

Sommaire

Présentation générale.....	7
Les «Hackers».....	7
Différents types de sécurités informatiques.....	8
Principe de la sécurisation des sites Internet.....	9
Connaissances informatiques.....	9
L'expérience.....	10
Définition d'une «vulnérabilité».....	10
Méthodologie et professionnalisme.....	11
Législation.....	11
A propos de cet ouvrage.....	13
Les différentes parties du livre.....	13
A qui s'adresse ce livre.....	14
Connaissance des protocoles Internet.....	16
Présentation d'Internet.....	16
Origine d'Internet.....	16
L'adressage sous Internet.....	17
Limite de l'adressage sous Internet.....	17
L'URL.....	18
Le protocole d'Internet.....	19
L'interface avec les programmes utilisateurs.....	20
La couche Application.....	21
Le protocole FTP.....	22
Le protocole HTTP.....	27
Le protocole IMAP.....	34
Le protocole IRC.....	34
Le protocole NNPT.....	35
Le protocole POP3.....	35
Le protocole SMTP.....	39
Le protocole TELNET.....	43
Le protocole SSL.....	47
Les flux RSS.....	49
Nouvelles tendances de développement d'applications Internet.....	49
XML et XHTML.....	49
Le Web 2.....	50
Ajax.....	51
SOAP.....	51
J2EE.....	51
Vulnérabilité associée au hachage.....	51
Le codage URL.....	52
Le codage en Base 64.....	52
Le codage MD5.....	52
Le codage SHA.....	53
Serveurs Internet.....	53
Méthodologie de détection de vulnérabilités.....	54

Etape 1 : Connaissance de l'entreprise.....	54
Examen général de la cible	55
Analyse de l'adresse IP.....	56
Recherche via la Whois	57
Etape 2 : Analyse de la structure du site et du code source	59
Analyse du code source	59
Recherche du type de serveur	62
Recherche de répertoires et fichiers cachés	63
Etape 3 : Recherche de vulnérabilités	65
Vulnérabilité URL	65
Vulnérabilité Header.....	67
Vulnérabilité CRLF	69
Vulnérabilités XSS	71
Vulnérabilité Cross Site Request Forgery ou CSRF.....	75
Vulnérabilité Injection SQL	76
Vulnérabilité Include	83
Vulnérabilité Upload	87
Vulnérabilité Reverse Directory Transversal	90
Vulnérabilité Authentification	91
Vulnérabilité HTTP authentification	93
Vulnérabilité Session.....	94
Vulnérabilité robots.txt.....	96
Vulnérabilités associées à la configuration d'Apache.....	97
Vulnérabilité BufferOverflow	99
Vulnérabilité cgi-bin.....	100
Attaques suite aux messages d'erreur	101
Vulnérabilités associées aux bibliothèques de logiciels	102
Vulnérabilités liées aux outils de développement.....	102
Vulnérabilités spécifiques aux hébergeurs	103
Les scanners de vulnérabilités.....	104
Acunetix.....	104
BurpSuite	105
DirBuster	106
Exploit-Me.....	108
HP Web Inspect.....	109
Rational AppScan.....	111
WebScarab.....	113
Wikto	114
Le Top 10 des menaces actuelles	116
Scénarios d'attaques.....	117
Scénario 1 : Revendication politique	117
Contexte:.....	117
Scénario:	117
Analyse du scénario.....	118
Scénario 2 : Modification de notes d'examen	118
Contexte.....	118
Scénario	118
Analyse du scénario.....	119

Sécurisation	120
Ingénierie sociale.....	121
Définition	121
Exemples de cas d'ingénierie sociale	121
L'arnaque nigérienne.....	121
L'appel au secours.....	122
Sécurisation	124
Modèle de menaces	125
Les normes sur la sécurité de l'information.....	125
Concept d'un modèle de menaces	126
L'analyse de risques	126
Vraisemblance technique de l'attaque.....	127
Les impacts techniques	128
Les impacts commerciaux	129
Calcul du risque	131
Remarques	132
Modèle de vulnérabilité	132
Identifier les objectifs de sécurité	133
Architecture de l'application	133
Fonctionnement de l'application	133
Identifier les menaces	134
Identifier les vulnérabilités	134
Exemple concret d'un modèle de menace	135
Objectifs de sécurisation.....	135
Architecture du site.....	136
Fonctionnement du site.....	137
Identification des vulnérabilités.....	145
Les menaces.....	145
Niveau de risques.....	147
Mesures & actions	148
Que faire si j'ai été hacké.....	151
Mon site a été defacé.....	151
Mon site a été piraté	151
Prévention	152
Contre-attaquer.....	152
Porter plainte.....	152
Quelques remarques complémentaires	153
A propos de Javascript & Java.....	153
Génération de page HTML sur le serveur	153
Base de Données de vulnérabilités.....	154
ANNEXES	155
Bibliographie.....	156
Articles.....	156
Abréviations.....	157
Exemples de répertoires connus.....	159
Exemples de fichiers et extensions connus	161
Exemples de vulnérabilités XSS	162
Exemples de Méta caractères à filtrer	163



Exemples de vulnérabilités CGI connues	164
Vulnérabilité directement sur le composant cgi-bin	164
Vulnérabilités exploitables via les formulaires associés au cgi-bin.....	166
Exemples d'outils de tests	169
Exemple de configuration PHP	170