

SÉCURITÉ DES SERVEURS ET DES APPLICATIONS

Méthodologie d'attaques



K. Poutrain



Aix*Marseille
université

02/04/2015

7^{ème} journée du réseau ARAMIS – Lyon

Plan



Les outils : Kali Linux & Owasp BWA

Méthodologie d'attaque : les étapes

Étude du cas : Les injections SQL

Démos



Les outils du test-lab

KALI LINUX™

"the quieter you become, the more you are able to hear"

Plateforme d'attaque

Distribution Linux (outils)

WEB APPLICATIONS

INFORMATION GATHERING

REVERSE ENGINEERING

FORENSICS TOOLS

VULNERABILITY ANALYSIS

WIRELESS ATTACKS EXPLOITATION TOOLS

PASSWORD ATTACKS

STRESS TESTING

<https://www.kali.org/>

KALI LINUX™ is a trademark of Offensive Security.

VS



OWASP BWA
(Broken Web Applications)

Plateforme web vulnérable

Machine virtuelle

Applications « école »

Applications réalistes vulnérables

Applications réelles vulnérables
(ancien wordpress, Joomla,...)

[https://www.owasp.org/index.php/
OWASP_Broken_Web_Applications_Project](https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)

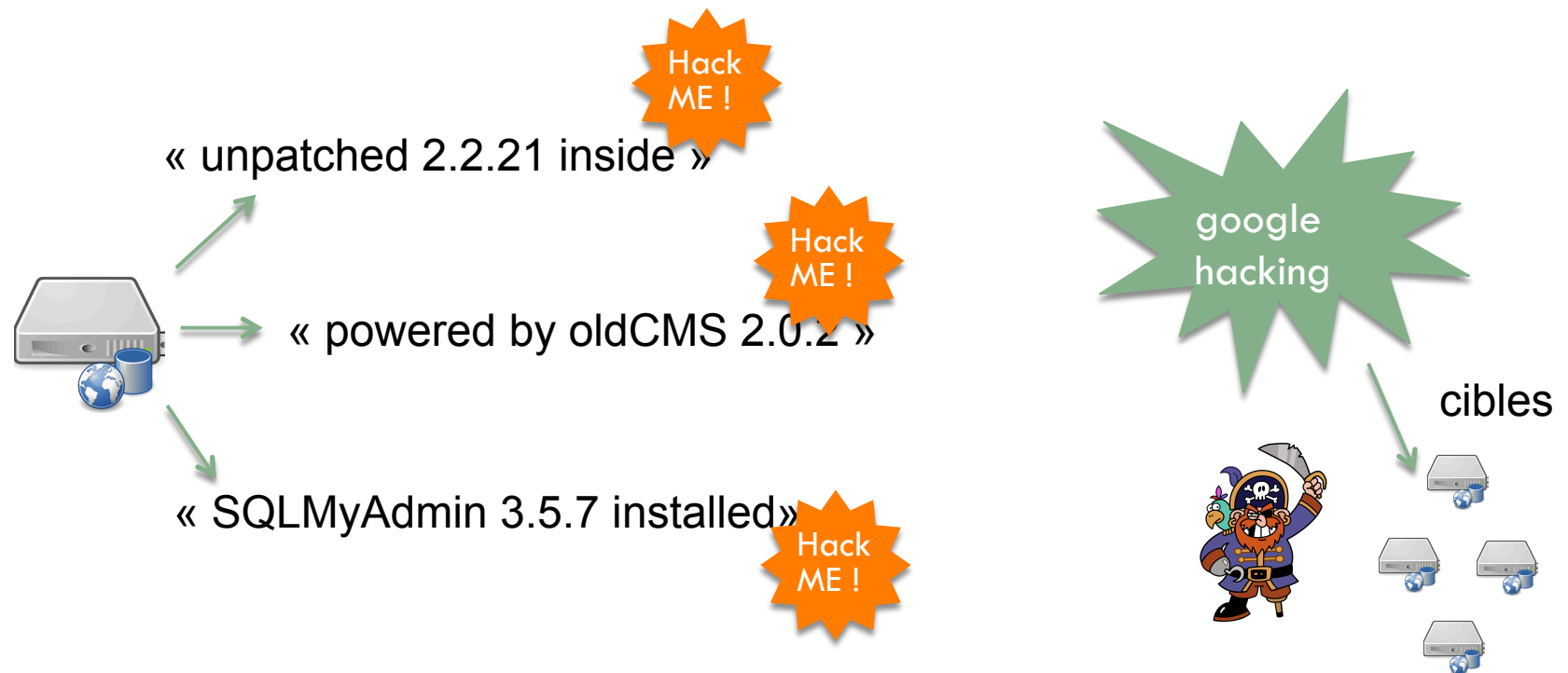
METHODOLOGIE D'ATTAQUE



Quelle(s) méthode(s) d'attaque ?

METHODOLOGIE D'ATTAQUE

CAS 1 : attaque opportuniste



LIMITER LA DIFFUSION D'INFORMATIONS !

METHODOLOGIE D'ATTAQUE

CAS 2 : attaque ciblée

- objectifs divers :
 - vol de données
 - altération d'information (défiguration)
 - mise en ligne de sites frauduleux (vente, phishing)
 - envoi de spams, obtention d'un shell, rebond...

=> Technique méthodique, exhaustive

METHODOLOGIE D'ATTAQUE : LES ÉTAPES CLES

- Reconnaissance (collecte d'informations)
- Cartographie de la surface d'attaque
- Exploitation (attaque)
- Élévation de privilège
- Conservation d'accès

RECONNAISSANCE



La plus importante des étapes !

- identifier le contenu de l'application ;
- analyser son comportement ;
- en comprendre le fonctionnement ;
- étudier son contexte (qui l'utilise, qui la développe ?).

=> cartographier l'application

- représentation structurelle (arborescence des fichiers, liens) ;
- représentation fonctionnelle (logique de l'application).

RECONNAISSANCE : CARTOGRAPHIE

Robot d'indexation automatique (spider/crawler) ?

Limites :

- liens dynamiques JavaScript ;
- liens accessibles après remplissage d'un formulaire...);
- risque de fermer la session (lien « logout ») ;
- attention aux actions dangereuses ! (reboot, réinitialiser la BDD...).

CARTOGRAPHIE PILOTÉE

Cartographie pilotée par l'utilisateur.

Proxy d'interception :



BurpSuite



OWASP-ZAP (Zed Attack Proxy)

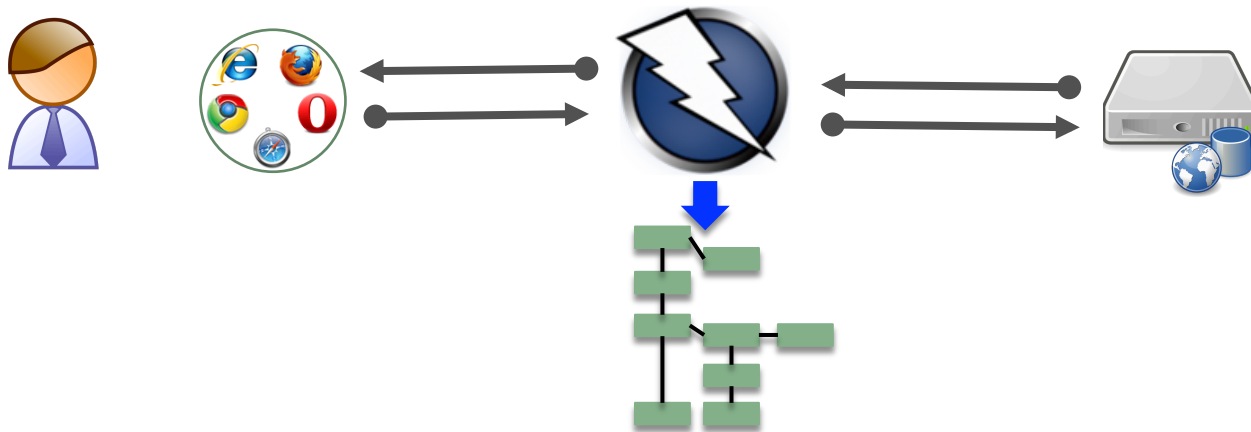
CARTOGRAPHIE PILOTÉE

1 - L'utilisateur réalise un **parcours exhaustif** des liens dans son navigateur.

Le proxy :

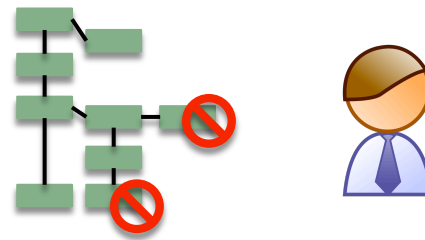
analyse les requêtes/réponses

construit la carte de l'application.

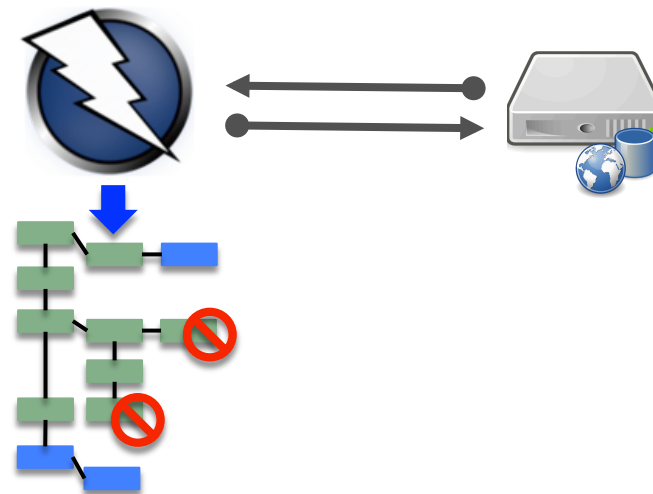


CARTOGRAPHIE PILOTÉE

2 – l'utilisateur **exclut** des liens dangereux



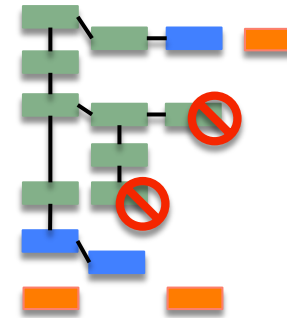
3 – on **complète** la cartographie à l'aide du mode automatique



RECONNAISSANCE

Recherche de contenu caché

- liens cachés (parties réservées de l'application) ;
- code de test ;
- fichiers de backup ;
- fichiers de logs ;
- etc...

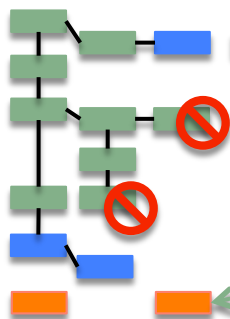


RECHERCHE DE CONTENU CACHÉ

robots.txt

User-agent: *
Disallow: /admin/
Disallow: /awstats/

Interface d'administration
Outil de statistiques
...



```
www.example.com/robots.txt
Disable
Cookies
CSS
Forms
Images
Informat

#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used: http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /logout/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/pass:ord/
Disallow: /user/login/
# Paths (no clean URLs)
Disallow: /?q=admin/
```

RECHERCHE DE CONTENU CACHÉ

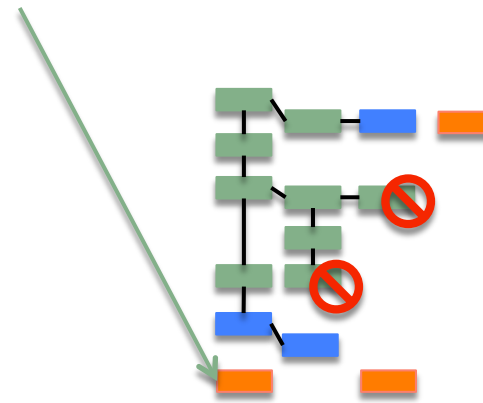
Force brute : listes de noms de fichiers/
répertoires (Dirbuster).

- « Parcours forcés » de ZAP
- Burp Intruder de BurpSuite.

Attention aux boucles infinies si l'application
WEB renvoie un 200 OK + page d'erreur
standard...

RECHERCHE DE CONTENU CACHÉ

- revue du code client (html, javascript) :
commentaires développeurs...
- raisonnement par inférence :
 - RapportActivites2014.pdf =>
RapportActivites2013.pdf
 - ForgotPassword.php => ResetPassword.php



DÉMO : CARTOGRAPHIE ZAP



RECONNAISSANCE



OSINT (OpenSource Intelligence)

- Principe : utiliser les sources publiques
- Avantage : totalement furtif

Ex : Google hacking

OSINT : GOOGLE HACKING

Quelques opérateurs de recherche avancée

Opérateur	Rechercher
<code>intitle:mot</code>	le mot dans le titre (élément HTML title).
<code>inurl:mot</code>	le mot dans l'URL de la page
<code>intext:mot</code>	le mot dans le corps du texte (élément HTML body)
<code>filetype:type</code>	un type de document (xls, pdf, doc, ...)
<code>site:domaine</code>	les pages indexées pour le domaine ex. site:www.cnrs.fr
<code>" phrase "</code>	la phrase exacte
<code>*</code>	un mot : ex <code>"un * DVD"</code> => un lecteur DVD, un graveur DVD
<code>.</code>	un caractère quelconque
<code>-mot</code>	les réponses qui n'ont pas ce mot ex <code>-intitle:forum</code>
<code>+mot</code>	le mot (force la prise en compte de : le, et, de, ...)
AND, OR	recherche ET (par défaut) / OU entre les termes

OSINT : GOOGLE HACKING

Informations sur le serveur HTTP

GOOGLE `intitle:"index of" intext:"Apache/2*" intext:"server at"`

`Apache/2.4.6 (Unix) PHP/5.4.17 OpenSSL/1.0.1 Server at`

Recherche ciblée

GOOGLE `site:www.ac-***** intitle:"index of" intext:"Microsoft.IIS/* server at"`

`Microsoft-IIS/8.0 Server at www.ac`

Erreurs MySQL

GOOGLE `mysql error -intitle:error -intitle:php -forum -forums -intitle:mysql`

`select * from theme_news where id=`

Mysql Error:You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

`SELECT * from theme_news where id=`

OSINT : GOOGLE HACKING DATABASE

En panne d'inspiration ? <http://www.exploit-db.com/google-dorks/>



The screenshot shows the Google Hacking Database website. At the top, the logo reads "GOOGLE HACKING-DATABASE" with "GOOGLE" in its multi-colored font and "HACKING-DATABASE" in white. Below the logo, it says "Welcome to the google hacking database". A paragraph follows: "We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!". Below this is a search section with the heading "Search Google Dorks". It features a "Category:" dropdown menu set to "All", a "Free text search:" input field, and a "Search" button. Underneath is a section titled "Latest Google Hacking Entries" which contains a table with three columns: "Date", "Title", and "Category".

Date	Title	Category
2015-03-16	allintext:Copyright Smart PHP Poll. All Rights Res...	Vulnerable Servers
2015-03-10	ext:sql intext:"alter user" intext:"...	Files containing passwords
2015-03-04	allinurl:moadmin.php -google -github	Vulnerable Servers
2015-02-27	inurl:/wp-content/wpbackup_backups	Sensitive Directories
2015-02-19	"Config" intitle:"Index of" in...	Sensitive Directories
2015-02-17	intitle:"AP Router New Generation" intex...	Various Online Devices
2015-02-11	inurl:./cgi-bin/webproc	Various Online Devices
2015-02-11	inurl:./cgi-bin/luci	Various Online Devices
2015-02-11	"jos_users" intitle:"Index of"	Sensitive Directories
2015-02-09	inurl:"security/xamppdirpasswd.txt"	Files containing passwords

OSINT : RETOUR VERS LE PASSÉ

Retrouver des fonctionnalités passées/cachées : <http://archive.org/web/>

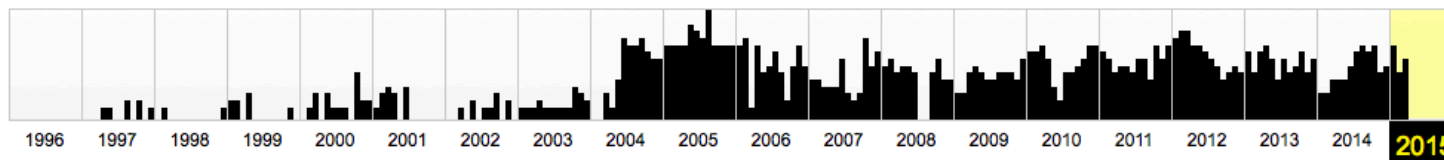


BROWSE HISTORY

<http://www.cnrs.fr>

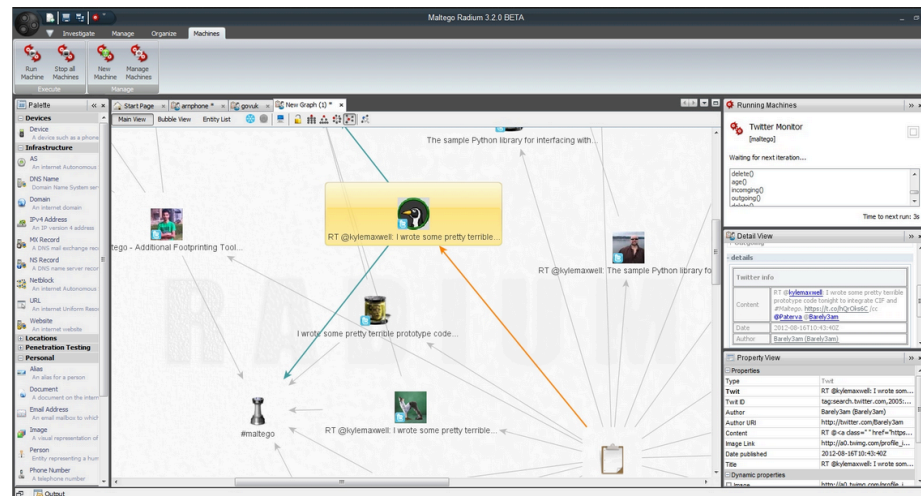
Saved **1 256 times** between **avril 10, 1997** and **mars 28, 2015**.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



RECONNAISSANCE : OSINT

- identifier les développeurs de l'application ;
- leurs interventions sur les forums ;
- facebook, twitter... ;
- bouts de code ;
- analyser leurs habitudes ;



MALTEGO (<https://www.paterva.com/web6/products/maltego.php>)



RECONNAISSANCE : INFRASTRUCTURE



Failles au niveau infrastructure web :

- Type de serveur, version ou modules installés ;
- Système d'exploitation
- Défauts de configuration httpd ;
- Composants logiciels (CMS...) ;
- ...

RECONNAISSANCE : INFRASTRUCTURE

Scanners de vulnérabilités

- WAPITI 2.3.0(10/2013)
- NIKTO 2.1.5 (03/2015)
- ARACHNI 1.0.6 (12/2014)
- SKIPFISH 2.10b (12/2012)
- W3AF (03/2014)



RECONNAISSANCE : INFRASTRUCTURE

Les fonctionnalités :

- Identifier le système d'exploitation, serveur, langage de programmation ;
- Fichiers intéressants (phpinfo, passwd.txt...) ;
- Scripts d'upload ;
- recherche de vulnérabilités (injections de code, SQL, LDAP, XSS, XPATH, CSRF, etc... indexes de répertoires, CMS obsolètes)

RECONNAISSANCE : INFRASTRUCTURE



Les limites :

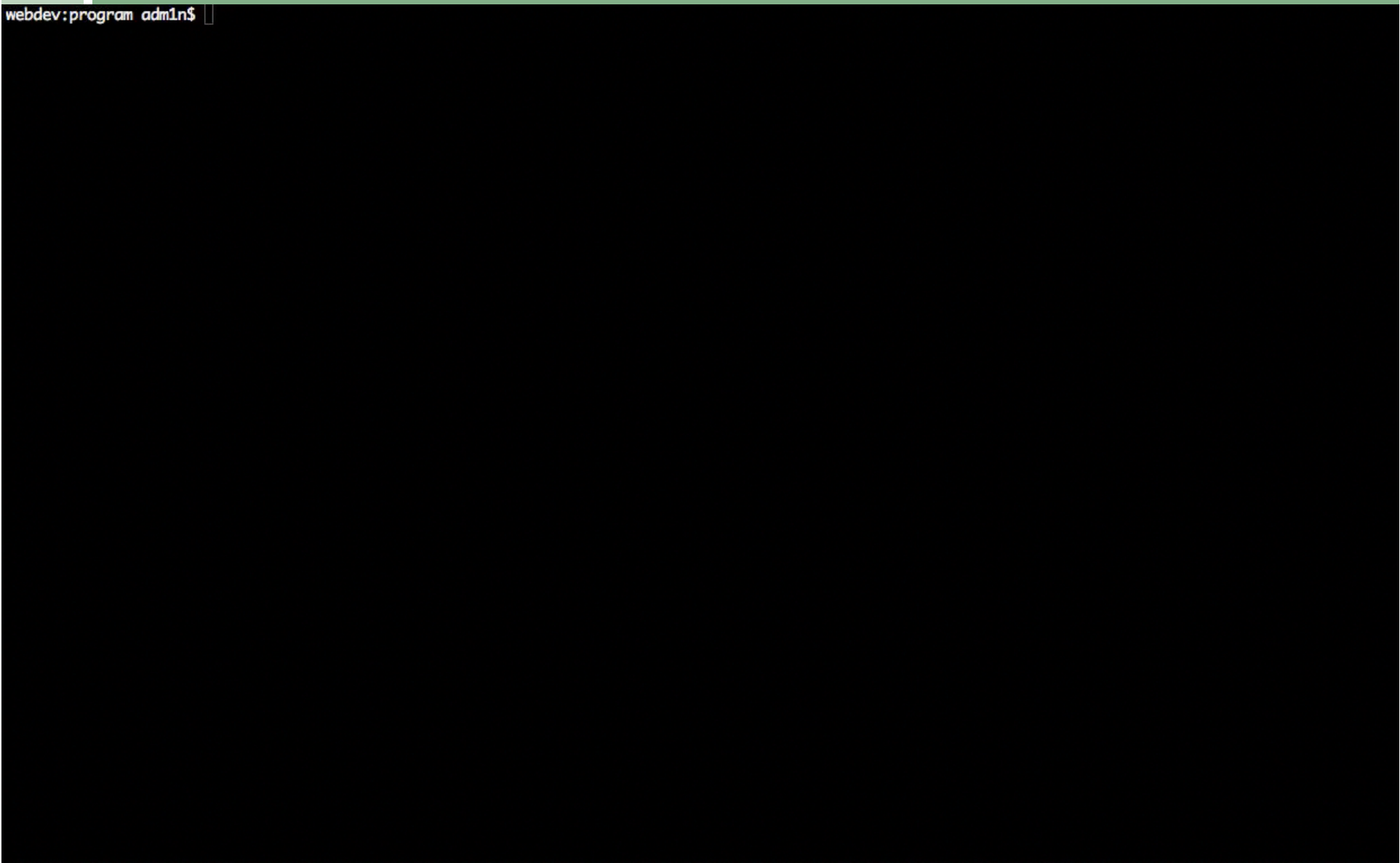
Génèrent de nombreux faux positifs/négatifs

⇒ Nécessite de vérifier manuellement les résultats.

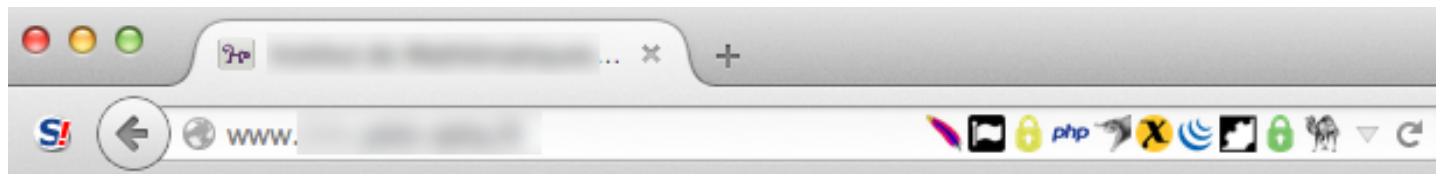
Attention au paramétrage de l'outil (scans hors contexte..., boucles infinies – page d'erreur unifiée)

DEMO : NIKTO

```
webdev:program admin$
```



RECONNAISSANCE : INFRASTRUCTURE



Identification des technologies web

-  **Apache 2.2.20**
Serveur web
-  **Font Awesome**
Script de police
-  **OpenSSL 1.0.0e**
Extension de serveur web
-  **PHP 5.2.17**
Language de programmation
-  **SPIP**
CMS
-  **UNIX**
Système d'exploitation
-  **jQuery**
Framework JavaScript
-  **mod_perl 2.0.4**
Extension de serveur web
-  **mod_ssl 2.2.20**
Extension de serveur web
-  **Perl**
Language de programmation


RECONNAISSANCE : INFRASTRUCTURE

Analyse de l'en-tête de la réponse HTTP (inspecteur du navigateur) :

Inspecteur			Console	Débugueur	Éditeur de style	Performances	Réseau
✓	Méthode		En-têtes	Cookies	Paramètres	Réponse	
● 200	GET	/	URL de la requête : http://www. [REDACTED] Méthode de la requête : GET Code de statut : ● 200 OK				
● 200	GET	color	Filter les en-têtes				
● 200	GET	barre	En-têtes de la réponse (1,316 Ko)				
● 200	GET	spip.r	Composed-By : "SPIP 3.0.17 @ www.spip.net + spip(3.0.17),compagnon(1.4.1),dump(1.6.7),images(1.1.9),forum(1.8.34),jqe...1.3.6),compresseur(1.				
● 200	GET	calen	Connection : "Keep-Alive"				
● 200	GET	jquer	Content-Type : "text/html; charset=utf-8"				
● 200	GET	jquer	Date : "Sat, 28 Mar 2015 17:42:31 GMT"				
● 200	GET	jquer	Keep-Alive : "timeout=5, max=100"				
● 200	GET	jquer	Last-Modified : "Sat, 28 Mar 2015 17:42:31 GMT"				
● 200	GET	ajaxC	Server : "Apache/2.2.20 (Unix) mod_ssl/2.2.20 OpenSSL/1.0.0e DAV/2 mod_fcgid/2.3.6 PHP/5.2.17 proxy_html/3.1.1 mod_perl/2.0.4 Perl/v5.12.3"				
● 200	GET	jquer	Transfer-Encoding : "chunked"				
● 200	GET	spip.r	Vary : "Cookie,Accept-Encoding"				
● 200	GET	jquer	X-Powered-By : "PHP/5.2.17"				
● 200	GET	jquer	X-Spip-Cache : "86400"				
● 200	GET	spip.r					

RECONNAISSANCE : INFRASTRUCTURE



 http://toolbar.netcraft.com/site_report?url=http://...

Site report for [www. \[redacted\]](#)

Search... →

Lookup another URL: Enter a URL here

Share: [f](#) [t](#) [in](#) [g+](#) [Y](#) [v](#)

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Registry Phishing Alerts
- Domain Registration Risk
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

Background

Network

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
[redacted]	[redacted]	Linux	Apache/2.2.22 Ubuntu	16-Jul-2014
[redacted]	[redacted]	Linux	Apache	26-May-2014
[redacted]	[redacted]	Linux	Apache	20-Dec-2011
[redacted]	[redacted]	Linux	Apache/2.2.11 Debian mod_jk/1.2.20-dev PHP/5.2.6-3 with Suhosin-Patch mod_python/3.3.1 Python/2.5.4 mod_ssl/2.2.11 OpenSSL/0.9.8g	8-Jun-2009
[redacted]	[redacted]	Linux	Apache/2.2.11 Debian mod_jk/1.2.20-dev PHP/5.2.6-3 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.11 OpenSSL/0.9.8g	7-Mar-2009
[redacted]	[redacted]	Linux	Apache/2.2.9 Debian mod_jk/1.2.20-dev PHP/5.2.6-1lenny2 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g	29-Jan-2009
[redacted]	[redacted]	Linux	Apache/2.2.9 Debian mod_jk/1.2.20-dev PHP/5.2.6-0.1lenny1 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g	27-Jan-2009
[redacted]	[redacted]	Linux	Apache/2.2.9 Debian mod_jk/1.2.20-dev PHP/5.2.6-5 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g	15-Oct-2008
[redacted]	[redacted]	Linux	Apache/2.2.9 Debian mod_jk/1.2.20-dev PHP/5.2.6-3 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g	22-Sep-2008
[redacted]	[redacted]	Linux	Apache/2.2.9 Debian mod_jk/1.2.20-dev PHP/5.2.6-2 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g	28-Jul-2008

Si aucune information dans la réponse HTTP => prise d'empreinte HTTP

RECONNAISSANCE : INFRASTRUCTURE



Différences HTTP :

- lexicales (ponctuation, phrases)

Requête	Apache/2.4.6	IIS/5.0
GET / xxx HTTP/1.1	404 Not Found	404 Object Not Found

- syntaxiques (ordre des champs, valeurs listées)

Requête	Apache/2.4.6	IIS/8.0
HEAD / HTTP/1.1	Date: Server:	Server: Date:

- sémantiques (interprétation différente)

Requête	Apache/2.4.6	IIS/8.0
GET / HTTP/ 5.0	200 OK	400 Bad Request
GOT / HTTP/1.1	405 Method Not Allowed	404 Not Found

RECONNAISSANCE : INFRASTRUCTURE



https://w3dt.net/tools/httprecon

HTTPRecon (Server Fingerprint)

Target: [REDACTED]
Tests: 9 test cases
Scan: [REDACTED]
Export: [REDACTED]

Contents

1. Summary
2. Matches
3. Responses
4. Details

Summary ↑

An advanced web server fingerprinting for the host [REDACTED] and port tcp/80 was done with 9 test cases at [REDACTED].

This analysis was able to determine the target httpd service as Apache 2.2.3 with 65 fingerprint hits in the database.

List of Matches ↑

Name	Hits	Match
1. Apache 2.2.3	65	100%
2. AOLserver 4.0.10	63	96.92%
3. Apache 1.3.33	63	96.92%
4. Apache 2.0.46	62	95.38%
5. nginx 0.6.16	62	95.38%

Cet outil laisse des traces dans les logs du serveur web !

RECONNAISSANCE : INFRASTRUCTURE



Identification des technologies côté serveur

- extensions de fichiers ;
- noms de répertoires ;
- jetons de session (JSESSIONID, ASPSESSIONID, PHPSESSIONID, etc...)

=> Recherche de vulnérabilités publiées pour tous les composants identifiés

RECONNAISSANCE : ANALYSE LOGIQUE

Analyser la logique de l'application

- Recenser les fonctionnalités :
 - principales, mais aussi secondaires
 - fonctions d'aide
 - génération de logs
 - gestion des erreurs
 - ...
- Trouver des paramètres (GET/POST) « secrets » :

test/debug = 1/true/yes

RECONNAISSANCE : ANALYSE LOGIQUE

Recenser les mécanismes de sécurité :

- gestion des sessions,
- authentification,
- contrôle d'accès,
- gestion des mots de passe : changement, recouvrement...

RECONNAISSANCE : POINTS D'ENTRÉES

Inventorier **tous les points d'entrées** utilisateurs (y compris cachés)

+ les traitements réalisés sur les données utilisateur :

- URL
- Paramètres query string
- Paramètres POST
- Cookies
- En-têtes HTTP

=> Vecteurs potentiels d'attaques

RECONNAISSANCE : VECTEURS PÉRIPHÉRIQUES

Identifier les vecteurs d'attaque périphériques.

Données échangées avec d'autres serveurs :

- Serveur de mails
- Autres serveurs webs
- Webservices
- NIDS analyse le trafic ?

CARTOGRAPHIE DE LA SURFACE D'ATTAQUE



Associer vecteurs ⇔ types de vulnérabilités

- Interaction avec un SGBD = injection SQL
- Affichage d'information utilisateur = XSS
- Formulaire d'authentification = attaque de force brute, énumération de noms
- Upload de fichiers = traversée de chemin, dépôt de scripts
- Contrôle d'accès = élévation de privilèges
- Messages d'erreur (php, mysql) = fuites d'informations
- etc...

DÉMO : ZAP, SCAN ACTIF

The screenshot displays the OWASP Zed Attack Proxy (ZAP) interface. The main window shows a welcome message in French: "Bienvenue dans OWASP Zed Attack Proxy (ZAP)". Below the message, there is a form to enter a URL to attack, with "http://" entered. The progress status is "Non démarré".

The left sidebar shows a tree view of the scanned site structure, including folders like "upload" and "users", and various endpoints such as "GET:login.php", "POST:register.php", and "GET:users".

At the bottom, a table displays the scan results. The table has columns for Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, Size Resp. Header, and Size Resp. Body. The scan is currently at 2% completion.

Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	Size Resp. Header	Size Resp. Body
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	444 bytes	0.00 KiB
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	443 bytes	1.01 KiB
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	443 bytes	1.91 KiB
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	443 bytes	1.09 KiB
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	443 bytes	3.18 KiB
07/03/15 08:28:45	07/03/15 08:28:45	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	444 bytes	354 bytes
07/03/15 08:28:46	07/03/15 08:28:46	GET	http://192.168.56.103:80/WackoPICKO/css/blueprint...	200	OK	443 bytes	2.22 KiB
07/03/15 08:28:54	07/03/15 08:28:54	GET	http://192.168.56.103:80/WackoPICKO/guestbook/	200	OK	516 bytes	8.01 KiB
07/03/15 08:29:07	07/03/15 08:29:07	GET	http://192.168.56.103:80/WackoPICKO/cart/	200	OK	357 bytes	1.46 KiB
07/03/15 08:29:09	07/03/15 08:29:09	GET	http://192.168.56.103:80/WackoPICKO/cart/action.p...	303	See Other	559 bytes	0 bytes
07/03/15 08:29:09	07/03/15 08:29:09	GET	http://192.168.56.103:80/WackoPICKO/cart/add_cou...	200	OK	376 bytes	0 bytes
07/03/15 08:29:09	07/03/15 08:29:09	GET	http://192.168.56.103:80/WackoPICKO/cart/confirm...	303	See Other	559 bytes	0 bytes
07/03/15 08:29:09	07/03/15 08:29:09	GET	http://192.168.56.103:80/WackoPICKO/cart/review.p...	303	See Other	559 bytes	0 bytes
07/03/15 08:29:32	07/03/15 08:29:32	GET	http://192.168.56.103:80/WackoPICKO/images/	200	OK	357 bytes	1.08 KiB

DÉMO : ZAP, SCAN ACTIF : les dégâts...

```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users;
```

id	login	firstname	lastname	password	salt	tradebux	created_on	last_login_on
1	Sample User	Sample	User	3e912f8fc814831804d735dc2fcbc3cfa75c28e3	NjM2	130	2009-01-05 14:29:00	2015-03-09 21:50:55
2	bob	I Am Bob	Gilbert	abd09072e674720d87ddd27122f67eedbc4b0d08	MjKx	96	2009-01-05 14:51:05	2009-02-18 14:54:26
4	scanner1	Scanner	1	af256af3d4fda990dbe546daa04e5c75eae356ea	ODUy	100	2009-02-18 14:46:21	2012-04-03 22:23:56
5	scanner2	Scanner	2	f9335d39b2b78018c2b8affa7fc7b0917a3300a7	MzI5	100	2009-02-18 14:46:34	2012-04-03 22:24:46
6	scanner3	Scanner	3	43754746b4043c852864bb321e4f2648d1421c18	Nzk3	100	2009-02-18 14:46:51	2009-02-18 14:46:51
7	scanner4	Number	4	e514a672396679528c766a92a857eac4b22bc667	NjEx	100	2009-02-18 14:47:04	2009-02-18 14:47:04
8	scanner5	Number	5	f38ae9b0b6b1ad2a2a2721841c0cc89b31e044cb	NTQw	100	2009-02-18 14:47:18	2009-02-18 14:47:18
9	wanda	Wanda	Granat	4e4465300b14b314384a6375a837f0532822d3c8	Nzcz	100	2009-02-18 14:53:23	2009-02-18 14:53:23
10	calvinwatters	Calvin	Watters	81418ed6e9bd15076d2f43e17b9f5a27c7e55ef7	Nzc5	100	2009-02-18 14:56:11	2009-02-18 14:56:11
11	bryce	Bryce	Boe	478fb0b83851b3d16ffc5a2554a4d616f1235156	NjY3	74	2009-02-18 14:57:36	2009-02-18 14:57:36
12	johnsmith	John	Smith	3144a389b6743324ba65f6bb7ba7c78a784cdfb0	NjE4	100	2015-03-09 18:28:47	2015-03-09 18:28:47
13	john	john	smith	d37831daa672859d5a66b9e63e7b708df95d025b	MTIx	100	2015-03-09 21:40:22	2015-03-09 21:40:22
14	ZAP	ZAP	ZAP	ab7aa166951ce42cd956f809ccdc04c3ca524c86	MTc-	100	2015-03-09 21:41:39	2015-03-09 21:49:04
15	/WEB-INF/web.xml	john	smith	d47f15114c301003b6afde8316514e929f0bf8f3	ODk2	100	2015-03-09 21:47:25	2015-03-09 21:47:25
16	/Windows/system.ini	john	smith	f8c4058f68794a1e68c54152ae8688d476e3a06b	NTIz	100	2015-03-09 21:47:25	2015-03-09 21:47:25
17	/etc/passwd	john	smith	2b18eebc968b00644951a2cb68ca6ebd95734eb7	NzY5	100	2015-03-09 21:47:25	2015-03-09 21:47:25
18	\\WEB-INF/web.xml	john	smith	dc0c673876538ab14e49c475d54c2c146d2c6a90	MzQ-	100	2015-03-09 21:47:26	2015-03-09 21:47:26
19	\\Windows/system.ini	john	smith	0a57394a524fbb707462ace044025873730cb3ca	NjQ0	100	2015-03-09 21:47:26	2015-03-09 21:47:26
20	\\etc/passwd	john	smith	b8b1e7c2b72fd98590b25066089d01d5b2a57c10	MjE0	100	2015-03-09 21:47:26	2015-03-09 21:47:26
21	c:/WEB-INF/web.xml	john	smith	b45d7023c12d936d77c503efd6e4b810dfc80ba	Mzg3	100	2015-03-09 21:47:26	2015-03-09 21:47:26
22	c:/Windows/system.ini	john	smith	9d069433e9eff89370c780825804f4c92ced7759	MzU5	100	2015-03-09 21:47:26	2015-03-09 21:47:26
23	c:/etc/passwd	john	smith	895e20454e9677101b58a92e711be1e3e69e38d7	MTUy	100	2015-03-09 21:47:26	2015-03-09 21:47:26
24	c:/WEB-INF/web.xml	john	smith	450730d907f189fac4174d97a22e925781e201f8	Njc0	100	2015-03-09 21:47:26	2015-03-09 21:47:26
25	c:/Windows/system.ini	john	smith	663c116454a721ad60c5d327f74668c3af982ffb	ODgx	100	2015-03-09 21:47:26	2015-03-09 21:47:26
26	c:/etc/passwd	john	smith	0325253d99e2d5f0b34e113bd12ba18ea8f190c9	Mjk2	100	2015-03-09 21:47:26	2015-03-09 21:47:26
27	../../../../../../../../../../../../../../../../	john	smith	393c192ae62ab01b31298bd8c58617cc3df5dd18	Mjk4	100	2015-03-09 21:47:26	2015-03-09 21:47:26
28	../../../../../../../../../../../../../../../../	john	smith	76b29e69fd5c211c8072c11800a20696154186e0	NDM0	100	2015-03-09 21:47:26	2015-03-09 21:47:26
29	../../../../../../../../../../../../../../../../WE	john	smith	d161fb9d4d93017d8316182a60a583e614126f10	MzI2	100	2015-03-09 21:47:27	2015-03-09 21:47:27
30	../../../../../../../../../../../../../../../../Wi	john	smith	bdefd6a498f6b352da5cbe21f20db055a0b869c	NDk4	100	2015-03-09 21:47:27	2015-03-09 21:47:27
31	../../../../../../../../../../../../../../../../et	john	smith	c9d0d4f130d61acc703c83713ced38a483901a5c	MTY5	100	2015-03-09 21:47:27	2015-03-09 21:47:27
32	../../../../../../../../../../../../../../../../WE	john	smith	cf01ba845e6ad0edb093416b45c01774ab580a0	NTg-	100	2015-03-09 21:47:27	2015-03-09 21:47:27
33	../../../../../../../../../../../../../../../../Wi	john	smith	3f2fe94547615639305ef5e12b5d06e8c219d462	MzA4	100	2015-03-09 21:47:27	2015-03-09 21:47:27
34	../../../../../../../../../../../../../../../../.et	john	smith	7e3b894735e2b5d5856e38a408a19844b61e15fa	NTY-	100	2015-03-09 21:47:27	2015-03-09 21:47:27
35	thisshouldnotexistandhopefullyitwillnot	john	smith	e79e937ec651753f1701240ed4b0baaafbe6100b	NTg3	100	2015-03-09 21:47:27	2015-03-09 21:47:27
36	http://www.google.com/	john	smith	aa021c5f710ea74b029398a605917a34310452be	NjUx	100	2015-03-09 21:47:34	2015-03-09 21:47:34
37	http://www.google.com:80/	john	smith	7afd25740a3de454dd1350fbdee247f66c685af1	Nzgy	100	2015-03-09 21:47:34	2015-03-09 21:47:34
38	http://www.google.com	john	smith	57cbb9039f7a5c689f269b283d67b9a5ca698665	NzQw	100	2015-03-09 21:47:34	2015-03-09 21:47:34
39	http://www.google.com/search?q=OWASP%20ZAP	john	smith	e51958ace1fa088adcc78c8d49072d18774be1cc	NDA0	100	2015-03-09 21:47:34	2015-03-09 21:47:34

EXPLOITATION



Exploitation : Attaque.

- **Altération méthodique** des données
 - Ajout de variables
 - Suppression de variables
 - Modification de valeurs de tous les paramètres recensés.

EXPLOITATION

- **But :**

- ❑ Provoquer un changement de comportement de l'application
- ❑ Révélateur d'une vulnérabilité exploitable :
 - ❑ Affichage de messages d'erreur (erreur php, mysql, java...)
 - ❑ Comportement spécifique au type de vulnérabilité testée (ex. fenêtre `alert("XSS");`)
 - ❑ Comportement anormal de l'application (attaque logique).

EXPLOITATION : Injections SQL



#1 du TOP 10 de l'OWASP 2013