SALON N°6

DE LA CYBERSECURITY

FORMATEURS

FORMATEURS

ISSIAGA KALTAMBA

Ingénieur en Cybersécurité

Spécialiste SOC niveau 1 et 2

Auditeur de Sécurité Technique et organisationnel

ERHARD FALEU

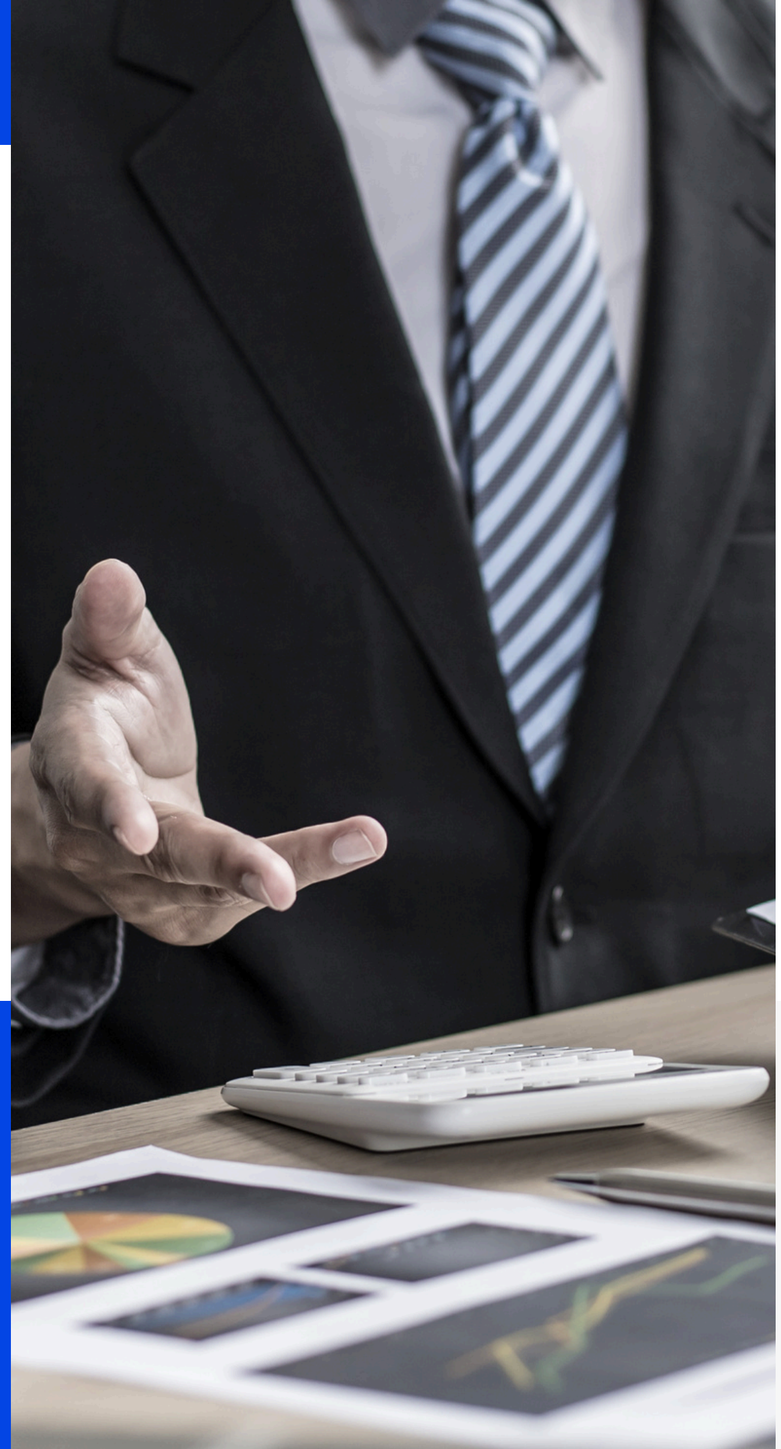
Ingénieur en Cybersécurité

Spécialiste en Risk Manager

THÈME:
INSTALLATION ET UTILISATION OWASP

info@cybernetic-security.com

www.cybernetic-security.com



PROGRAMME

01 Introduction OWASP

02 Pourquoi OWASP est Important

03 Installation de OWASP ZAP

04 Utilisation de OWASP ZAP

05 Top 3 des vulnérabilités du Top 10 OWASP

06 Conclusion

QU'EST-CE QUE L'OWASP ?

OWASP (Open Web Application Security Project) est une organisation internationale à but non lucratif qui se consacre à l'amélioration de la sécurité des logiciels et des applications web. Elle fournit des ressources, des outils et des guides pour aider les développeurs, les administrateurs systèmes, et les experts en sécurité à identifier et corriger les vulnérabilités des applications web.

01

OWASP

OWASP (Open Web Application Security Project) est une fondation dédiée à la sécurité des applications web.

02

Objectif

Sensibiliser et former les développeurs et les professionnels à la sécurité des applications.

03

Le Top 10 OWASP

Le Top Ten OWASP est une liste des 10 principales vulnérabilités de sécurité sur les applications web, maintenue par l'OWASP (Open Web Application Security Project). Cette liste aide les développeurs, les architectes, et les professionnels de la sécurité à identifier les vulnérabilités les plus courantes dans les applications web et à appliquer des mesures de sécurité pour les éviter.

LE TOP 10 OWASP

CyberNetic-Security

01

Broken Access Control (Contrôle d'accès défaillant)

- **Description** : Lorsque les restrictions sur les actions des utilisateurs ne sont pas correctement appliquées. Cela peut permettre à des utilisateurs malveillants d'accéder à des ressources non autorisées.
- **Exemples** : Escalade de privilèges, modification des informations d'autres utilisateurs, accès non autorisé à des données sensibles.

02

Cryptographic Failures (Défaillances cryptographiques)

- Description : Problèmes liés à la mauvaise protection des données, en particulier concernant les informations sensibles comme les mots de passe et les données financières.
- Exemples : Absence de chiffrement, utilisation d'algorithmes de chiffrement faibles, non-sécurisation des données en transit.

03

Injection (Injection)

- **Description** : Lorsqu'un attaquant injecte des données malveillantes dans une application, généralement via des requêtes SQL, des commandes système, ou des injections de code.
- **Exemples** : Injection SQL, injection de commandes dans des scripts système, LDAP ou XML.

04

Insecure Design (Conception non sécurisée)

- **Description** : Failles dans la conception de l'application qui ne prennent pas en compte les aspects de sécurité dès la phase de développement.
- **Exemples** : Absence de contrôle d'accès bien pensé, architecture vulnérable aux attaques par force brute ou attaque DDoS.

05

Security Misconfiguration (Mauvaise configuration de sécurité)

- **Description** : Mauvaise configuration des serveurs, des applications ou des bases de données qui entraîne des vulnérabilités exploitables.
- **Exemples** : Services inutiles activés, paramètres par défaut non modifiés, erreurs non gérées affichant des informations sensibles.

06

Vulnerable and Outdated Components (Composants vulnérables et obsolètes)

- **Description** : Utilisation de bibliothèques, frameworks ou autres composants logiciels qui comportent des failles de sécurité connues.
- **Exemples** : Utilisation de versions obsolètes de logiciels, absence de mises à jour des systèmes.

07

Identification and Authentication Failures (Défaillances d'identification et d'authentification)

- **Description** : Faiblesses dans les mécanismes d'identification et d'authentification qui permettent à des utilisateurs non autorisés d'accéder à des systèmes.
- **Exemples** : Authentification par défaut, faiblesse dans les sessions de gestion, mots de passe facilement devinables.

08

Software and Data Integrity Failures (Défaillances d'intégrité logicielle et des données)

- **Description** : Failles liées à l'intégrité des données ou des logiciels, souvent causées par un manque de vérification des mises à jour ou du contenu téléchargé.
- **Exemples** : Injection de logiciels malveillants via des sources non fiables, absence de signature numérique pour vérifier les composants.

09

Security Logging and Monitoring Failures (Défaillances de journalisation et de surveillance)

- **Description** : Absence de journalisation efficace et de surveillance pour détecter les attaques en temps réel, ce qui permet aux attaques de passer inaperçues.
- **Exemples** : Absence de journaux d'accès aux données sensibles, incapacité à détecter les comportements anormaux.

10

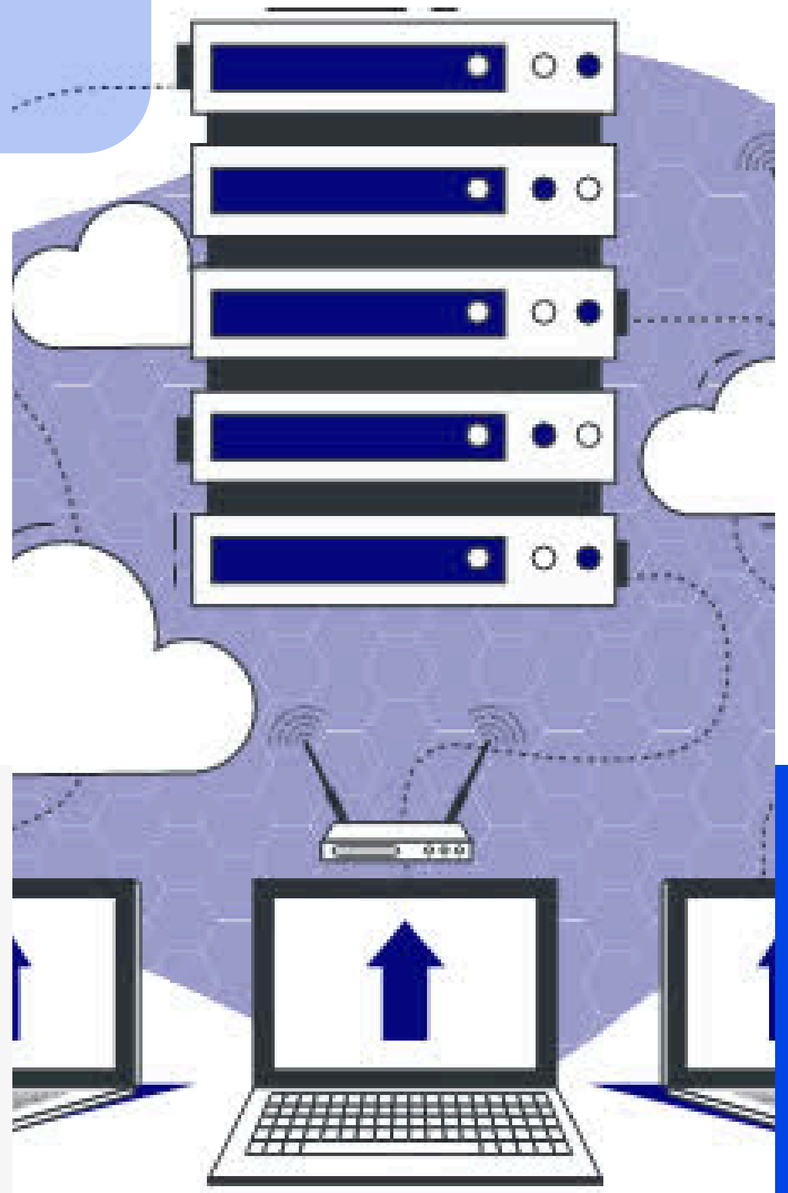
Server-Side Request Forgery (SSRF) (Contournement des requêtes côté serveur)

- **Description** : Lorsque l'application extrait des données ou interagit avec des ressources internes en se basant sur des entrées non fiables d'un attaquant.
- **Exemples** : Un attaquant exploite cette faille pour obtenir des informations non accessibles directement, comme des fichiers internes ou des informations réseau sensibles.

POURQUOI OWASP EST IMPORTANT

OWASP (Open Web Application Security Project) est essentiel car il fournit des lignes directrices et des outils pour sécuriser les applications web. Son Top 10 OWASP, qui recense les principales vulnérabilités de sécurité des applications web, est une référence mondiale utilisée par les développeurs et les professionnels de la cybersécurité. En suivant les recommandations d'OWASP, les organisations peuvent améliorer la sécurité de leurs applications, prévenir les cyberattaques, et se conformer aux réglementations de protection des données. De plus, OWASP propose des outils open source qui aident à identifier et corriger les failles de sécurité.

MERCI
CAS PRATIQUE



Plus d’informations

SITE WEB: CYBERNETIC-SECURITY.COM

EMAIL: INFO@CYBERNETIC-SECURITY.COM

TÉLÉPHONE:

+221 78 833 88 47

+221 78 896 49 96

+221 76 355 19 09

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY