Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

Retour ANF : Nouvelles Menaces Sécurité des Applications Web

- Formation sur 3 jours suivie en janvier 2017
- Programme très dense
  - Risques, Réglementation sur les données à caractère personnel, Confiance et cryptographie, HTTP et HTTPS
  - Maîtrise d'œuvre déléguée en développement, Sensibilisation à la sécurité offensive, Bonnes pratiques
  - HTML5 et la sécurité, Méthodologies de politique de sécurité, Analyse de risques
- Focus sur Sensibilisation à la sécurité offensive et les Bonnes pratiques

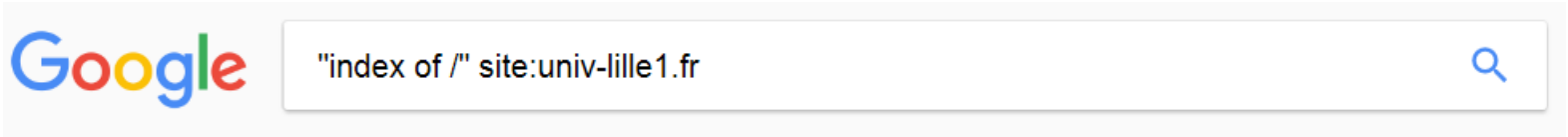
Resinfo

cnrs

DEVLOG RÉSEAU DU DEVELOPPEMENT LOGICIEL Recherche et Enseignement Supérieur

Google Dorks

- Méthode de recherche avancée sur Google
- Commande de base



- Liste de commandes http://www.webrankinfo.com/commandes/google
- Des centaines de Google Dorks sur le site exploit-db.com

EXPLOIT DATABASE

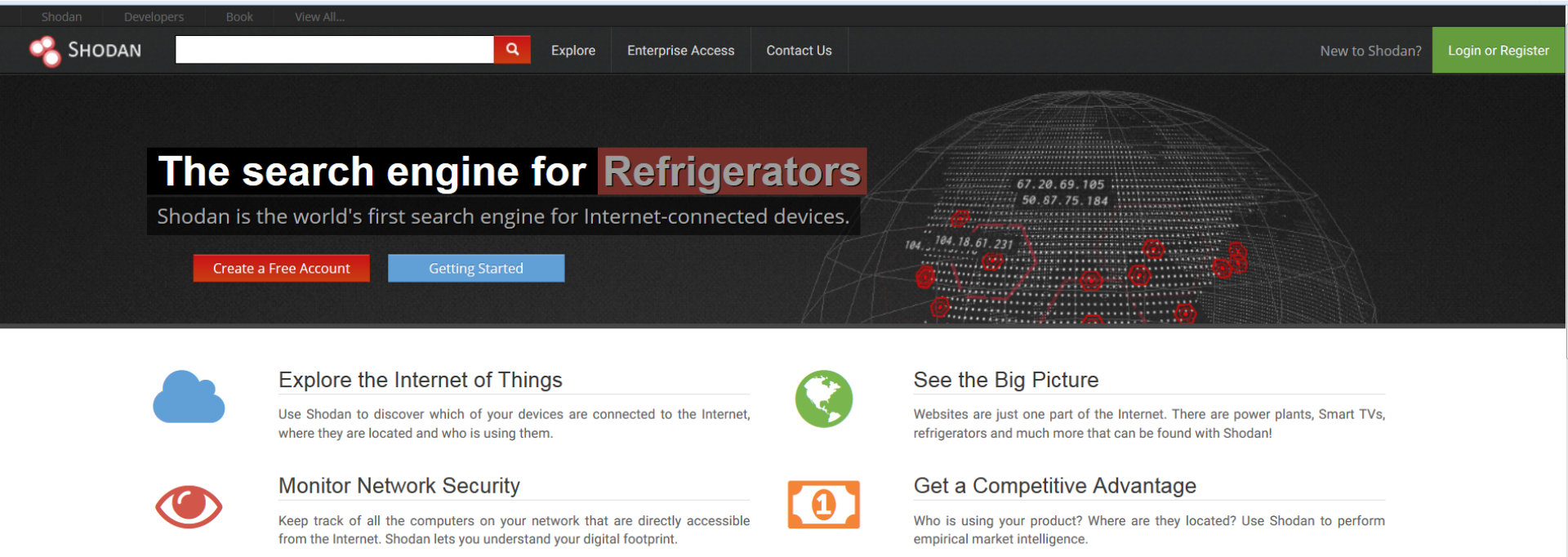
Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security's Exploit Database Archive

37026
Exploits Archived

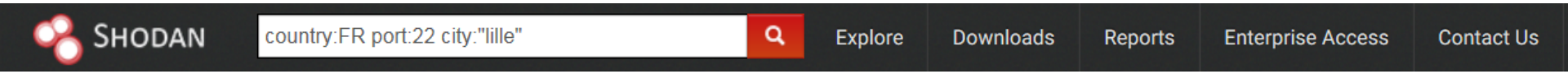
The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn **about the Exploit Database**.

Shodan


Shodan
Developers
Book
View All...
SHODAN
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
The search engine for Refrigerators
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.105
50.87.75.184
104.18.61.231
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Shodan

- Moteur de recherche le plus dangereux au monde
  - S'il y a une interface internet, Shodan peut la trouver
- Commande de base



Comment se prémunir

- Empêcher le listing d'un répertoire
  - Configuration générale d'Apache
  - Configuration du VirtualHost
  - Dans un fichier .htaccess
- Ne pas être trop bavard, livrer un minimum d'information
- Et aussi
  - Protéger son accès ssh
  - Adopter une politique de mots de passe robuste
  - Avoir un système à jour

OBSERVATORY by Mozilla

- Outil gratuit en ligne
- https://observatory.mozilla.org/
- Projet conçu pour aider les développeurs et les administrateurs système
  - Tester son site Web
  - Sécuriser son site Web
- Indique une note allant de A à F

Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

Test Scores

Test	Pass	Score	Explanation
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented
Cookies	–	0	No cookies detected
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented
Redirection	✓	0	Initial redirection is to https on same host, final destination is https
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented

- Content Security Policy qui fournit un en-tête HTTP pour déterminer des sources sûres de contenus pouvant être chargés sur une page
- Une redirection vers HTTPS mais affaiblie avec une redirection initiale HTTP

Resinfo

cnrs

DEVLOG RÉSEAU DU DEVELOPPEMENT LOGICIEL

httpd.conf

```
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header set X-Frame-Options "sameorigin"
Header set X-Content-Type-Options "nosniff"
#Header set Content-Security-Policy "default-src 'self'; script-src 'self'; https:"
#Header set Set-Cookie HttpOnly;Secure
```

- Paramétrage possible également dans .htaccess
- Sécurisation possible par l'administrateur système et par le développeur

Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

Scan Summary

B

Host:	lasir.univ-lille1.fr
Scan ID #:	3539189 (unlisted)
Test Time:	March 25, 2017 1:39 PM
Test Duration:	14 seconds
Score:	70/100
Tests Passed:	9/11

Recommended Change

Initiate Rescan

You're doing a great job with HTTPS and HTTP Strict Transport Security!

Since you're now only allowing connections over HTTPS, consider using the `Secure` flag to protect your cookies against their accidental transmission over HTTP. Furthermore, the use of `HttpOnly` protects your session cookies from malicious JavaScript.

- Mozilla Web Security Guidelines (cookies)

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

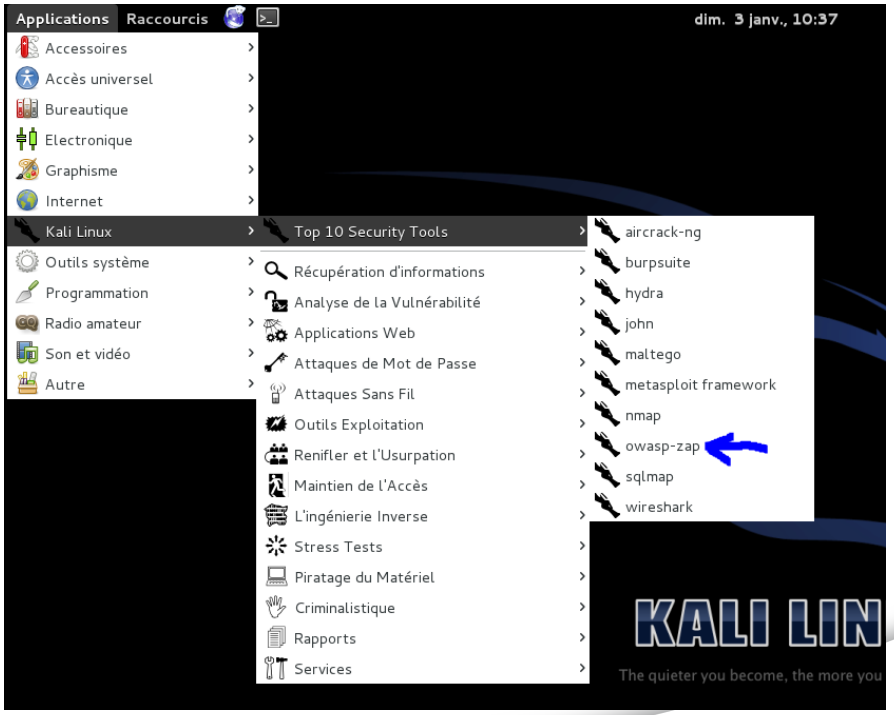
Resinfo

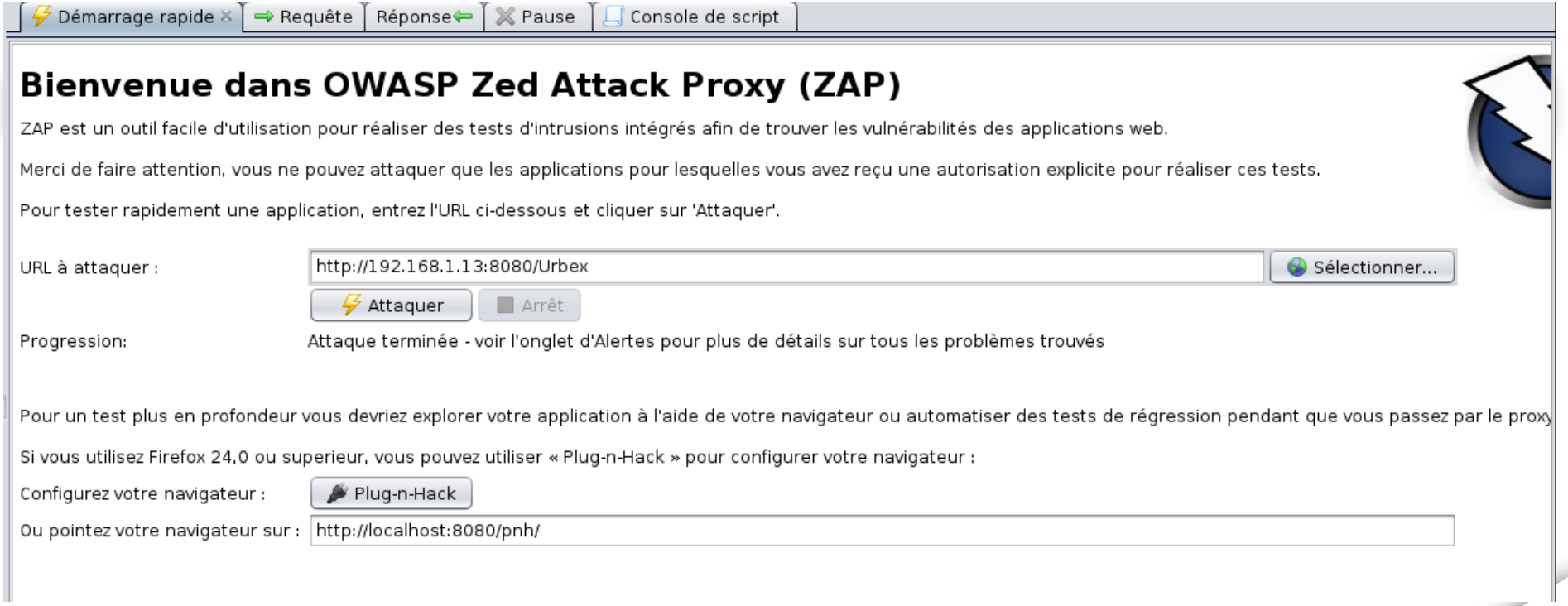
cnrs

DEVLOG RÉSEAU DU DEVELOPPEMENT LOGICIEL

OWASP Zed Attack Proxy Project

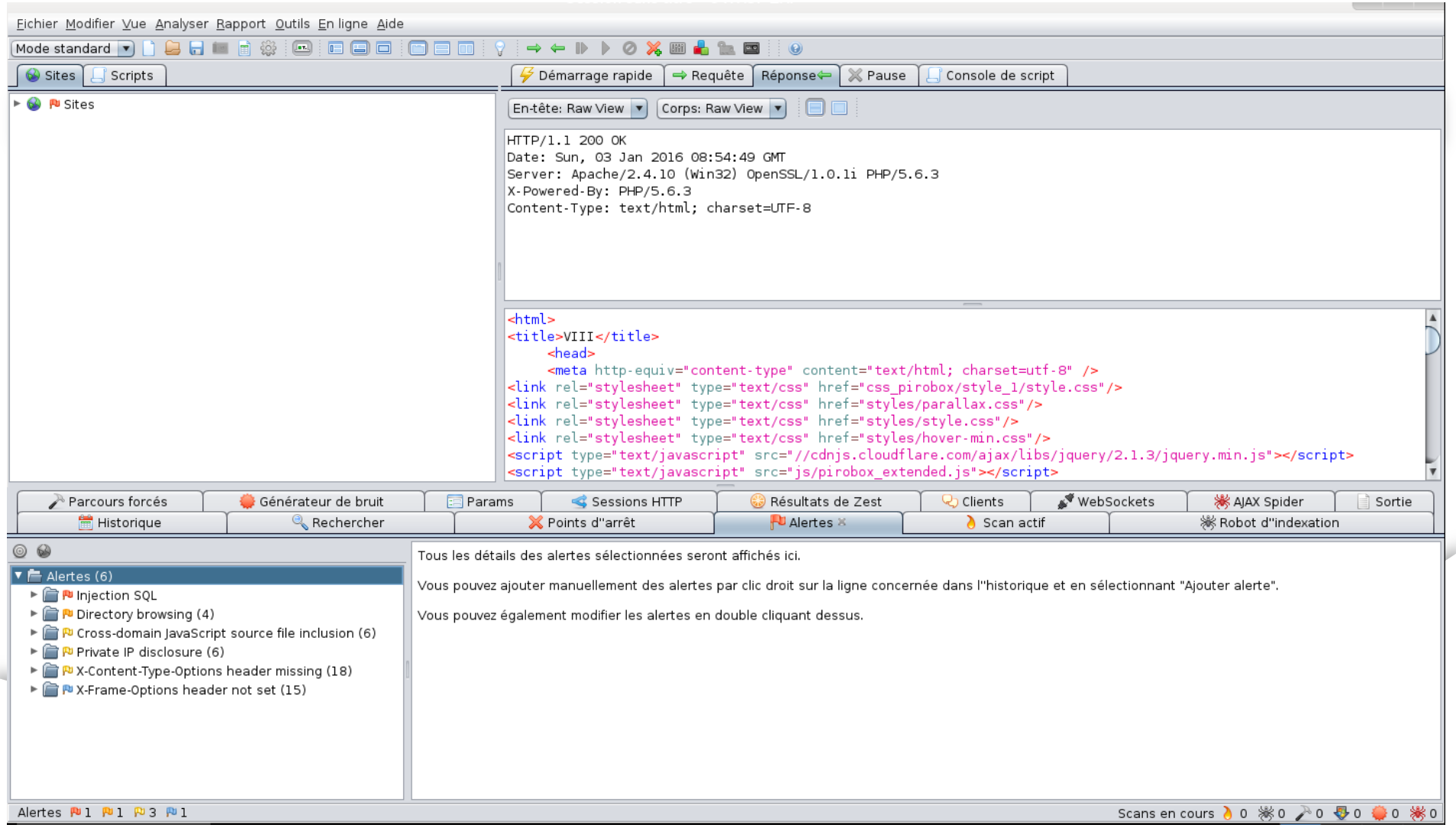
- OWASP ZAP via Kali Linux
  - Sécurité d'un site web
  - Sécurité d'un réseau
  - Sécurité d'un logiciel
  - …




Démarrage rapide
Requête
Réponse
Pause
Console de script
Bienvenue dans OWASP Zed Attack Proxy (ZAP)
ZAP est un outil facile d'utilisation pour réaliser des tests d'intrusions intégrés afin de trouver les vulnérabilités des applications web.
Merci de faire attention, vous ne pouvez attaquer que les applications pour lesquelles vous avez reçu une autorisation explicite pour réaliser ces tests.
Pour tester rapidement une application, entrez l'URL ci-dessous et cliquer sur 'Attaquer'.
URL à attaquer :
http://192.168.1.13:8080/Urbex
Sélectionner...
Attaquer
Arrêt
Progression:
Attaque terminée - voir l'onglet d'Alertes pour plus de détails sur tous les problèmes trouvés
Pour un test plus en profondeur vous devriez explorer votre application à l'aide de votre navigateur ou automatiser des tests de régression pendant que vous passez par le proxy
Si vous utilisez Firefox 24,0 ou superieur, vous pouvez utiliser « Plug-n-Hack » pour configurer votre navigateur :
Configurez votre navigateur :
Plug-n-Hack
Ou pointez votre navigateur sur :
http://localhost:8080/pnh/

Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

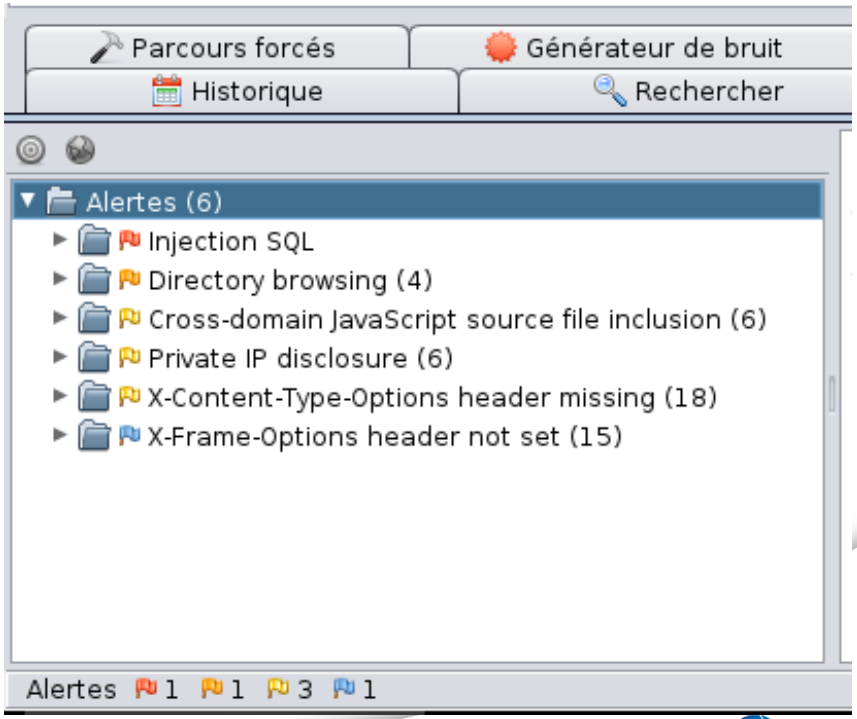


OWASP Zed Attack Proxy Project

- 6 alertes de sécurité
  - Injection SQL

    n°1 TOP 10 OWASP 2013
  - Alerte Cross-Domain
  - Alerte X-Frame-Options

    Header set X-Frame-Options DENY
  - ...



Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

10 points de sécurité qui devraient être inclus dans tout projet de développement

- Requêtes paramétrées
  - Éviter les injections (SQL, OS, LDAP)
- Encoder les données
  - Chaînes de caractères purement littérales et non interprétables par le navigateur.
- Valider toutes les entrées
  - Ne faire confiance à personne
- Implémenter les contrôles d'accès appropriés

Resinfo

cnrs

DEVLOG RÉSEAU DU DEVELOPPEMENT LOGICIEL

Min2RIEN

Métiers de l'Informatique Réunis en Réseau Inter-Etablissement du Nord

10 points de sécurité qui devraient être inclus dans tout projet de développement

- Établir les contrôles d'identité et d'authentification
- Protéger les données et la vie privée
  - Cartes de crédit, identifiants, informations d'authentification
- Implémenter la journalisation, la gestion des erreurs et la détection des intrusions
- Exploiter les fonctionnalités de sécurité des frameworks et bibliothèques de sécurité
- Inclure les exigences de sécurité spécifiques
- Conception et architecture de sécurité

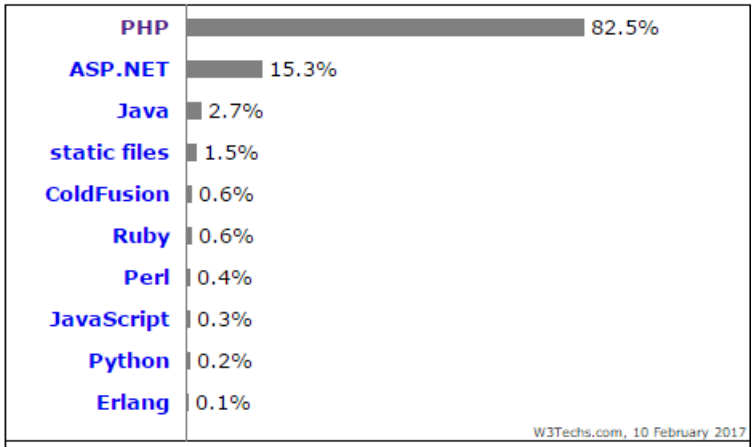
Resinfo

cnrs

DEVLOG RÉSEAU DU DEVELOPPEMENT LOGICIEL Recherche et Enseignement Supérieur

php et la sécurité

- Frameworks
  - Laravel, Symfony, Zend ...
- OWASP PHP Security Cheat Sheet
- Tester son code
  - https://repl.it/languages/php
- Brider votre php
  - Désactiver la commande exec()
  - php.ini



Percentages of websites using various server-side programming languages
Note: a website may use more than one server-side programming language

Conclusion

- Appliquer les correctifs de sécurité sur les systèmes , les CMS, les frameworks …
- Suivre les avis de sécurité. Consulter les RFC
- Culture sécurité
- Utiliser les frameworks et les IDE
- Utiliser des méthodologies orientées sécurité
- Tester, Tester, Tester ...

Conclusion

- Merci pour votre attention