

Sécurité informatique sur le Web

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

Collection
Epsilon

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EPSECAW** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Préface

Avant-propos

Chapitre 1

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

Chapitre 2

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

2 — Sécurité informatique sur le Web

Apprenez à sécuriser vos applications

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	Digital 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

Chapitre 3

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

4 — Sécurité informatique sur le Web

Apprenez à sécuriser vos applications

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

Chapitre 4

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	178
1.8 CSRF	178

- 1.9 Clickjacking. 179
- 1.10 Enregistrement des événements 179
- 2. Outils indispensables de la sécurité web 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
 - 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
 - 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

6 — Sécurité informatique sur le Web

Apprenez à sécuriser vos applications

Chapitre 5

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	283
5.11 Blacklist des fonctions obsolètes	284

- 5.12 Analyse statique du code 287
- 5.13 Exemple..... 289
- 6. Test 291
 - 6.1 Analyse dynamique 291
 - 6.2 Test de fuzzing 292
 - 6.3 Test de pénétration (Pentest) 292
 - 6.4 Exemple..... 295
- 7. Déploiement 297
 - 7.1 Création d'un plan de réponse aux incidents 297
 - 7.2 Conduite d'une revue finale..... 301
 - 7.3 Exemple..... 302

Chapitre 6
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

Editions ENI

Sécurité informatique et Malwares

**Analyse des menaces
et mise en œuvre des contre-mesures**

(2^e édition)

Collection
Epsilon

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EP2MAL** dans la zone de recherche
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1

Identification d'un malware

1. Présentation des malwares par familles	9
1.1 Introduction	9
1.2 Backdoor	10
1.3 Ransomware et locker	11
1.4 Stealer	12
1.5 Rootkit	12
2. Scénario d'infection	14
2.1 Introduction	14
2.2 Scénario 1 : l'exécution d'une pièce jointe	14
2.3 Scénario 2 : le clic malencontreux	15
2.4 Scénario 3 : l'ouverture d'un document infecté	16
2.5 Scénario 4 : les attaques informatiques	16
2.6 Scénario 5 : les attaques physiques : infection par clé USB	17
3. Techniques de communication avec le C&C	17
3.1 Introduction	17
3.2 Mise à jour de la liste des noms de domaine	18
3.3 Communication via HTTP/HTTPS/FTP/IRC	18
3.4 Communication via e-mail	19
3.5 Communication via un réseau point à point	19
3.6 Communication via des protocoles propriétaires	19
3.7 Communication passive	19
3.8 Fast flux et DGA (Domain Generation Algorithms)	20

2 _____ Sécurité informatique et Malwares

Analyse des menaces et mise en œuvre des contre-mesures

4.	Collecte d'informations	21
4.1	Introduction	21
4.2	Collecte et analyse de la base de registre.	22
4.3	Collecte et analyse des journaux d'événements	24
4.4	Collecte et analyse des fichiers exécutés au démarrage	25
4.5	Collecte et analyse du système de fichiers	26
4.6	Gestion des fichiers bloqués par le système d'exploitation	32
4.7	Framework d'investigation inforensique.	33
4.8	Outil FastIR Collector	35
5.	Image mémoire	37
5.1	Présentation	37
5.2	Réalisation d'une image mémoire	38
5.3	Analyse d'une image mémoire	41
5.4	Analyse de l'image mémoire d'un processus	48
6.	Fonctionnalités des malwares	49
6.1	Techniques pour rester persistant	49
6.2	Techniques pour se cacher	51
6.3	Malware sans fichier	55
6.4	Contournement de l'UAC	56
7.	Mode opératoire en cas d'attaques ciblées persistantes (APT)	57
7.1	Introduction	57
7.2	Phase 1 : reconnaissance.	58
7.3	Phase 2 : intrusion	58
7.4	Phase 3 : persistance	59
7.5	Phase 4 : pivot	59
7.6	Phase 5 : exfiltration.	60
7.7	Traces laissées par l'attaquant	60
8.	Conclusion	61

Chapitre 2
Analyse de base

- 1. Création d'un laboratoire d'analyse 63
 - 1.1 Introduction 63
 - 1.2 VirtualBox 64
 - 1.3 L'outil de gestion d'échantillons de malware Viper 70
- 2. Informations sur un fichier 76
 - 2.1 Format d'un fichier 76
 - 2.2 Chaînes de caractères présentes dans un fichier 77
- 3. Analyse dans le cas d'un fichier PDF 79
 - 3.1 Introduction 79
 - 3.2 Extraire le code JavaScript 79
 - 3.3 Désobfusquer du code JavaScript 84
 - 3.4 Conclusion 88
- 4. Analyse dans le cas d'un fichier Adobe Flash 88
 - 4.1 Introduction 88
 - 4.2 Extraire et analyser le code ActionScript 89
- 5. Analyse dans le cas d'un fichier JAR 90
 - 5.1 Introduction 90
 - 5.2 Récupération du code source depuis les classes 91
- 6. Analyse dans le cas d'un fichier Microsoft Office 93
 - 6.1 Introduction 93
 - 6.2 Outils permettant l'analyse de fichiers Office 93
 - 6.3 Cas de malware utilisant des macros : Dridex 94
 - 6.4 Cas de malware utilisant une vulnérabilité 96
- 7. Utilisation de PowerShell 98
- 8. Analyse dans le cas d'un binaire 98
 - 8.1 Analyse de binaires développés en AutoIt 98
 - 8.2 Analyse de binaires développés avec le framework .NET 100
 - 8.3 Analyse de binaires développés en C ou C++ 101

4 Sécurité informatique et Malwares

Analyse des menaces et mise en œuvre des contre-mesures

9. Le format PE	101
9.1 Introduction	101
9.2 Schéma du format PE	102
9.3 Outils pour analyser un PE	109
9.4 API d'analyse d'un PE	112
10. Suivre l'exécution d'un binaire	116
10.1 Introduction	116
10.2 Activité au niveau de la base de registre	117
10.3 Activité au niveau du système de fichiers	119
10.4 Activité réseau	120
10.5 Activité réseau de type HTTP(S)	128
11. Utilisation de Cuckoo Sandbox	129
11.1 Introduction	129
11.2 Configuration	130
11.3 Utilisation	135
11.4 Limitations	144
11.5 Conclusion	146
12. Ressources sur Internet concernant les malwares	146
12.1 Introduction	146
12.2 Sites permettant des analyses en ligne	146
12.3 Sites présentant des analyses techniques	151
12.4 Sites permettant de télécharger des samples de malwares	153

Chapitre 3

Reverse engineering

1. Introduction	155
1.1 Présentation	155
1.2 Législation	156
2. Assembleur x86	157
2.1 Registres	157
2.2 Instructions et opérations	162

2.3	Gestion de la mémoire par la pile	169
2.4	Gestion de la mémoire par le tas	171
2.5	Optimisation du compilateur	172
3.	Assembleur x64	173
3.1	Registres	173
3.2	Paramètres des fonctions	173
4.	Analyse statique	174
4.1	Présentation	174
4.2	IDA Pro	175
4.2.1	Présentation	175
4.2.2	Navigation	178
4.2.3	Renommages et commentaires	181
4.2.4	Script	182
4.2.5	Plug-ins	183
4.3	Radare2	187
4.3.1	Présentation	187
4.3.2	Ligne de commande	187
4.3.3	Interfaces graphiques non officielles	189
4.4	Techniques d'analyse	189
4.4.1	Commencer une analyse	189
4.4.2	Sauts conditionnels	191
4.4.3	Boucles	192
4.5	API Windows	193
4.5.1	Introduction	193
4.5.2	API d'accès aux fichiers	194
4.5.3	API d'accès à la base de registre	197
4.5.4	API de communication réseau	203
4.5.5	API de gestion des services	208
4.5.6	API des objets COM	210
4.5.7	Exemples de l'utilisation de l'API	211
4.5.8	Conclusion	220
4.6	Limites de l'analyse statique	220

6 Sécurité informatique et Malwares

Analyse des menaces et mise en œuvre des contre-mesures

5. Analyse dynamique	220
5.1 Présentation	220
5.2 Immunity Debugger	221
5.2.1 Présentation	221
5.2.2 Contrôle de flux d'exécution	225
5.2.3 Analyse d'une librairie	229
5.2.4 Points d'arrêt	230
5.2.5 Visualisation des valeurs en mémoire	232
5.2.6 Copie de la mémoire	233
5.2.7 Support du langage Python	234
5.2.8 Conclusion	235
5.3 WinDbg	235
5.3.1 Présentation	235
5.3.2 Interface	236
5.3.3 Commandes de base	238
5.3.4 Plug-in	243
5.3.5 Conclusion	244
5.4 Analyse noyau Windows	244
5.4.1 Présentation	244
5.4.2 Mise en place de l'environnement	244
5.4.3 Protections kernel Windows	245
5.4.4 Conclusion	246
5.5 Limites de l'analyse dynamique et conclusion	246

Chapitre 4 Techniques d'obfuscation

1. Introduction	247
2. Obfuscation des chaînes de caractères	249
2.1 Introduction	249
2.2 Cas de l'utilisation de ROT13	249
2.3 Cas de l'utilisation de la fonction XOR avec une clé statique	252

- 2.4 Cas de l'utilisation de la fonction XOR avec une clé dynamique 258
- 2.5 Cas de l'utilisation de fonctions cryptographiques 260
- 2.6 Cas de l'utilisation de fonctions personnalisées 267
- 2.7 Outils permettant de décoder les chaînes de caractères. 276
- 3. Obfuscation de l'utilisation de l'API Windows 277
 - 3.1 Introduction 277
 - 3.2 Étude du cas Duqu 278
 - 3.3 Étude du cas EvilBunny 282
- 4. Packers 284
 - 4.1 Introduction 284
 - 4.2 Packers utilisant la pile 286
 - 4.3 Packers utilisant le tas 299
 - 4.4 Encodeur Metasploit 308
- 5. Autres techniques 310
 - 5.1 Anti-VM 310
 - 5.2 Anti-reverse engineering et anti-debug 312
- 6. Conclusion 316

Chapitre 5
Détection, confinement et éradication

- 1. Introduction 317
- 2. Indicateurs de compromission réseau 318
 - 2.1 Présentation 318
 - 2.2 Utilisation des proxys 319
 - 2.3 Utilisation des détecteurs d'intrusions 322
 - 2.4 Cas complexes 324
- 3. Détection de fichiers 325
 - 3.1 Présentation 325
 - 3.2 Empreintes (ou Hash) 326
 - 3.3 Signatures avec YARA 328

8 _____ Sécurité informatique et Malwares

Analyse des menaces et mise en œuvre des contre-mesures

3.4	Signatures avec ssdeep	335
4.	Détection et éradication de malwares avec ClamAV.....	337
4.1	Présentation	337
4.2	Installation	338
4.3	Utilisation.....	340
5.	Artefacts système	347
5.1	Types d'artefacts.....	347
5.2	Outils.....	348
6.	Utilisation d'OpenIOC.....	350
6.1	Présentation	350
6.2	Utilisation.....	351
6.3	Interface graphique d'édition.....	352
6.4	Détection.....	355
7.	Conclusion	361
	Index	363