Une image contenant Graphique, logo, Police, symbole

Description générée automatiquement

**Rapport d’Audit web**

**${LN}**

**${PRJ} pour l’année ${Y}**

**${icon:200:201}**

|  |  |  |
| --- | --- | --- |
| **Version du document** | **Date** | **Diffusion** |
| 1.0 | ${date} | Restricted |

**Table de matière**

[**Avant-propos**](#_heading=h.5f8pxguv5c7e) **3**

[Confidentialité du document](#_heading=h.ojq7mkiedpkj) 3

[Historique des modifications](#_heading=h.w7ma01fankxo) 3

[Diffusion du document](#_heading=h.nxebxuwpeliv) 3

[**Cadre de la mission**](#_heading=h.9kw53n719zwl) **4**

[**Champ d’audit**](#_heading=h.bispceat0fhp) **4**

[**Synthèse des résultats**](#_heading=h.56dhvzc045mb) **4**

[Niveau de sécurité global](#_heading=h.iqs3dzxh4wnp) 4

[Défauts constatés](#_heading=h.fy0tw016vqls) 4

[**Termes et définitions**](#_heading=h.28yvrn1cval8) **5**

[**Présentation de l’organisme audité**](#_heading=h.v8b62e8tq1sl) **6**

[**Présentation de SmartSkills**](#_heading=h.coeb7t4n4bd7) **6**

[**L’équipe du projet côté: SmartSkills**](#_heading=h.61dibbcvwmdk) **6**

[**Références**](#_heading=h.8i0dpvj23za5) **7**

[**Méthodologie d’audit, outils utilisés et système de notation**](#_heading=h.m2dys0wgf91k) **7**

[Méthode d’audit](#_heading=h.d82yzxwfxd40) 7

[Les outils de test de vulnérabilité utilisés](#_heading=h.73ww60el07u6) 8

[Description de système de notation](#_heading=h.prmpgde4538b) 9

[**Tableau récapitulatif des anomalies trouvées**](#_heading=h.jh3g2wn5kkg2) **11**

[**Présentation détaillée des vulnérabilités trouvées**](#_heading=h.2cgipi5ri5l4) **12**

[Anomalie 1: LFI](#_heading=h.mzqwo7ssfnla) 12

[Anomalie 2: Sensitive information disclosure](#_heading=h.5rg9rl3nesk4) 15

[**Bilan des actions correctives**](#_heading=h.15pse7kw9y9i) **17**

[**Tests réalisés**](#_heading=h.t7dtn2dmmbgg) **18**

# 

# Avant-propos

## Confidentialité du document

Le présent document est confidentiel et sa confidentialité consiste à :

* + - La non divulgation desdites informations confidentielles auprès de tierce partie,
    - Les non reproduction des informations dites confidentielles, sauf accord de l’organisme audité,
    - Ne pas profiter ou faire profiter tierce partie du contenu de ces informations en matière de savoir-faire,
    - Considère toutes les informations relatives à la production et au système d’information de l’organisme audité déclarées Confidentielles.

## Historique des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Auteur** | **Modifications** |
| 1.0 | ${date} | Equipe SMART SKILLS | Version initiale |

## Diffusion du document

Vue la criticité de ce document, sa diffusion doit être restreinte aux parties concernées.

# Cadre de la mission

* La présente mission est un Web.
* L’objectif de cette mission d’audit (Recherche de vulnérabilité en rapport avec la méthode OWASP et WASC-TC, évaluation du risque, recommandations).
* La méthode métier de référence dont laquelle est réalisée la présente mission d’audit, c’est la méthode OWASP et WASC-TC.
* La mission de l’audit se base sur un échantillonnage de l’application web ${PRJ}

# Champ d’audit

* Pour identifier la liste de vulnérabilité web, il est important de spécifier la structure à auditer qui lui correspond au site web de la société ‘${SN}’ :

|  |  |  |
| --- | --- | --- |
|  | **Application** | **URL** |
| 1 | ${PRJ} | ${URL} |

# Synthèse des résultats

## Niveau de sécurité global

Au vu des résultats de cet audit, effectué pour ${SN}, le périmètre audité dans le contexte précisé présente un niveau de sécurité global **${level}**

Cette évaluation se base sur trois critères :

* la sécurité du socle (système d’exploitation, serveur d’application et serveur de base de données),
* la sécurité de la ou les applications auditée(s),
* la sécurité des données,

## Défauts constatés

Durant cet audit, ${all} défauts de sécurité ont été identifiés :

|  |  |  |  |
| --- | --- | --- | --- |
| **Critique ${critique}** | **Majeur ${majeur}** | **Important ${important}** | **Mineur ${mineur}** |

# Termes et définitions

**Test d’intrusion Boîte Noire :**Les menaces proviennent d’un attaquant ayant uniquement accès au périmètre, sans aucun privilège spécifique ou compte utilisateur. Ce type d’audit permet d’évaluer les menaces engendrées par un attaquant extérieur à la société.

**Test d’intrusion Boîte Grise:** Les menaces proviennent d’un attaquant ayant un compte. Ce type d’audit permet d’évaluer les menaces engendrées par un utilisateur standard, ou un attaquant externe ayant élevé ses privilèges en tant qu’utilisateur standard.

**Cross-site Scripting (XSS) :** XSS se produit lorsqu'une application Web utilise une entrée utilisateur non validée ou non codée dans la sortie qu'elle génère.

**Formulaire HTML sans protection CSRF :** La falsification de requête intersites (CSRF ou XSRF) est une vulnérabilité dans laquelle un attaquant trompe une victime en lui faisant faire une requête qu'elle n'avait pas l'intention de faire.

**Clickjacking(en-tête X-Frame-Options manquant ) :** Le détournement de clic (attaque de réparation de l'interface utilisateur) est une technique malveillante qui consiste à inciter un utilisateur Web à cliquer sur quelque chose de différent de ce sur quoi l'utilisateur perçoit qu'il clique, révélant ainsi potentiellement des informations confidentielles ou prenant le contrôle de son ordinateur tout en cliquant sur des pages Web apparemment inoffensives.

**Cookie (s) sans indicateur HttpOnly défini :** Ce cookie n'a pas l'indicateur HTTPOnly défini. Lorsqu'un cookie est défini avec l'indicateur HTTPOnly, il indique au navigateur que le cookie n'est accessible que par le serveur et non par des scripts côté client. Il s'agit d'une protection de sécurité importante pour les cookies de session.

**Cookie (s) sans drapeau sécurisé :** Ce cookie n'a pas le drapeau sécurisé défini. Lorsqu'un cookie est défini avec l'indicateur sécurisé, il indique au navigateur que le cookie n'est accessible que via des canaux SSL sécurisés. Il s'agit d'une protection de sécurité importante pour les cookies de session.

**Téléchargement de fichiers :** Cette page permet aux visiteurs de télécharger des fichiers sur le serveur (tels que des images, des sons, ...). Les fichiers téléchargés peuvent poser un risque important s'ils ne sont pas traités correctement.

**Répertoires sensibles possibles :**Ce répertoire n'est pas directement lié au site Web. Cette vérification recherche les ressources sensibles communes telles que les répertoires de sauvegarde, les vidages de bases de données, les pages d'administration, les répertoires temporaires.

**Cookie de session limité au domaine parent :** Ce cookie de session est limité au domaine parent au lieu d'un sous-domaine. Si un cookie est limité à un domaine parent, ce cookie sera accessible par le domaine parent et également par tous les autres sous-domaines du domaine parent. Cela pourrait entraîner des problèmes de sécurité.

**Liens brisés :** Un lien rompu fait référence à tout lien qui devrait vous conduire vers un document, une image ou une page Web, qui entraîne en fait une erreur. Cette page a été liée à partir du site Web mais elle est inaccessible.

**Adresse e-mail trouvée :** La majorité du spam provient d'adresses e-mail récoltées sur Internet. Les robots anti-spam (également connus sous le nom de collecteurs d'e-mails et d'extracteurs d'e-mails) sont des programmes qui parcourent Internet à la recherche d'adresses e-mail sur les sites Web qu'ils rencontrent. Les programmes de spam bot recherchent des chaînes comme myname@mydomain.com puis enregistrent toutes les adresses trouvées.

**Méthode OWASP :** Le Top 10 de l'OWASP fournit des techniques de base pour se protéger contre ces problématiques web à haut risque et fournit également des conseils sur où aller pour mieux sécurisé.

**Méthode WASC-TC :** La classification des menaces de sécurité Web compilera et distillera les classes d'attaque uniques connues, qui ont présenté une menace pour les sites Web.

# Présentation de l’organisme et l’application auditée

${DESC}

# 

# Présentation de SmartSkills

**SMART SKILLS** est un bureau d’audit certifié ANSI, sous le numéro 06, créée en Septembre

2016. Elle met à disposition des grands comptes, publics et privés, en Tunisie comme à

l’International une large gamme de solutions axés sur l’audit technique et organisationnel ainsi que la formation. Son but est d’offrir aux entreprises et aux administrations des solutions de sécurité fiables, stables, et sécurisées.

# Références

Méthode **OWASP**(Open web application security project)

Méthode **WASC-TC** (Web application security consortium threat classification)

# Méthodologie d’audit, outils utilisés et système de notation

## Méthode d’audit

* La méthode d’audit adoptée, est la combinaison de 2 méthodes **(OWASP, WASC-TC)** dont **OWASP** décrit toutes les attaques possibles sur une application Web et les conséquences des principales faiblesses de sécurité, alors que, **WASC-TC** lui correspond à la classification des menaces de sécurité Web et d'attaque uniques connues, qui ont présenté une menace pour les sites Web.
* Les domaines de classification des vulnérabilités couvertes par les méthodologies d’audit sont définis ci-dessous.

**Remarques et Recommandations :**

* + La maturité des mesures et classification des vulnérabilités mis en place doit être établie en rapport avec les dix (10) domaines dudit méthode **OWASP**:

A.1 Injection

A.2 Authentification cassé

A.3 Script intersites (XSS)

A.4 Exposition de données sensibles

A.5 Désérialisation non sécurisée (+XXE)

A.6 Contrôle d'accès cassé

A.7 Journalisation et surveillance insuffisantes

A.8 Contrefaçon de requête côté serveur (SSRF)

A.9 Vulnérabilités connues

A.10 Mauvaise configuration de la sécurité

* + La maturité des mesures et classification des menaces liés à la sécurité web mis en place doit être établie en rapport avec les six (6) domaines dudit méthode **WASC-TC**:

1. **Authentification**
2. **Autorisation**
3. **Attaques côté client**
4. **Exécution de commandes**
5. **Révélation d'informations**
6. **Attaques logiques**

## Les outils de test de vulnérabilité utilisés

|  |  |  |
| --- | --- | --- |
| **Outils** | **Version utilisée** | **Fonctionnalités** |
| **Acunetix** | **10.5** | Un outil de scan de vulnérabilité dédié pour les applications web. Il permet d’identifier les failles par rapport au référentiel OWASP Top 10 |
| **SQLmap** | **1.5.4** | Un outil open source permettant d'identifier et d'exploiter une injection SQL sur des applications web. |
| **Nikto** | **2.1.6** | Nikto est un scanner de vulnérabilité de ligne de commande de logiciel gratuit qui analyse les serveurs Web pour les fichiers / CGI dangereux, les logiciels de serveur obsolètes et d'autres problèmes. Il effectue des vérifications génériques et spécifiques au type de serveur. |
| **Nmap** | **7.60** | Un scanner de port qui permet d’identifier les ports ouverts ainsi que les services qui tournent derrière. Il permet également d’identifier les versions, du système et des versions utilisées. |
| **OWASP ZAP** | **2.10** | OWASP Zed Attack Proxy est un outil basé sur Java qui est fourni avec une interface graphique intuitive, permettant aux testeurs de sécurité des applications web d'effectuer des fuzzing, des scripts, des spiders et des proxy afin d'attaquer les applications web. Le fait d'être un outil Java signifie qu'il peut être exécuté sur la plupart des systèmes d'exploitation qui supportent Java. |
| **Nessus** | **8.14** | Nessus est un outil de [sécurité informatique](https://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information). Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :   * les services vulnérables à des attaques permettant la [prise de contrôle](https://fr.wikipedia.org/wiki/Prise_de_contrôle) de la machine, l'accès à des informations sensibles (lecture de fichiers confidentiels par exemple), des dénis de service... * les fautes de configuration (relais de messagerie ouvert par exemple) * les patchs de sécurité non appliqués, que les failles corrigées soient exploitables ou non dans la configuration testée * les [mots de passe](https://fr.wikipedia.org/wiki/Mot_de_passe) [par défaut](https://fr.wikipedia.org/wiki/Valeur_par_défaut), quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. Nessus peut aussi appeler le programme externe Hydra ([de](https://de.wikipedia.org/wiki/Hydra_(software))) pour attaquer les mots de passe à l'aide d'un [dictionnaire](https://fr.wikipedia.org/wiki/Attaque_par_dictionnaire). * les services jugés faibles (on suggère par exemple de remplacer [Telnet](https://fr.wikipedia.org/wiki/Telnet) par [SSH](https://fr.wikipedia.org/wiki/Secure_Shell)) * les [dénis de service](https://fr.wikipedia.org/wiki/Attaque_par_déni_de_service) contre la [pile TCP/IP](https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet) |

## Description de système de notation

Pour calculer le niveau de risque, nous utilisons les métriques CVSS qui caractérisent l’exploitabilité et l’impact dans l’appréciation des risques apportés par les vulnérabilités techniques.

L’outil de calcul de l’échelle [CVSSv3](https://www.first.org/cvss/calculator/3.0) (Common Vulnerability Scoring System version 3)

|  |
| --- |
| Une image contenant texte, capture d’écran, ligne, diagramme  Description générée automatiquement |

Cet outil se base sur trois groupes de métriques d’évaluation afin de calculer le score de risque d’une vulnérabilité donnée. Ces groupes sont :

Le groupe de « Base » : évalue l’impact maximal théorique de la vulnérabilité.

Le groupe « Temporel » : permet l’évaluation de la vulnérabilité dans le temps en analysant son exploitabilité et ces niveaux de correction et de confiance.

Le groupe « Environnemental » : il prend en compte les modifications engendrées, une fois l’exploitation de la vulnérabilité effectuée, sur le périmètre et les capacités nouvellement accessibles par le malveillant.

Dans le cadre de cette étude et afin de simplifier l’analyse de celle-ci, la métriques Environnementale ne sera pas utilisée dans le calcul du score ; seuls les scores CVSS de Base et Temporel seront pris en compte.

Pour plus de détails sur les trois groupes cités, vous pouvez retrouver les éléments les composant dans la figure ci-dessous :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Le score calculé est une note échelonnée de 0 à 10. La note de 0 représentant le cas idéal et 10 représentant le risque maximal.

Ceci va servir de base à l’évaluation du niveau de risque des vulnérabilités. Le niveau de risque sera défini comme suit :

|  |  |
| --- | --- |
| **Faible** | si le score est compris entre 0.1 et 3.9 |
| **Moyen** | si le score est compris entre 4 et 6.9 |
| **Elevé** | si le score est compris entre 7 et 8.9 |
| **Critique** | si le score est supérieur ou égal à 9 |

# Tableau récapitulatif des anomalies trouvées

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Nom de anomalies** | **Description** | **Score CVSS 3.0** | **Risque** | **Complexité de la solution** |
| ${id} | ${name} | ${description} | ${score} | ${image} | ${compl} |

# Présentation détaillée des vulnérabilités trouvées

${block\_name}

## Anomalie ${trieValue} : ${name}

|  |  |  |  |
| --- | --- | --- | --- |
| **ID DE LA VULNÉRABILITÉ** | ${trieValue} | **RISQUE** | ${image} |
| **NOM DE LA VULNÉRABILITÉ** | ${name} | | |
| **ÉLÉMENTS IMPACTÉS** | ${element\_imp} | | |
| **DESCRIPTION** | | | |
| ${description} | | | |
| **RISQUES TECHNIQUES ET MÉTIER** | | | |
| ${risque} | | | |
| **SCORE CVSS v3: ${score\_cvss}** | | | |
| **${score}** | **Métriques d’exploitabilité** | **Vecteur d'attaque** | ${AV} |
| **Complexité de l'attaque** | ${AC} |
| **Privilèges requis** | ${UI} |
| **Interaction d’un utilisateur légitime** | ${PR} |
| **Périmètre** | ${S} |
| **Métriques d’impact** | **Impacte sur la confidentialité** | ${C} |
| **Impact sur l’intégrité** | ${I} |
| **Impact sur la disponibilité** | ${A} |
| **RÉFÉRENCES** | | | |
| ${ref} | | | |
| **PROOF OF CONCEPT** | | | |
| ${preuve:800:800} | | | |
| **RECOMMENDATIONS** | | | |
| ${recommendation} | | | |

${/block\_name}