3. Installation de la plateforme de travail **83**

4. Les injections **89**

4.1 Les risques 89

4.2 Injection SQL 90

4.3 Injection XPath 107

4.4 Injection XXE (XML External Entity) 110

4.5 Injection LDAP 111

4.6 Injection de code 113

5. Violation de gestion d'authentification et de session **116**

5.1 Présentation et risques 116

5.2 Vol de session (session hijacking) 117

5.3 Faiblesses des mots de passe 118

5.4 Mot de passe non protégé en base de données 122

5.5 Faiblesses dans la conception des sessions 125

6. Cross-Site Scripting (XSS) **127**

6.1 Présentation et risques 127

6.2 XSS stocké (stored) 128

6.3 XSS Réfléchi (reflected) 133

6.4 XSS DOM (Document Object Model)

138

7. Références directes non sécurisées à un objet **141**

7.1 Présentation et risques 141

7.2 Entrées directes cachées et non contrôlées 142

7.3 Entrées indirectes cachées et non contrôlées 143

8. Mauvaise configuration de sécurité **145**

8.1 Présentation et risques 145

8.2 Scénarios 146

9. Exposition de données sensibles **147**

9.1 Présentation et risques 147

9.2 Scénarios 149

10. Manque de contrôle d'accès au niveau fonctionnel **150**

10.1 Présentation et risques 150

10.2 Local/remote file inclusion 151

10.3 Host Header Attack 153

10.4 User-agent spoofing 158

10.5 Server Side Request Forgery (SSRF) 159

11. Cross Site Request Forgery (CSRF) **160**

11.1 Présentation et risques 160
11.2 CSRF et requête POST 162

12. Exploitation de vulnérabilités connues 164

12.1 Présentation et risques 164
12.2 WPScan 165
12.3 Nikto 166
12.4 OpenVAS 167
12.5 Qualys SSL Labs 169

13. Redirections et renvois non validés 170

Les concepts du développement sécurisé

1. Les 10 commandements du code sécurisé 173

1.1 Authentification 174
1.2 Management des sessions 175
1.3 Contrôle d'accès 176
1.4 Validation des entrées 176
1.5 Encodage des sorties 177
1.6 Upload de fichiers 178
1.7 XSS

1.8 CSRF 178
1.9 Clickjacking 178
1.10 Enregistrement des événements 179
2. Outils indispensables de la sécurité web 179
180
2.1 Analyse de code 180
2.2 Fuzzing 183
2.3 Web Application Firewall (WAF) 184
2.4 Scan de vulnérabilités 187
2.5 Test de pénétration (Pentest) 193
3. Secure by design 195
195
3.1 Réduction des surfaces d’attaque 195
3.2 Défense en profondeur 200
3.3 Séparation des privilèges 201
3.4 Paramètres par défaut respectant la sécurité 202
4. Modélisation des menaces (threat modeling) 202
202
4.1 Qu’est-ce que la modélisation des menaces ? 202
4.2 Schéma de votre architecture avec DFD 204
4.3 Identification des menaces avec la méthode STRIDE 209

4.4 Documentation et atténuation des menaces 212
4.5 Validation de votre rapport 213

5. Respect de la vie privée 213

5.1 Types de données personnelles 213
5.2 Principes de la protection des données personnelles 214
5.3 Notifications 216
5.4 Consentements 217

Établir un cycle de développement sécurisé

1. Introduction 219

2. Sensibilisation des parties prenantes 222

2.1 Thèmes à enseigner 222
2.2 Évaluation des stagiaires 224
2.3 Exemple 233

3. Exigences 236

3.1 Définition du projet 236
3.2 Évaluation des exigences pour la sécurité 238
3.3 Évaluation des exigences pour les données personnelles 242

3.4 Plan d'action et analyse des coûts 248
3.5 Identification du responsable et du conseiller 250
3.6 Amélioration de la gestion des bugs 251
3.7 Exemple 252

4. Conception 263

4.1 Définition des exigences de conception 263
4.2 Réduction de la surface d'attaque 268
4.3 Modélisation des menaces (Threat Modeling) 270
4.4 Exemple 272

5. Code 277

5.1 Revue de code manuelle 277
5.2 Management des sessions 279
5.3 Contrôle d'accès 280
5.4 Validation des entrées 280
5.5 Encodage des sorties 281
5.6 Upload de fichiers 281
5.7 XSS 282
5.8 CSRF 282
5.9 Clickjacking 283
5.10 Enregistrement des événements

5.11 Blacklist des fonctions obsolètes 283
5.12 Analyse statique du code 284
5.13 Exemple 287

6. Test 289

6.1 Analyse dynamique **291**
6.2 Test de fuzzing 291
6.3 Test de pénétration (Pentest) 292
6.4 Exemple 292
295

7. Déploiement 297

7.1 Création d'un plan de réponse aux incidents **297**
7.2 Conduite d'une revue finale 297
7.3 Exemple 301
302

Aller plus loin avec un modèle de maturité

1. Process model vs maturity model **307**

2. BSIMM vs OpenSAMM **308**

2.1 BSIMM 308
2.2 De OpenSAMM

311

3. Exemple **313**

3.1 Questionnaire d'évaluation 313

3.2 Création de scorecard 320

3.3 Mise en place d'une feuille de route 321

4. Conclusion **326**

Conclusion 327

Index 329