***(Ce document est uniquement un exemple de rapport à adapter qui se base sur le top 10 OWASP, merci de ne pas l’utiliser tel quel à l’examen)***

**Rapport de Pentest – Exemple.com**

**Details d’audit**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Référence** : |  | AAAA-MM |  |  | **Version :** | **1.0** |
| Type : |  | Audit de sécurité **technique (pentest)** |  |  | | |
| Date : |  | **JJ/MM/AAAA** |  |  | Durée : | 7 jours |
| Lieu : |  | Audit en ligne |  |  | Contact : | adresse@mail.com |
| Nom de l’auditeur : | | XX |  |  |  |  |

Table des matières

[Contexte et cadre du test d’intrusion 1](#_Toc178600726)

[Méthodologie et classification 1](#_Toc178600727)

[Types de preuve et de correction 2](#_Toc178600728)

[Périmètre technique 3](#_Toc178600729)

[Participants 3](#_Toc178600730)

[Sommaire des Vulnérabilités trouvées et recommandations 3](#_Toc178600731)

[Résumé de l’expertise et recommandations 3](#_Toc178600732)

[Analyse du risque global 3](#_Toc178600733)

[Détails des vulnérabilités 5](#_Toc178600734)

[A3:2017 : Exposition de données sensibles [Mettre un numéro arbitraire, un CWE ou l’identifiant CVE si besoin, ici « A3:2017 » vient du référentiel Owasp et est à utiliser uniquement s’il y a des vulnérabilités web] 5](#_Toc178600735)

[A2:2017 Contrôle d’authentification non sécurisé 5](#_Toc178600736)

[A5:2017 : Contrôle d’accès non sécurisé 6](#_Toc178600737)

[A7:2017 : Cross-site scripting 6](#_Toc178600738)

[Annexes 7](#_Toc178600739)

# Contexte et cadre du test d’intrusion

Michel KARTNER (Cyberini) a été invité à réaliser un audit de sécurité technique pour la société EXEMPLE, éditrice du site exemple.com sur lequel [CONTEXTE ET ACTIVITE].

Après premières prises de contact au sujet de la mise en place technique de [BESOINS], il a été rapporté [PROBLEME A REGLER]. Dans ce contexte de sécurisation du site, un contrat d’audit a été établi pour tester plus généralement la sécurité de la plateforme exemple.com par le protocole dit « en boite noire ». Le pentest concerne le site exemple.com ainsi que [CADRE VISE].

# Méthodologie et classification

La méthodologie employée est le test dit en boite « noire » sans connaissance préalable du fonctionnement interne du système visé. Plus particulièrement, la « Cyber kill chain » a été suivie et adaptée sous forme de 4 phases telles que spécifiées ci-dessous :

• Phase 1 : Reconnaissance – recherche de détails sur la cible

• Phase 2 : Scan réseau – recherche de services actifs et de vulnérabilités probables

• Phase 3 : Exploitation des vulnérabilités – envers les services vulnérables

• Phase 4 : Post-exploitation – actions supplémentaires et élévation de privilèges

Le tableau suivant récapitule les niveaux de criticité basés sur le [*Common Vulnerability Scoring System*](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) (CVSS). Ce système se base sur 3 métriques :

1. la métrique de **base** est unique et immuable, elle se base sur les qualités intrinsèques de la vulnérabilité.
2. la métrique **temporelle** est unique mais peut évoluer au cours du temps.
3. la métrique **environnementale** est multiple et évolue en fonction de l'environnement informatique. Elle dépend du système informatique dans lequel elle est présente.

Tableau récapitulatif des niveaux de criticité vulnérabilité :

|  |  |  |
| --- | --- | --- |
| **Critique** | 9-10 | Les vulnérabilités de niveau critique sont exploitables à distance (grande portée) et/ou sans conditions particulières d’accès et/ou sans authentification. Elles peuvent compromettre rapidement et facilement le système ciblé, voire les données utilisateurs. Elles doivent être traitées de façon urgente et prioritaire. |
| **Haut** | 7-8.9 | Les vulnérabilités de niveau haut ont un impact sur le système ciblé et/ou peuvent être exploitées à distance et/ou sans authentification. |
| **Moyen** | 4-6.9 | Les vulnérabilités de niveau moyen n’ont qu’une portée ou un impact réduit. L’exploitation requiert par exemple une authentification. |
| **Bas** | 0.1-3.9 | Les vulnérabilités de niveau bas sont sans effet ou presque sur le système visé. |
| **Nul** | 0 | Les vulnérabilités de niveau nul n’ont aucun impact sur le système visé. |

[Le référentiel [Top 10 OWASP](https://owasp.org/www-project-top-ten/) a été utilisé pour la classification des vulnérabilités web]

# Types de preuve et de correction

Chaque vulnérabilité rapportée est fournie avec au moins un élément de preuve réplicable.

Voici quelques exemples de preuves [A ADAPTER SELON PREUVES FOURNIES] :

|  |  |
| --- | --- |
| 1. | Preuves techniques (bout de code, lien vers une page web, etc) |
| 2. | Preuves méthodologiques (utilisation d’outil, de méthodologies) |
| 3. | Preuves informelles (informations divulguée, etc) |

Chaque vulnérabilité rapportée est fournie avec un élément de correction (capture d’écran, preuve écrite ou lien web) [A ADAPTER SELON CORRECTIONS FOURNIES].

# Périmètre technique

L’audit de sécurité a été mené sur l’environnement suivant :

<https://exemple.fr> (127.0.0.1 :80)

Les actifs suivants n’ont pas été audités : XYZ [SI NECESSAIRE DE PRECISER]

# Participants

Les personnes suivantes ont participé au test d’intrusion :

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom et prénom** | **E-mail** | **Téléphone** | **Rôle** |
| XX | [adresse@mail.com](mailto:adresse@mail.com) | 0612345678 | Auditeur technique |

# Sommaire des Vulnérabilités trouvées et recommandations

## Résumé de l’expertise et recommandations

|  |  |  |  |
| --- | --- | --- | --- |
| Page | Vulnérabilité et Niveau de criticité | Recommandations | Actifs concernés |
| 5 | A3:2017 : Exposition de données sensibles – niv 9 | Introduire un identifiant de session | Exemple.fr/compte |
| 5 | A2:2017 : Contrôle d’authentification non sécurisé – niv 8 |  | Exemple.fr/compte |
| 6 | A5:2017 : Contrôle d’accès non sécurisé – niv 8 | Arrêter les services inutilisés | Exemple.fr/admin |
| 7 | A6:2017 : Cross-site scripting – niv 7 | Filtrer les entrées utilisateurs. | Exemple.fr |
| 8 | A9:2017 : Utilisation de composants vulnérables – niv 4 | Mettre à jour ou s’assurer de l’application des mises à jour de sécurité. | 127.0.0.1 :82 |

[TABLEAU A ADAPTER ENTIEREMENT]

Les tests effectués ont permis de dévoiler 5 vulnérabilités, dont plusieurs de niveau critique. Il a été possible de nous authentifier sur le site en contournant les accès, puis de tirer parti de composants vulnérables. [FAIRE UN RÉSUMÉ DE LA SITUATION]

## Analyse du risque global

La probabilité d’exploitation est considérée comme étant élevée compte tenu des facteurs suivants [A ADAPTER] :

|  |  |  |
| --- | --- | --- |
| Type | Classification | Explications |
| Vecteur d’attaque | Réseau | Attaque qui peut être menée depuis Internet |
| Complexité | Faible | Pas d’effort ou de préparation requis |
| Privilèges requis | Moyen | Un compte utilisateur avec un accès à une interface cliente est requis |
| Interaction humaine | Faible | Aucune interaction utilisateur requise |

La force d’impact est considérée comme étant élevée compte tenu des facteurs suivants :

|  |  |  |
| --- | --- | --- |
| Type | Classification | Explications |
| Portée | Réseau | Ensemble du site et de l’activité |
| Perte de confidentialité | Élevée | Les mots de passe peuvent être compromis |
| Perte de disponibilité | Élevée | Le site peut être mis hors ligne |
| Perte d’intégrité | Élevée | Les données en base de données peuvent être modifiées |

# Détails des vulnérabilités

## A3:2017 : Exposition de données sensibles [Mettre un numéro arbitraire, un CWE ou l’identifiant CVE si besoin, ici « A3:2017 » vient du référentiel Owasp et est à utiliser uniquement s’il y a des vulnérabilités web]

|  |  |
| --- | --- |
| **Reference :** | **Évaluation de la criticité :** |
| A3:2017 | **Critique – Score : 9** |
| **Outils utilisés :** | |
| Burp Suite | |
| **Description de la vulnérabilité :** | |
| Lors de l’étape du scanning (Phase 2), nous avons repéré un port ouvert qui a permis de connaître des informations sur la page web. | |
| **Mode de découverte** | |
| Analyse manuelle et automatisée | |
| **Actif(s) vulnérable(s)** | |
| IP/URL/AUTRE | |
| **Implications / Conséquences** | |
| Un adversaire pouvant retrouver les données affichées pourrait s’en servir pour contourner d’autres mécanismes de sécurité ou opérer un chantage auprès des collaborateurs. | |
| **Recommandations suggérées** | |
| * Introduire un identifiant de session * Faire ceci et cela * BONUS : ne pas oublier de | |
| **Références** | |
| <https://owasp.org/> | |

[PREUVES (ETAPE POUR LE REFAIRE), DETAILS ADDITIONNELS ET CAPTURES D’ECRAN]

## A2:2017 Contrôle d’authentification non sécurisé

|  |  |
| --- | --- |
| **Reference :** | **Évaluation de la criticité :** |
| A2:2017 | **Haute – Score : 8** |
| **Outils utilisés :** | |
| Burp Suite / Nmap / autre | |
| **Description de la vulnérabilité :** | |
| Lors de l’étape de l’exploitation, nous avons pu tirer partie d’un identifiant non sécurisé pour nous connecter à l’interface web d’un membre. | |
| **Mode de découverte** | |
| Analyse manuelle et automatisée | |
| **Actif(s) vulnérable(s)** | |
| IP/URL/AUTRE | |
| **Implications / Conséquences** | |
| Un adversaire pouvant se connecter sans authentification forte obtient un accès privilégie au système qu’il convient d’éviter. | |
| **Recommandations suggérées** | |
| * Faire ceci et cela * BONUS : ne pas oublier de | |
| **Références** | |
| <https://owasp.org/> | |

[PREUVES (ETAPE POUR LE REFAIRE), DETAILS ADDITIONNELS ET CAPTURES D’ECRAN]

## A5:2017 : Contrôle d’accès non sécurisé

|  |  |
| --- | --- |
| **Reference :** | **Évaluation de la criticité :** |
| A3:2017 | **Haute – Score : 8** |
| **Outils utilisés :** | |
| … | |
| **Description de la vulnérabilité :** | |
| … | |
| **Mode de découverte** | |
| … | |
| **Actif(s) vulnérable(s)** | |
| IP/URL/AUTRE | |
| **Implications / Conséquences** | |
| … | |
| **Recommandations suggérées** | |
| * … | |
| **Références** | |
| … | |

[PREUVES (ETAPE POUR LE REFAIRE), DETAILS ADDITIONNELS ET CAPTURES D’ECRAN]

## A7:2017 : Cross-site scripting

[A CONTINUER POUR CHAQUE VULNERABILITE]

# Annexes

[SI PERTINENT]