RAPPORT D’AUDIT DE SECURITE

{company.name}

|  |  |  |
| --- | --- | --- |
| Classification | Document public  Document interne  Document confidentiel  Document secret | (C1)  (C2)  (C3)  (C4) |
| C3 |

|  |  |  |  |
| --- | --- | --- | --- |
| Objet | Rapport d’audit sécurité {company.name} | | |
| Référence | *{company.name}\_Audit\_{date\_end}.docx* | Date | {date | convertDateFR: 'short'} |
| Rédacteur | {creator.firstname} {creator.lastname}{#collaborators}  {firstname} {lastname}{/collaborators} | Lieu | [Lieu] |

{%company.logo\_small}

Les informations contenues dans ce document demeurent la propriété de [ENTREPRISE] et ne doivent pas être divulguées par le destinataire à des tiers sans l’accord écrit de [ENTREPRISE].

**SOMMAIRE**

[1. Vos contacts 2](#_Toc133167561)

[2. Suivi du document 2](#_Toc133167562)

[3. Introduction 4](#_Toc133167563)

[3.1 Contexte et Objectifs 4](#_Toc133167564)

[3.2 Intervenants Familiprix inc. et Référents client 4](#_Toc133167565)

[3.3 Liste de diffusion 4](#_Toc133167566)

[3.4 Période et Confidentialité 5](#_Toc133167567)

[3.5 Périmètre 5](#_Toc133167568)

[3.6 Notes concernant l’audit 5](#_Toc133167569)

[4. Résumé managérial 8](#_Toc133167570)

[4.1 Travaux réalisés 8](#_Toc133167571)

[4.2 Niveau global de sécurité 9](#_Toc133167572)

[4.3 Présentation des vulnérabilités et constats 12](#_Toc133167573)

[4.4 Présentation des recommandations 15](#_Toc133167574)

[5. Travaux Détaillés 18](#_Toc133167575)

[5.1 Recherche de vulnérabilités 18](#_Toc133167576)

[5.2 Vulnérabilités découvertes 21](#_Toc133167577)

[5.3 Mesures de durcissement 23](#_Toc133167578)

[6. Annexes 25](#_Toc133167579)

[6.1 Table des figures 25](#_Toc133167580)

[6.2 Echelle de niveau de sécurité global 26](#_Toc133167581)

[6.3 Classification des recommandations 27](#_Toc133167582)

[6.4 Classification des vulnérabilités – Scorring CVSS 28](#_Toc133167583)

[6.5 Top 10 OWASP 2021 29](#_Toc133167584)

# Vos contacts

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom** | **Fonction** | **Téléphone** | **Adresse E-Mail** |
| Prénom NOM | Directeur Activité Cybersécurité | 06.XX.XX.XX.XX | prenom.nom@mail.com |
| Prénom NOM | Auditeur SSI et Référent Equipe Technique | 06.XX.XX.XX.XX | prenom.nom@mail.com |
| {creator.firstname} {creator.lastname} | Consultant Cybersécurité et Auditeur SSI | {creator.phone} | {@creator.email | mailto: creator.email | p: 'Contenudetableau'} |
| {#collaborators}{firstname} {lastname} | Consultant Cybersécurité et Auditeur SSI | {phone} | {@email | mailto: email | p: 'Contenudetableau'}{/collaborators} |

# Suivi du document

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Nom du rédacteur** | **Nature de la modification** |
| 1.0 | {date\_end | convertDateFR: 'short'} | {creator.firstname} {creator.lastname} | Création du document |

Contexte, objectIfs et périmètre

# Introduction

## Contexte et Objectifs

La démarche de {company.name} s’inscrit dans une logique d’amélioration continue de la qualité de ses services et de la sécurité de l’information, pour sa propre sécurité mais aussi pour celle de ses clients et partenaires.

Les objectifs de cet audit sont de :

* Disposer d’un avis d’expert sur le niveau de sécurité,
* S’assurer du respect des bonnes pratiques et des règles de sécurité internes,
* Évaluer et diminuer le niveau de risque,
* Disposer d’axes d’améliorations.

## Intervenants Familiprix inc. et Référents client

**Familiprix inc.**

* {creator.firstname} {creator.lastname}, Consultant Cybersécurité et Auditeur SSI{#collaborators}
* {firstname} {lastname}, Consultant Cybersécurité et Auditeur SSI{/collaborators}

{company.name}

* {client.firstname} {client.lastname}, {client.title}

## Liste de diffusion

|  |  |  |
| --- | --- | --- |
| **Entreprise** | **Personne** | **Fonction** |
| {company.name} | {client.firstname} {client.lastname} | {client.title} |
| Familiprix inc. | {creator.firstname} {creator.lastname} | Consultant Cybersécurité et Auditeur SSI |
| {#collaborators}Familiprix inc. | {firstname} {lastname} | Consultant Cybersécurité et Auditeur SSI{/collaborators} |

## Période et Confidentialité

L’audit de sécurité s’est déroulé sur la(les) période(s) suivante(s) :

|  |  |
| --- | --- |
| **Activité d’audit** | **Date** |
| Test d’intrusion | Du {date\_start | convertDateFR: 'short' } au {date\_end | convertDateFR: 'short' } |

Toutes les données collectées pendant l’audit seront transmises à leur propriétaire ({company.name}) sur demande et/ou détruites à l’issue de la mission.

## Périmètre

### Périmètre technique

{company.name} a notifié à Familiprix inc. l’autorisation de test d’intrusion et a fourni les ressources suivantes :

* {-w:p scope}{name}{/scope}

L’ensemble de la prestation est effectué à distance à partir des adresses IP publiques [IP PUBLIQUES].

## Notes concernant l’audit

### Plages d’adresses

Les tests d’intrusion depuis Internet ont été menés depuis une liste d’IP limitée, appartenant à Familiprix inc., contrairement aux attaquants qui disposent de plusieurs machines situées sur des réseaux attaquants différents. Les balayages ou les attaques ont donc comme adresse source les adresses mentionnées ci-dessus. Ces attaques sont alors facilement décelables par vos services.

### Audit méthodique

Contrairement aux attaquants qui s'orientent vers une voie dès qu'ils trouvent une piste, les auditeurs privilégient une étude organisée. Ceci permet de balayer plus largement le périmètre et donc de mettre à jour beaucoup de zones sensibles. En effet, un attaquant utilise souvent la première vulnérabilité qu'il découvre, mais l'objectif d'un audit est de recenser un ensemble de domaines à risque.

Le principal inconvénient de cette démarche est que les auditeurs laissent le temps aux administrateurs pour sécuriser les failles éventuelles, car les « exploits » sont réalisés lors des étapes suivantes de l'audit. Dans le cadre d'une attaque réelle, les attaquants utilisent la faille seulement quelques minutes après l'avoir trouvée : cela leur laisse le temps d'effacer leurs traces et donc de ne pas être repérés par les administrateurs.

Nous tenons à insister sur cette différence. Le but d’un attaquant n’est généralement pas d’identifier toutes les vulnérabilités d’un système mais d’exploiter celle(s) qu’il a pu trouver. La complétude n’est donc pas recherchée contrairement au cas de la prestation d’expertise. Un expert cherche, dans un délai et une charge bornée, à mettre en évidence un maximum de vulnérabilités, réelles ou potentielles, et identifiables à un instant donné. Nous ne garantissons donc pas l’exhaustivité des découvertes des vulnérabilités sur le périmètre concerné dans le temps imparti.

### Période limitée

Nous avons testé les vulnérabilités divulguées et parues avant et durant la période d’audit dont les dates sont précédemment mentionnées dans le rapport.

Si, durant un audit, une faille importante est découverte, il est possible de l'exploiter durant les quelques heures nécessaires à l'administrateur pour installer un correctif.

L’exploitation d'une faille lors d'un audit est alors assujettie aux vulnérabilités découvertes durant cette période. Un attaquant, quant à lui, peut attendre plusieurs semaines avant d'utiliser une faille importante.

### Limites de la prestation

Le but de la prestation est de fournir un avis d’expert sur la sécurité du système d’information cible, à un instant donné, assorti de recommandations et de conseils.

Les mesures mises en place suite aux avis de nos experts ont pour objectif d’augmenter la confiance de {company.name} dans son système d’information, si les mesures préconisées sont correctement mises en œuvre.

Nous attirons l’attention de {company.name} sur les limites d’un tel avis :

* Les techniques d’attaques évoluant, un système sûr à un instant donné peut ne plus l’être quelques temps après. Nous conseillons à {company.name} de maintenir une veille technique sur ce sujet et d’appliquer au plus tôt les corrections préconisées par certains services spécialisés ;
* L'avis de l’expert a pour but d’augmenter le niveau de confiance dans la sécurité à un instant donné en fonction des éléments qui sont fournis et de la profondeur de l’analyse qu’il a pu effectuer. Ce niveau de confiance ne saurait être considéré comme absolu. L’atteinte de ce niveau de confiance suppose que {company.name} mette correctement en œuvre les mesures préconisées.

### Audit de validation

Un audit de validation est fortement recommandé afin de vérifier l’implémentation des mesures de sécurité.

Résumé Managérial

# Résumé managérial

## Travaux réalisés

Une méthodologie en 3 phases, illustrée par le schéma ci-dessous, a été mise en œuvre pour répondre aux objectifs de l’audit.

Découverte et exploration du périmètres

Analyse détaillée des services

Identification et exploitation des vulnérabilités

Les travaux menés ont permis de mettre en évidence plusieurs vulnérabilités sur le périmètre d'audit. Les parties suivantes présentent :

* Les vulnérabilités identifiées avec leur niveau de gravité,
* La répartition en termes de gravité des vulnérabilités identifiées,
* Les recommandations pour y remédier.

## Niveau global de sécurité

En se basant sur ses expériences, Familiprix inc. évalue la maturité du périmètre audité en termes de sécurité comme étant ... La société {company.name} a su mettre en œuvre des mesures de sécurité ....

**?**

**EXCELLENT A**

**BON B**

**MOYEN C**

**FAIBLE D**

**TRES FAIBLE F**

En effet, …

Le tableau ci-dessous décrit les grandes forces et faiblesses du SI de la société {company.name} en reprenant le référentiel du [TOP 10 OWASP 2021](https://owasp.org/www-project-top-ten/).

|  |  |
| --- | --- |
| **Légende** | |
| Très bon niveau |  |
| Bon niveau |  |
| Insuffisant |  |
| Inexistant |  |

|  |  |  |
| --- | --- | --- |
| **Forces et faiblesses** | **Commentaires** | **Niveau de protection** |
| Contrôle d’accès aux fonctionnalités restreintes | TODO |  |
| Erreurs Cryptographiques (protection de données) | TODO |  |
| Injections | TODO |  |
| Conception non sécurisée | TODO |  |
| Mauvaises configurations de sécurité | TODO |  |
| Utilisation de composants vulnérables ou obsolètes | TODO |  |
| Problèmes d’authentification | TODO |  |
| Problèmes d’intégrité des données et du logiciel | TODO |  |
| Problèmes de supervisions et de logs | N/A | N/A |
| Server Side Request Forgery (SSRF) | Cette vulnérabilité particulière n’a pas été observée sur le périmètre audité. |  |

## Présentation des vulnérabilités et constats

* Liste des vulnérabilités

Le tableau ci-dessous liste les vulnérabilités constatées lors de l’audit. Chaque vulnérabilité est associée à une ou plusieurs recommandations, à une ou plusieurs menaces et à un niveau de gravité basé sur l’échelle CVSS, c’est-à-dire en fonction de l’impact et de la facilité d’exploitation, conformément à l’état de l’art.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **référence** | **Intitulé** | **Périmètre** | **Scoring CVSS** | **Risque(s)** |
| {#findings | where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}{@'VULN-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | **{@cvss.cellColor}**  {@('CVSS ' + cvss.baseMetricScore) | linkTo: 'https://www.first.org/cvss/calculator/3.1#'+cvss.vectorString | p:'CVSS'} | {-w:p description}{@text | convertHTML: 'ContenudeTableauSmall'}{/description}{/} |

* LISTE DES MESURES DE DURCISSEMENT

Le tableau ci-dessous liste les mesures de durcissement constatées lors de l’audit. Une mesure de durcissement est une faiblesse jugée mineure. Chaque point de contrôle est associé à une ou plusieurs recommandations ainsi qu’à une ou plusieurs menaces.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Préférence** | **Intitulé** | **PéRimètre** | **Scoring CVSS** | **Risque(s)** |
| {#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")'}{@'HARDENED-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {@cvss.cellColor}  N/A | {-w:p description}{@text | convertHTML: 'ContenudeTableauSmall'}{/description}{/} |

* Vulnérabilités par Criticités

{c\_crit = (findings | count: 'Critical'); c\_high = (findings | count: 'High'); c\_med = (findings | count: 'Medium'); c\_low = (findings | count: 'Low'); c\_total = (c\_crit + c\_high + c\_med + c\_low); c\_hard = (findings | count: 'None'); cv\_i = ((c\_high && c\_med) || (c\_high && c\_low) || (c\_med && c\_low)); cv\_ii = (c\_med && c\_low); cv\_iii = (c\_med || c\_low); ''}Le graphique ci-dessous permet d’avoir une vision globale du niveau et du nombre de vulnérabilités du périmètre audité. La présence {#c\_crit}de {c\_crit} vulnérabilité{#c\_crit>1}s{/} qualifiée{#c\_crit>1}s{/} de « critique{#c\_crit>1}s{/} »{#c\_crit!=c\_total}{#cv\_i},{/}{^cv\_i} et{/} {/}{/}{#c\_high}de {c\_high} vulnérabilité{#c\_high>1}s{/} qualifiée{#c\_high>1}s{/} de « forte{#c\_high>1}s{/} »{#cv\_iii}{#cv\_ii},{/}{^cv\_ii} et{/} {/}{/}{#c\_med}de {c\_med} vulnérabilité{#c\_med>1}s{/} qualifiée{#c\_med>1}s{/} de « moyenne{#c\_med>1}s{/} » {#c\_low}et {/}{/}{#c\_low}de {c\_low} vulnérabilité{#c\_low>1}s{/} « faible{#c\_low>1}s{/} »{/} implique des actions {#c\_crit}immédiates {/}de la part de {company.name} ou de ses prestataires.{#c\_hard}{#c\_hard==1} La mesure de durcissement est{/}{#c\_hard>1} Les {c\_hard} mesures de durcissement sont{/} également à prendre en compte afin d’améliorer la sécurité globale du SI exposé.{/}

## Présentation des recommandations

Le tableau ci-dessous liste les recommandations permettant de traiter les vulnérabilités ou constats d’audit.

Chaque constat ou vulnérabilité est associé à un ou plusieurs risques, à une ou plusieurs recommandations et à un niveau de priorité.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **référence** | **Intitulé** | **périmètre** | **Recommandation(s)** | **Complexite** | **Niveau de Priorité** |
| {#findings | where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}{@'VULN-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {-w:p remediation}{@text | convertHTML: 'ContenudeTableauSmall'}{/remediation} | {@remediation.cellColorComplexity}  {#remediationComplexity == '1'}Faible{/}{#remediationComplexity == '2'}Moyenne{/}{#remediationComplexity == '3'}Elevée{/} | {@remediation.cellColorPriority}  {priority}{/} |
| {#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")'}{@'HARDENED-'+($index+1) | bookmarkRef | p : 'VulnRef'} | {title} | {@affected | convertHTML: 'Contenudetableau'} | {-w:p remediation}{@text | convertHTML: 'ContenudeTableauSmall'}{/remediation} | {@remediation.cellColorComplexity }  {#remediationComplexity == '1'}Faible{/}{#remediationComplexity == '2'}Moyenne{/}{#remediationComplexity == '3'}Elevée{/} | {@remediation.cellColorPriority}  {priority}{/} |

Travaux Détaillés

# Travaux Détaillés

## Recherche de vulnérabilités

[METHODOLOGIE]

## Vulnérabilités découvertes{#findings| where: '(cvss.baseSeverity != "None" && cvss.baseSeverity != "")' | sortArrayByField: 'cvss.baseMetricScore':-1}

### {title}

|  |  |  |
| --- | --- | --- |
| **{@cvss.cellColor}** | **{@cvss.cellColor}**  {@'VULN-'+($index+1) | bookmarkCreate | p : 'VulnDef'} | **{@cvss.cellColor}** |
| **Titre** | **{title}** | **{@cvss.cellColor}**  {@('CVSS ' + cvss.baseMetricScore) | linkTo: 'https://www.first.org/cvss/calculator/3.1#'+cvss.vectorString | p:'CVSS'} |
| **Cible** | {@affected | convertHTML: 'Normal10'} |
| **Description** | {-w:p description}{@text | convertHTML: 'Normal10'}{/description} | |
| **Recommandation** | {-w:p remediation}{@text | convertHTML: 'Normal10'}{/remediation} | |
| **Références** | {#references | loopObject}  {@value | linkTo: value | p: 'reflink'}  {/} | |

#### Constat(s) d’audit

{-w:p observation}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/observation}

#### Preuve(s) d’audit

{-w:p poc}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/poc}

#### Recommandation(s)

{-w:p remediation}{@text | convertHTML}{/remediation}

{/}

## Mesures de durcissement{#findings | where: '(cvss.baseSeverity == "None" || cvss.baseSeverity == "")' }

### {title}

|  |  |  |
| --- | --- | --- |
| **{@cvss.cellColor}** | **{@cvss.cellColor}**  {@'HARDENED-'+($index+1) | bookmarkCreate | p : 'VulnDef'} | **{@cvss.cellColor}** |
| **Titre** | **{title}** | **{@cvss.cellColor}**  **N/A** |
| **Cible** | {@affected | convertHTML: 'Normal10'} |
| **Description** | {-w:p description}{@text | convertHTML: 'Normal10'}{/description} | |
| **Recommandation** | {-w:p remediation}{@text | convertHTML: 'Normal10'}{/remediation} | |
| **Références** | {#references | loopObject}  {@value | linkTo: value | p: 'reflink'}  {/} | |

#### Constat(s) d’audit

{-w:p observation}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/observation}

#### Preuve(s) d’audit

{-w:p poc}{@text | convertHTML}

{-w:p images}{%image}

Figure 1 **-** {caption}{/images}{/poc}

#### Recommandation(s)

{-w:p remediation}{@text | convertHTML}{/remediation}

{/}

# Annexes

## Table des figures

[Figure 1 **-** nom 0](#_Toc99378187)

## Echelle de niveau de sécurité global

Dans la mesure où :

* Le niveau de sécurité d’un composant n’est pas uniquement lié aux efforts de sécurisation entrepris mais peut également être dépendant du composant lui-même ;
* La démarche d’audit et d’étude des vulnérabilités tiens compte du niveau de sécurité à l’instant « T » indépendamment des impacts métiers des vulnérabilités ;
* Une vulnérabilité critique présente un risque immédiat et important pour le SI ou le composant impacté ;
* La prestation d’audit est réalisée en temps partiellement contraint et a pour but l’exhaustivité des vulnérabilités et faiblesses de configuration.

Familiprix inc. établit le niveau de sécurité global du périmètre audité selon les critères suivants.

|  |  |
| --- | --- |
| **Niveau** | **Description** |
| **Excellent** | Aucune vulnérabilité ayant un risque « Critique » ou « Majeur » n’a été identifiée. Des mesures de sécurité adéquates et optimales sont présentes, ce qui permet d’avoir une confiance établie dans la sécurité du SI audité et de limiter les potentiels impacts d’une vulnérabilité. Le SI audité est très largement supérieur à la moyenne des entreprises sur des périmètres équivalents. |
| **Bon** | Aucune vulnérabilité ayant un risque « Critique » ou « Majeur » n’a été identifiée. Quelques vulnérabilités mineures, moyennes ou mesures de durcissement sont présentes. Le SI audité présente néanmoins des mesures de sécurité et est globalement supérieur à la moyenne des SI audités sur des périmètres équivalents, en termes de sécurité. |
| **Moyen** | Plusieurs vulnérabilités ayant un risque « Important » ou « Majeur » ont été découvertes. Certaines mesures de sécurité sont en place mais sont encore insuffisante pour assurer la sécurité du SI. Le SI audité est dans la moyenne des entreprises auditées sur des périmètres équivalents en termes de sécurité. |
| **Faible** | Au moins une vulnérabilité « Majeur » ou « Critique » a été identifiée sur le périmètre d’audit et permet de prendre le contrôle d’un composant ou de récupérer des données sensibles. Malgré la présence éventuelle de quelques mesures, la maturité du SI auditée est considérée comme non satisfaisante. La sécurité du SI audité est inférieure à la moyenne des entreprises sur des périmètres équivalents. |
| **Très faible** | Plusieurs vulnérabilités « Critiques » ont été découvertes. La compromission d’un composant ou du SI est possible depuis plusieurs axes et la sécurité des données n’est pas assurée. Le niveau de sécurité global est inférieur à la moyenne des SI audités sur des périmètres équivalents et la maturité du SI en termes de sécurité est très insatisfaisante. |

## Classification des recommandations

### Complexité de correction

Chaque recommandation émise par Familiprix inc. est attribuée un niveau estimé de complexité de mise en œuvre, fourni à titre indicatif et basé sur les investissements nécessaires, notamment en termes de temps. L’échelle suivante permet d’illustrer les différents niveaux existants.

|  |  |
| --- | --- |
| **Niveau de complexité** | **Description** |
| **Faible** | Correspond à une tâche peu complexe, pouvant être réalisé en quelques heures, n’entrainant pas de coût financier supplémentaire et n’ayant que peu voire pas d’impact opérationnel (ex : modification d’un paramètre de configuration). |
| **Moyenne** | Correspond à une tâche moyennement complexe, pouvant nécessiter un travail de quelques jours ou un investissement financier et nécessitant une prise en compte des potentiels impacts opérationnels (ex : travail autour de comptes privilégiés, comptes de services, mise à jour de machines « clientes »). |
| **Elevée** | Elevée Correspond à une tâche complexe nécessitant une préparation afin de prendre en compte les impacts potentiels au niveau du SI. La complexité de la mise en œuvre peut venir de la durée nécessaire à l’application, pouvant être de plusieurs jours ou semaines (ex : chantier important de mises à jour de machines) ou de l’évolution des processus actuels de fonctionnement (ex : modification d’un grand nombre de mots de passe, évolution de solution technologique). |

### Priorité de correction

En accord avec le niveau de risque et la sévérité de chaque vulnérabilité, Familiprix inc. propose une priorité indicative pour l’application de chaque recommandation, en adéquation avec la totalité de ces dernières. Cette priorité tient également compte de la complexité de mise en œuvre. L’échelle suivante permet d’illustrer les différents niveaux de priorité.

|  |  |
| --- | --- |
| **Niveau de Priorité** | **Description** |
| **1** | La recommandation n’est pas prioritaire compte tenu du risque induit et peut être remise à plus tard dans le but de perfectionner la sécurité du SI. |
| **2** | La recommandation nécessite une étude complémentaire avant d’être mise en œuvre, ou peut-être embarquée dans des modifications ultérieures, sans urgence significative. |
| **3** | La recommandation a une priorité élevée et devrait être appliquée dans un délai relativement court afin de limiter les risques identifiés. Elle doit cependant faire l’objet de vérifications avant application. |
| **4** | La recommandation est absolument prioritaire et devrait être considérée en premier dans le plan d’action car elle permet d’évacuer un risque direct (point d’entrée, élévation de privilège, compromission). |

## Classification des vulnérabilités – Scorring CVSS



|  |
| --- |
| Common Vulnerability Scoring System (CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. Cette évaluation est constituée de 3 mesures appelées métriques : la métrique de base, la métrique temporelle et la métrique environnementale. |

Métriques :

Le CVSS est construit à partir de la métrique de base qui nous donne une évaluation du CVSS de base qui sera ensuite pondérée avec la métrique temporelle puis avec la métrique environnementale. Ces trois métriques se définissent comme suit :

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

Pour plus de détails : <https://www.first.org/cvss>

## Top 10 OWASP 2021

La fondation « OWASP » (Open Web Application Security Project) édite un projet global nommé « TOP 10 Web Application Security Risks » visant à rassembler sous la forme d’une liste détaillée les différentes vulnérabilités applicables les plus communes.

Une image contenant texte, clipart

Description générée automatiquement

Projet très largement adopté par la communauté et utilisé comme référence afin d’adresser les risques principaux dans le développement et la mise en production d’applications, une mise à jour du référentiel a été publié en septembre 2021. Cette dernière permet d’apporter une nouvelle version au précédent référentiel datant de 2017.

A01:2021-Broken Access Control moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicates that on average, 3.81% of applications tested had one or more Common Weakness Enumerations (CWEs) with more than 318k occurrences of CWEs in this risk category. The 34 CWEs mapped to Broken Access Control had more occurrences in applications than any other category.

A02:2021-Cryptographic Failures shifts up one position to #2, previously known as A3:2017-Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed name focuses on failures related to cryptography as it has been implicitly before. This category often leads to sensitive data exposure or system compromise.

A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3.37%, and the 33 CWEs mapped into this category have the second most occurrences in applications with 274k occurrences. Cross-site Scripting is now part of this category in this edition.

A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for A4:2017-XML External Entities (XXE) is now part of this risk category.

A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. A8:2017-Insecure Deserialization is now a part of this larger category.

A09:2021-Security Logging and Monitoring Failures was previously A10:2017-Insufficient Logging & Monitoring and is added from the Top 10 community survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

**Les ressources suivantes permettent d’en apprendre plus sur le référentiel :**

* OWASP Top 10 Web Application Security Risks ([lien](https://owasp.org/www-project-top-ten/))
* Introduction à l'OWASP Top 10 2021 ([lien](https://owasp.org/Top10/fr/))