{{ client }}

{{ contract }}

{{ month|translate }} {{ 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 chef de projet de l’audit est {{ owner.surname }} {{ owner.name }} {{ owner.email }}

Les pentesters ayant participés sont :

|  |  |
| --- | --- |
| **Nom** | **E-mail** |
| {%tr for pentester in pentesters %} |  |
| {{ pentester.surname }} {{ pentester.name }} | {{ pentester.email }} |
| {%tr endfor %} |  |

Le périmètre considéré pour l’audit est le suivant :

{%p for scope in scopes %}

{{ scope.scope }}

{%p endfor %}

# Synthèse des résultats



## Niveau de sécurité global

Todo

## Défauts constatés

Durant cet audit, {{ defects|count }} **défauts de sécurité** ont été identifiés :

|  |  |  |  |
| --- | --- | --- | --- |
| Critique : **{{ defects | selectattr('risk','equalto', 'Critical')|list|count }}** | Majeur : **{{ defects | selectattr('risk','equalto', 'Major')|list|count }}** | Important : **{{ defects | selectattr('risk','equalto', 'Important')|list|count }}** | Mineur : **{{ defects | selectattr('risk','equalto','Minor')|list|count }}** |

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.

{%p if positive\_remarks | count is ge 1 %}

## Points forts

{%p for positive\_remark in positive\_remarks %}

* {{ positive\_remark }}

{%p endfor %}

{%p endif %}

{%p if negative\_remarks | count is ge 1 %}

## Mauvaises pratiques

{%p for negative\_remark in negative\_remarks %}

* {{ negative\_remark }}

{%p endfor %}

{%p endif %}

{%p if neutral\_remarks | count is ge 1 %}

## Points de vigilance

{%p for neutral\_remark in neutral\_remarks %}

* + {{ neutral\_remark }}

{%p endfor %}

{%p endif %}

# Tableau récapitulatif des défauts de sécurité

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Libellé** | **Exploitation** | **Impact** | **Type** |
| **{%tr for x in defects|selectattr('risk','equalto', 'Critical') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Major') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Important') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate}} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |
| **{%tr for x in defects|selectattr('risk','equalto', 'Minor') %}** |  |  |  |  |
| **D{{ x.id }}** | {{ x.title }} | {{ x.ease|translate }} | {{ x.impact|translate }} | {{ x.type|translate|getInitials }} |
| **{%tr endfor %}** |  |  |  |  |

***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.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Libellé** | **Mise en œuvre** | **Gain en sécurité** |
| **{%tr for fix in fixes %}** |  |  |  |
| **A{{ fix.id }}** | {{ fix.title }} | **{% cellbg colors.fix[fix.execution] %}{{ fix.execution|translate }}** | **{% cellbg colors.fix[fix.gain] %}{{ fix.gain|translate }}** |
| **{%tr endfor %}** |  |  |  |

***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{% for x in defects|selectattr('risk','equalto', 'Critical') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Major') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Important') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}{% for x in defects|selectattr('risk','equalto', 'Minor') %}

|  |  |  |  |
| --- | --- | --- | --- |
| **D{{ x.id }}** | {{ x.title }} | *Exploitation* | *Impact* |
| **{{ x.ease|translate }}** | **{{ x.impact|translate }}** |
| {{ x.synthesis }} | | | |

{%p for para in x.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% for instance in x.instances %}

{%p for para in instance.notes\_paragraphs %}

{{ para }}

{%p endfor %}

{%p for proof in instance.proofs %}

{{ proof }}

{%p endfor %}

{% endfor %}

{% for fix in x.fixes %}

|  |  |  |  |
| --- | --- | --- | --- |
| **A{{ fix.id }}** | {{ fix.title }} | *Mise en œuvre* | *Gain en sécurité* |
| **{{ fix.execution|translate }}** | **{{ fix.gain|translate }}** |
| {{ fix.synthesis }} | | | |

{%p for para in fix.description\_paragraphs %}

{{ para }}

{%p endfor %}

{% endfor %}{% endfor %}

# 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Hôtes | Port | Service | Commentaire |
| {%tr for port in ports %} |  |  |  |
| {{ port.ip }} | {{ port.port }}/{{ port.proto }} | {{ port.service }} | {{ port.product }} |
| {%tr endfor %} |  |  |  |