var\_client

var\_contract

var\_month var\_year

Rapport de test d’intrusion

Sommaire

[1. Introduction 2](#_Toc77552529)

[1.1 Contexte de l’audit 2](#_Toc77552530)

[2. Synthèse des résultats 3](#_Toc77552531)

[2.1 Niveau de sécurité global 3](#_Toc77552536)

[2.2 Défauts constatés 3](#_Toc77552537)

[2.3 Points forts 3](#_Toc77552538)

[2.4 Mauvaises pratiques 3](#_Toc77552539)

[2.5 Points de vigilance 3](#_Toc77552540)

[3. Tableau récapitulatif des défauts de sécurité 4](#_Toc77552541)

[4. Tableau récapitulatif des actions correctives 5](#_Toc77552542)

[5. Détail des défauts et actions correctives 6](#_Toc77552543)

[6. Annexes 7](#_Toc77552544)

[6.1 Échelle de classification des vulnérabilités 7](#_Toc77552551)

[6.2 Services ouverts 9](#_Toc77552552)

# Introduction

## Contexte de l’audit

Le périmètre considéré pour l’audit est le suivant :

(périmètre)

# Synthèse des résultats



## Niveau de sécurité global

var\_synthesis

## Défauts constatés

Durant cet audit, **var\_nb\_d\_total défauts de sécurité** ont été identifiés :

|  |  |  |  |
| --- | --- | --- | --- |
| Critique : **var\_nb\_d\_critical** | Majeur : **var\_nb\_d\_major** | Important : **var\_nb\_d\_important** | Mineur : **var\_nb\_d\_minor** |

L’évaluation de leur criticité est basée sur l’échelle de classification des vulnérabilités proposée par l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information), fournie dans les annexes.

## Points forts

* var\_remarks\_positive

## Mauvaises pratiques

* var\_remarks\_negative

## Points de vigilance

* + var\_remarks\_neutral

# Tableau récapitulatif des défauts de sécurité

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **var\_dsum\_colId** | **var\_dsum\_colTit** | **var\_dsum\_colEase** | **var\_dsum\_colImpact** | **var\_dsum\_colType** |

***Critère « Type »****: S = Socle, A = Application, D = Données, P = Politique de sécurité*

*Le détail de l’échelle de classification des défauts de sécurité est donné en Annexe.*

# Tableau récapitulatif des actions correctives

Le critère de mise en œuvre est donné à titre indicatif, en se basant sur notre expérience, mais ne reflète pas les particularités de votre environnement qui pourraient complexifier la tâche.

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_csum\_colId** | **var\_csum\_colTit** | **var\_csum\_colEase** | **var\_csum\_colGain** |

***Critère « Mise en œuvre »***

*Quick Win : paramétrage d’un composant, protection d’une saisie d’une application*

*Modérée : changements de code restreints, mise en place d’une solution*

*Envergure : changements conséquents dans le code ou l’architecture de la solution*

# Détail des défauts et actions correctives

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_d\_id** | var\_d\_title | *var\_h\_exploitation* | *var\_h\_impact* |
| **var\_d\_ease** | **var\_d\_impact** |
| var\_d\_description | | | |

var\_d\_separator

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_d\_id** | var\_d\_title | *var\_h\_exploitation* | *var\_h\_impact* |
| **var\_d\_ease** | **var\_d\_impact** |
| var\_d\_description | | | |

var\_d\_separator

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_d\_id** | var\_d\_title | *var\_h\_exploitation* | *var\_h\_impact* |
| **var\_d\_ease** | **var\_d\_impact** |
| var\_d\_description | | | |

var\_d\_separator

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_d\_id** | var\_d\_title | *var\_h\_exploitation* | *var\_h\_impact* |
| **var\_d\_ease** | **var\_d\_impact** |
| var\_d\_description | | | |

var\_d\_separator

|  |  |  |  |
| --- | --- | --- | --- |
| **var\_c\_id** | var\_c\_title | *var\_h\_ease* | *var\_h\_gain* |
| **var\_c\_ease** | **var\_c\_gain** |
| var\_c\_description | | | |

# Annexes



## Échelle de classification des vulnérabilités

Les vulnérabilités identifiées sont évaluées suivant l’échelle standard de classification des vulnérabilités proposée par l’ANSSI, l’Agence Nationale de la Sécurité des Systèmes d’Information, à destination des Prestataires-Auditeurs de la Sécurité des Systèmes d’Information (PASSI).

Elles sont classées en fonction du risque qu’elles font peser sur le système d’information, c'est-à-dire en fonction de l’impact de la vulnérabilité sur le système d’information et de sa difficulté d’exploitation, et ce qu’elles soient d’origine technique ou organisationnelle

Exploitation :

* **Facile :** exploitation triviale, sans outil particulier ;
* **Modérée :** exploitation nécessitant des techniques simples et des outils publics ;
* **Difficile :** exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d’information et le développement d’outils simples ;
* **Très difficile :** exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d’information et le développement d’outils spécifiques et ciblés.

Impact :

* **Mineur :** pas de conséquence directe sur la sécurité du système d’information audité ;
* **Important :** conséquences isolées sur des points précis du système d’information audité ;
* **Majeur :** conséquences restreintes sur une partie du système d’information audité ;
* **Critique :** conséquences généralisées sur l’ensemble du système d'information audité.

Risque résultant :

* **Mineur :** faible risque pouvant nécessiter une correction ;
* **Important :** risque modéré nécessitant une correction à moyen terme ;
* **Majeur :** risque majeur nécessitant une correction à court terme ;
* **Critique :** risque critique nécessitant une correction immédiate ou un arrêt immédiat.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **↓ Impact Exploit. →** | **Très difficile** | **Difficile** | **Modérée** | **Facile** |
| **Mineur** | Mineur | Mineur | Important | Majeur |
| **Important** | Mineur | Important | Important | Majeur |
| **Majeur** | Important | Majeur | Majeur | Critique |
| **Critique** | Important | Majeur | Critique | Critique |

## Services ouverts

Le tableau suivant récapitule les services disponibles sur chaque port ouvert de chaque adresse IP de la plage auditée, associé d’un commentaire.

|  |  |  |  |
| --- | --- | --- | --- |
| var\_ssum\_ip | var\_ssum\_port | var\_ssum\_proto | var\_ssum\_comment |