**Rapport de Pentest – Exemple.com**

## Details d’audit

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Référence : | 2024-XYZ |  | | |
| Type : | Audit de sécurité **technique (pentest)** |  | | |
| Date : | **JJ/MM/AAA** |  | Durée : | 7 jours |
| Lieu : | Audit en ligne |  | Contact : | adresse@mail.com |
| Auditeur : | Michel KARTNER |  |  |  |

## Historique des modifications

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| V1.0 | JJ/MM/AAAA | Publication initiale |

Table des matières

[Details d’audit 1](#_Toc176965959)

[Historique des modifications 1](#_Toc176965960)

[Contexte et cadre du test d’intrusion 2](#_Toc176965961)

[Méthodologie technique et évaluation 2](#_Toc176965962)

[Types de preuve et de correction 3](#_Toc176965963)

[Périmètre technique 3](#_Toc176965964)

[Participants 3](#_Toc176965965)

[Sommaire des Vulnérabilités trouvées et recommandations 3](#_Toc176965966)

[Résumé de l’expertise 3](#_Toc176965967)

[Analyse du risque global 4](#_Toc176965968)

[Détails des vulnérabilités 5](#_Toc176965969)

[Éléments de correction 5](#_Toc176965970)

[Références 5](#_Toc176965971)

[Éléments de correction 6](#_Toc176965972)

[Références 6](#_Toc176965973)

[Annexes 7](#_Toc176965974)

## 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 <http://ip10-21-112-5-crgpu3lg0m1h0olkng5g-8080.direct.labs.cyberini.com/> à fin de tester la robustesse du site web et de l’infrastructure sous-jacente.

A l’issue d’un piratage passé, la société Exemple a mandaté un test d’intrusion pour vérifier la mise en place des solutions correctives apportées par l’équipe de développeurs. 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 l’infrastructure système.

Pour rappel un pentest ne peu par nature pas garantir l’identification de toutes les vulnérabilités d’un système. Un processus de sécurisation se déroule sur le long terme à l’aide de mises à jour régulières et de formation du personnel.

## Méthodologie technique et évaluation

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).

CVSS est un standard industriel pour évaluer la sévérité d’une vulnérabilité selon différentes métriques comme la complexité d’une attaque ou les privilèges requis.

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 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. |
| **Info** |  | Information donnée au sujet d’une vulnérabilité ou d’un système |

## Types de preuve et de correction

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

Voici quelques exemples de preuves possibles :

|  |  |
| --- | --- |
| 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).

## Périmètre technique

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

- http://ip10-21-112-5-crgpu3lg0m1h0olkng5g-8080.direct.labs.cyberini.com/ (10.21.112.5 port 8080)

- 10.21.112.5 port 21 (ftp)

## Participants

Les personnes suivantes ont participé au test d’intrusion :

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

## Sommaire des Vulnérabilités trouvées et recommandations

### Résumé de l’expertise

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Page | Vulnérabilité et Niveau de criticité | Recommandations | Actifs concernés | Score CVSS |
| 6 | CWE-78 - CVE-2011-2523 | Mettre à jour vsftpd | Vsftpd (10.21.112.5 :21) | 9.5 |
| 5 | CWE-79 - XSS | Filtrer les entrées utilisateurs dans search.php | http://ip10-21-112-5-crgpu3lg0m1h0olkng5g-8080.direct.labs.cyberini.com/search.php | 6.9 |

Les tests effectués ont permis de dévoiler 2 vulnérabilités, dont une de niveau critique. Il a été possible de nous connecter à distance sur le système en tant qu’utilisateur « toto » afin de lancer des commandes arbitraires. L’exploitation pourrait être effectuée depuis n’importe quel endroit dans le monde, et peut déjà avoir été faite. Il est recommandé de modifier tous les mots de passe utilisateurs après mise en place du correctif et d’observer les fichiers logs à la recherche d’éventuelles traces d’intrusion.

## Analyse du risque global

La probabilité d’exploitation générale est considérée comme étant élevée compte tenu des facteurs suivants :

|  |  |  |
| --- | --- | --- |
| Type | Classification | Explications |
| Vecteur d’attaque | Réseau (Network) - AV:N | Attaque qui peut être menée depuis Internet |
| Complexité | Faible (Low) - AC:L | Pas d’effort ou de préparation requis |
| Privilèges requis | Aucun (None) - PR:N | Pas de compte utilisateur requis |
| Interaction humaine | Aucune (None) - UI:N | Aucune interaction utilisateur requise |

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

|  |  |  |
| --- | --- | --- |
| Type | Classification | Explications |
| Périmètre | Changé - S:C | L’attaque peut permettre d’exploiter davantage le système |
| Perte de confidentialité | Élevée - C:H | Les données systèmes de l’utilisateur peuvent être lues |
| Perte de disponibilité | Élevée - A:HH | Des composants peuvent être touchés/édités |
| Perte d’intégrité | Élevée - I:H | Les données peuvent être modifiées |

# Détails des vulnérabilités

**CWE-79: Improper Neutralization of Input During Web Page Generation (XSS)**

**Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement**

**Lien vers le test reproductible :** [**http://ip10-21-112-5-crgpu3lg0m1h0olkng5g-8080.direct.labs.cyberini.com/search.php?query=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E**](http://ip10-21-112-5-crgpu3lg0m1h0olkng5g-8080.direct.labs.cyberini.com/search.php?query=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E)

Une faille XSS de type « Réfléchi » a été découverte dans le champ de recherche du site web. Cela permet à un attaquant d’entrer du code arbitraire dans les pages, et cela peut notamment mener à du vol de fichiers cookies dans certains cas. Ici la portée de l’attaque est relativement réduite par la nature même de la vulnérabilité.

**Score CVSS (6.9) :** [**AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:X**](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:X&version=3.1)

### Éléments de correction

Éditer le code source de la page search.php pour y ajouter un filtre des caractères html spéciaux. Exemple : htmlspecialchars().

### Références

<https://cwe.mitre.org/data/definitions/79.html>

<https://www.php.net/manual/en/function.htmlspecialchars.php>

|  |  |
| --- | --- |
|  | **CWE-78 : Improper Neutralization of Special Elements used in an OS Command** |

**Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement**

**Actif et port concerné : 10.21.112.5 port 21**

Une version vulnérable de Vsftpd a été découverte. Celle-ci contient une porte dérobée (backdoor) permet à un attaquant d’accéder au système.

**Score CVSS 9.5 :** [**AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C**](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C&version=3.1)

**Vulnérabilité CVE concernée : CVE-2011-2523**

**CWE complémentaire : CWE-912: Hidden Functionality**

### Éléments de correction

Mettre le plus rapidement possible vsftpd à jour.

Exemple de commande Linux : sudo apt update && sudo apt install vsftpd -y

### Références

<https://nvd.nist.gov/vuln/detail/CVE-2011-2523>

<https://www.exploit-db.com/exploits/49757>

<https://nvd.nist.gov/vuln/detail/CVE-2011-2523>

# Annexes

[SI PERTINENT]