



**INSI**

## *Syllabus de la Formation Cyber Attaque et Applications Web*

Aucune description

*Niveau* : Avancée

*Prix* : à partir de 0,00 Ar HT

*Durée* : jours | heures

*Place* : personnes

### Sessions

### Objectifs de cette formation

- Comprendre les bases des cyberattaques et les méthodes de sécurisation des applications web.
- Appliquer les meilleures pratiques pour sécuriser les applications web.
- Identifier et exploiter les vulnérabilités courantes des applications web.
- Utiliser des outils de pentesting pour évaluer la sécurité des applications web
- Participer à des challenges CTF pour renforcer les compétences pratiques.
- Développer des stratégies de défense pour protéger les applications web

## Programmes de cette formation

- - Concepts Fondamentaux et Sécurité des Applications Web

1. **Accueil et présentation**
2. Objectifs de la formation
3. Tour de table des participants
4. **Concepts fondamentaux des cyberattaques**
5. Principes de base de la cybersécurité (confidentialité, intégrité, disponibilité)
6. Modèle CIA (Confidentiality, Integrity, Availability)
7. OWASP Top 10
8. **Sécurisation des applications web**
9. Configuration sécurisée des serveurs web (Apache, Nginx)
10. Sécurisation des bases de données (MySQL, PostgreSQL)
11. Gestion des sessions et des cookies

#### **4.Introduction aux outils de sécurité web**

1. Présentation des principaux outils de sécurité web (Burp Suite, OWASP ZAP, etc.)
2. Installation et configuration des outi

- - Techniques de Cyberattaques sur les Applications Web

1. **Injection SQL**
2. Comprendre les attaques par injection SQL
3. Techniques d'exploitation des injections SQL
4. Méthodes de prévention
5. **Cross-Site Scripting (XSS)**
6. Comprendre les attaques XSS
7. Techniques d'exploitation des vulnérabilités XSS
8. Méthodes de prévention
9. **Cross-Site Request Forgery (CSRF)**
10. Comprendre les attaques CSRF

11. Techniques d'exploitation des vulnérabilités CSRF
12. Méthodes de prévention
13. **Autres vulnérabilités courantes**
14. Attaques par inclusion de fichiers (LFI/RFI)
15. Attaques sur les fichiers de configuration
16. Attaques par déni de service (DoS/DDoS)

- - Pentesting, CTF et Études de Cas

1. **Méthodologie de pentesting web**
2. Phases de pentesting (reconnaissance, analyse, exploitation, post-exploitation)
3. Utilisation de frameworks de pentesting (OWASP Testing Guide)
4. **Analyse des vulnérabilités**
5. Scan des vulnérabilités (Nessus, OpenVAS)
6. Utilisation de Burp Suite pour le pentesting
7. **Capture The Flag (CTF)**
8. Introduction aux challenges CTF
9. Mise en place d'un environnement CTF
10. Résolution de challenges CTF en équipe
11. **Études de cas pratiques**
12. Analyse de cyberattaques réelles
13. Discussion des leçons apprises et des stratégies de défense
14. Simulation d'un pentesting complet sur une application web
15. Élaboration d'un rapport de pentesting