# Besoins LOT 2

Fourniture de prestations de transfert de compétences de haut niveau d'expertise en exploitation de vulnérabilités web

**Description du profil attendu pour les formateurs**

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en pentest d'applications web.
- Pratique démontrable **en recherche et exploitation de vulnérabilités web** avancées (XXE, SSRF, injections, etc.).
- Pratique régulière dans l'audit de technologies et frameworks web modernes, notamment Java, PHP, Python (Django) et ASP.NET.
- Expérience dans l'utilisation d'outils d'audit web dans des contextes d'intrusion complexes.

2. Compétences techniques indispensables

- Maîtrise des **fondamentaux des technologies web**.
- Connaissance approfondie des techniques et mécanismes de sécurité applicative abordés en formation.
- Maîtrise des TP réalisés en formation.
- Très bonne compréhension des spécificités d'exploitation par langage ou framework abordés en formation.
- Usage confirmé des mécanismes de sécurité des langages et de leurs contournements étudiés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à enseigner les méthodes de reconnaissance web avancée.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à expliquer les approches d'analyse utilisées pour les vulnérabilités.

4. Éléments différenciants (facultatif)

- Diplômes ou certifications spécialisés dans le domaine.
- Formations récentes reçues en cybersécurité.
- Expérience dans l'audit technique de frameworks ou dans la recherche de vulnérabilités complexes.
- Expérience dans des scénarios réels proches de ceux enseignés.
- Contributions open-source liées au développement ou à la cybersécurité.
- Participation à des conférences, CTF ou publications techniques avancées.

**Description détaillée des prestations attendues**

| Ref | Libellé | Description | Travaux pratiques | Durée envisagée |
|---|---|---|---|---|
| TC02/01 | Hacking web PHP | **Objectif pédagogique** :<br>Appréhendez les mécanismes de sécurité des serveurs web PHP et les méthodes d'exploitation offensives avancées PHP Core.<br><br>Le transfert de compétences avancées traitera *a minima* les thèmes suivants :<br>- Vulnérabilités WEB PHP majeures de l'année.<br>- PHP Core : fonctionnement de la heap PHP, tooling GDB<br>- Développement d'un POC et d'un exploit PHP Core. | Travaux pratiques sur l'ensemble des méthodes et outils présentés. | Durée de 2 à 4 jours pour le cours en présentiel. |

| Ref | Libellé | Description | Travaux pratiques | Durée envisagée |
|---|---|---|---|---|
| TC02/02 | Intrusion sur les applications web | **Objectif pédagogique** :<br>Étudiez les mécanismes de sécurité des applications web modernes et les méthodes d'exploitation avancées permettant de les contourner.<br><br>Le transfert de compétences avancées traitera *a minima* les thèmes suivants :<br>- Reconnaissance, utilisation avancée de Burpsuite<br>- OAuth, JWT, SAML, exploitation avancée XXE, SSRF, attaques cryptographiques.<br>- Exploitation de vulnérabilités spécifiques PHP.<br>- Python Django en mode debug, désérialisation ASP.NET. | Travaux pratiques sur l'ensemble des méthodes et outils présentés. | Durée de 3 à 5 jours pour le cours en présentiel. |

| Ref | Libellé | Description | Travaux pratiques | Durée envisagée |
|---|---|---|---|---|
| TC02/03 | Recherche de vulnérabilités lors d'une intrusion web | **Objectif pédagogique** :<br>Optimiser la recherche de vulnérabilité web en boîte blanche pour les pentesteurs et développeurs.<br><br>Le transfert de compétences avancées traitera *a minima* les thèmes suivants :<br>- Méthodologie d'analyse, fonctionnement et vulnérabilités PHP.<br>- Java, spécificités des serveurs web, instrumentation et analyse de code.<br>- Java Spring et .Net, spécificités et analyse de vulnérabilités.<br>- Analyse et identification des configurations vulnérables. | Travaux pratiques sur l'ensemble des méthodes et outils présentés. | Durée de 3 à 5 jours pour le cours en présentiel. |