CAPHEX

CONSEILS & INVESTIGATIONS

07.62.26.66.44

CAPHEX@Protonmail.com

3 approches possibles

Black Box

Nous agissons comme un **hacker** ayant repéré votre site web

- *Aucune information fournie au préalable*

Grey Box

Nous nous comportons comme une personne malveillante ayant **un compte** sur votre application

- *Pour déterminer le champ d'action d'un utilisateur*

White Box

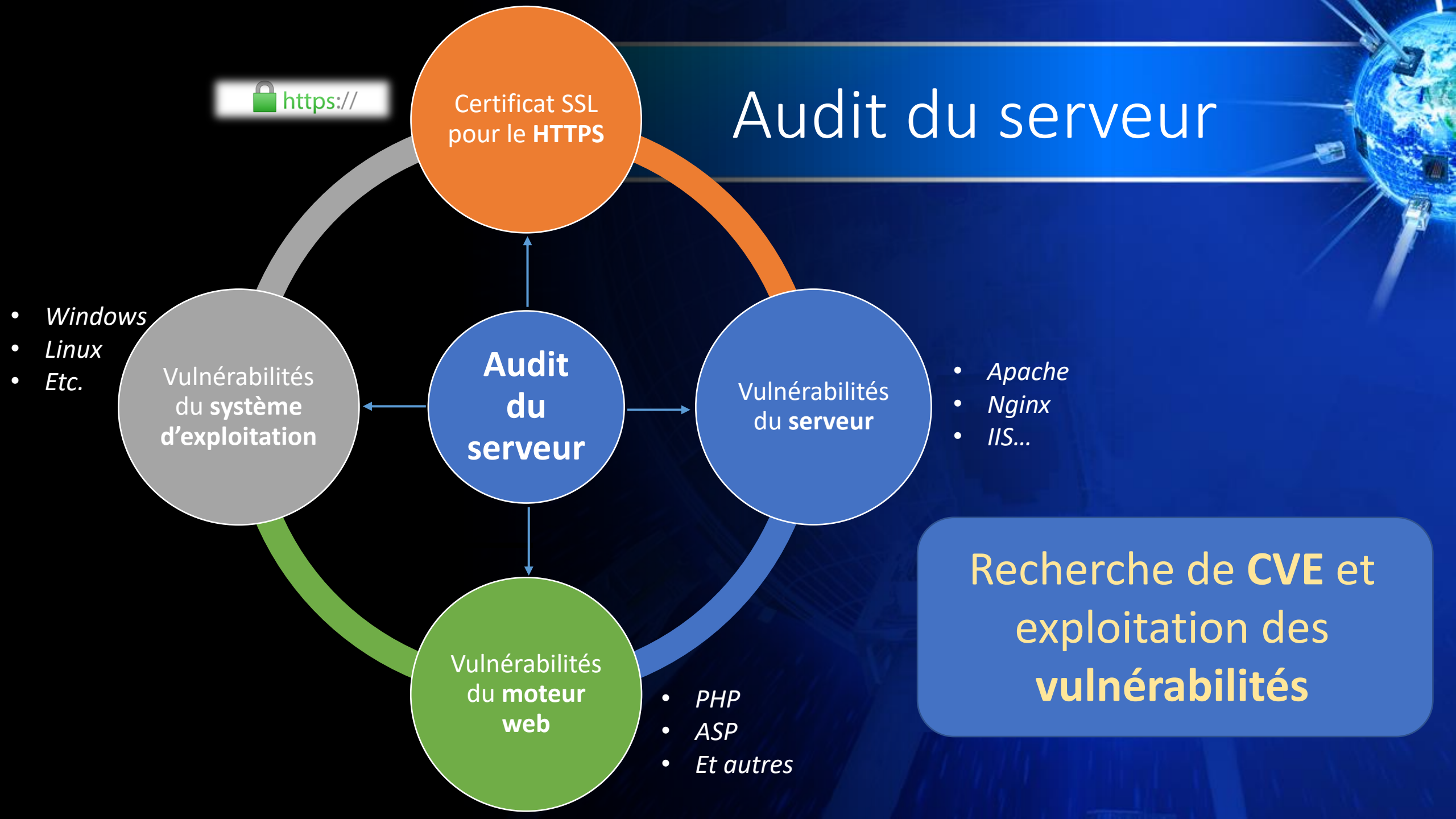
Nous prenons la place de **l'administrateur** du site

- *Avec tous les accès, les codes sources etc.*

Pour 2 audits :

- Audit du serveur
- Audit de vos sites Web

Audit du serveur



- *Windows*
- *Linux*
- *Etc.*

- *Apache*
- *Nginx*
- *IIS…*

- *PHP*
- *ASP*
- *Et autres*

Recherche de **CVE** et exploitation des **vulnérabilités**

Audit du site web

- Analyse selon le **Top 10 OWASP**
  - *Les 10 failles de sécurité les plus exploitées*
  - *Injection de code, exposition de données sensibles, XSS etc.*
- Recherche de **répertoires** cachés
- Recherche de **pages** cachées
  - *Fichiers de configuration, pages de test, scripts …*
- Evaluation des **bonnes pratiques** de sécurité
  - *Fuite d'informations techniques, sécurisation des cookies …*

Audit du site web

- Vulnérabilités du **CMS**
  - *WordPress, Jumla, Drupal et autres*
- Vulnérabilités des **modules** du CMS
- Audit de **code source**
- Enumération des utilisateurs
  - *Recherche d'Email*
- Evaluation de la réputation du site web

Recherche de **CVE** et exploitation des **vulnérabilités**

Les outils utilisés

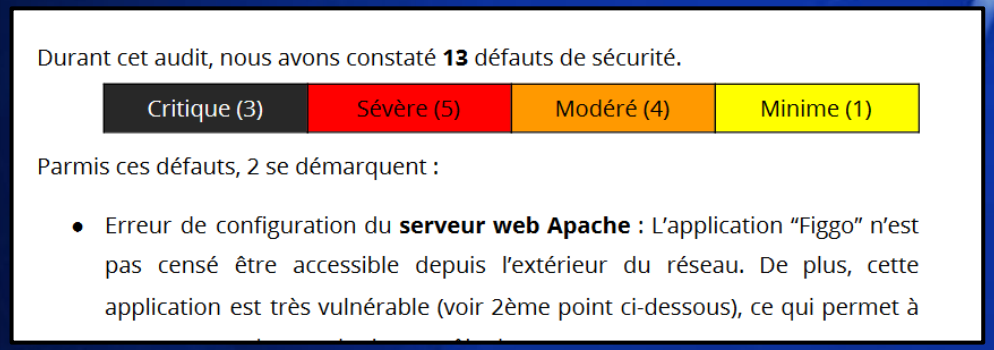
- Scanners de vulnérabilité des applications web
- Scanners de vulnérabilités des serveurs
- Framework d'exploitation
- Outil de récupération des enregistrements DNS
- Outil d'évaluation du SSL/TLS
- Recherche de sous-domaine et d'Email (OSINT)
- Recherche et Exploitation « à la main »
- Scanners de ports
- Outil d'exploitation des injections SQL
- Crawler de fichiers / répertoires
- Proxy Web
- Scripts « fait maison »

Le rapport

Un rapport **confidentiel** vous est fourni.

Ce dernier détaille :

- Les **vulnérabilités** trouvées.
- Leurs **impacts** et leurs **difficultés** d'exploitation.
- Les **recommandations** pour corriger ces failles.



Durant cet audit, nous avons constaté **13** défauts de sécurité.

Critique (3)	Sévère (5)	Modéré (4)	Minime (1)

Parmis ces défauts, 2 se démarquent :

- Erreur de configuration du **serveur web Apache** : L'application "Figgo" n'est pas censé être accessible depuis l'extérieur du réseau. De plus, cette application est très vulnérable (voir 2ème point ci-dessous), ce qui permet à

Ce rapport est en 2 parties :

- Une partie simplifiée, pour le comprendre sans connaissance technique particulière.
- Une partie technique, plus détaillée, pour guider les techniciens à résoudre ces failles.

CAPHEX CONSEILS & INVESTIGATIONS - 07.62.26.66.44 – CAPHEX@Protonmail.com