Fingerprinting d'applications Web

Nicolas Massaviol
Toucan System

nicolas.massaviol@
toucan-system.com

Agenda

- Fingerprinting
- Serveur Web
- Fichiers statiques
- Frameworks
- Questions

Fingerprinting

Fingerprinting ?

- Empreinte digitale
- Elément d'identification : traces, caractéristiques... (nmap OS)

Fingerprinting

Application Web ?

- Serveur Web
- Serveur d'application
- Framework
- BDD
- Code métier

Fingerprinting

Scanner de vulnérabilités (classique)
- Nessus
- Qualys
- ...

La version est souvent suffisante pour en déduire les vulns.

Fingerprinting = découvrir l'application et sa version

Agenda

- Comprendre les risques
- Serveur Web
- Fichiers statiques
- Frameworks
- Questions

Serveur Web

- Bannière

Apache 1.3.3 :

HTTP/1.1 200 OK
Server: Apache/1.3.3 (Unix) (Red Hat/Linux)

IIS 5.0 :

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0

Serveur Web

- Implémentation du protocole
  a) Ordre des champs des en-têtes

Apache :

HTTP/1.1 200 OK
Date: Sun, 15 Jun 2003 17:10: 49 GMT
Server: Apache/1.3.23

IIS :

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://iis.example.com/Default.htm
Date: Fri, 01 Jan 1999 20:13: 52 GMT

Serveur Web

b) Réponses à des requêtes invalides
HTTP/3.0, TOTO/1.1, ...

Outils :

- httprint, largement abandonné
- httprecon, vb :-(mais aussi nse :-)

Serveur Web : exemple

```
# nmap -p80 --script httprecon.nse www.owasp.org

Starting Nmap 5.21 ( http://nmap.org ) at 2011-03-10 16:13 CET
NSE: Script Scanning completed.
Nmap scan report for www.owasp.org (216.48.3.18)
Host is up (0.12s latency).
PORT    STATE SERVICE
80/tcp open  http
| httprecon: Pos  Implementation    Score  Hits
| 1    Apache 2.2.2     98     42
| 2    Apache 2.2.6     90     40
| 3    Apache 2.0.54    88     38
| 4    Apache 2.2.3     86     38
| 5    Apache 2.2.4     85     39
| 6    Apache 2.0.52    84     36
| 7    Apache 2.0.46    80     34
| 8    Apache 1.3.33    76     36
| 9    Apache 2.0.50    76     32
|_10   AOLserver 3.4.2  74     33

Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
```

Agenda

- Comprendre les risques
- Serveur Web
- Fichiers statiques
- Frameworks
- Questions

Fichiers statiques

Méthodes de fingerprinting existantes : regexp

- Maintenance difficile
- Pas résistant au hardening
- Facile à leurrer

Outils : Sedusa, Wappalyser, BackendInfo ...

Fichiers statiques

Idée générale du fingerprinting par fichiers statiques

- établir une liste de tous les fichiers statiques (*.js, *.css,...) ainsi que leur hash (md5, sha1, ...) de toutes les versions d'une application web

- Comparer suffisamment de fichiers sur l'application cible avec les hash de la liste précédente pour en déduire une application et une version

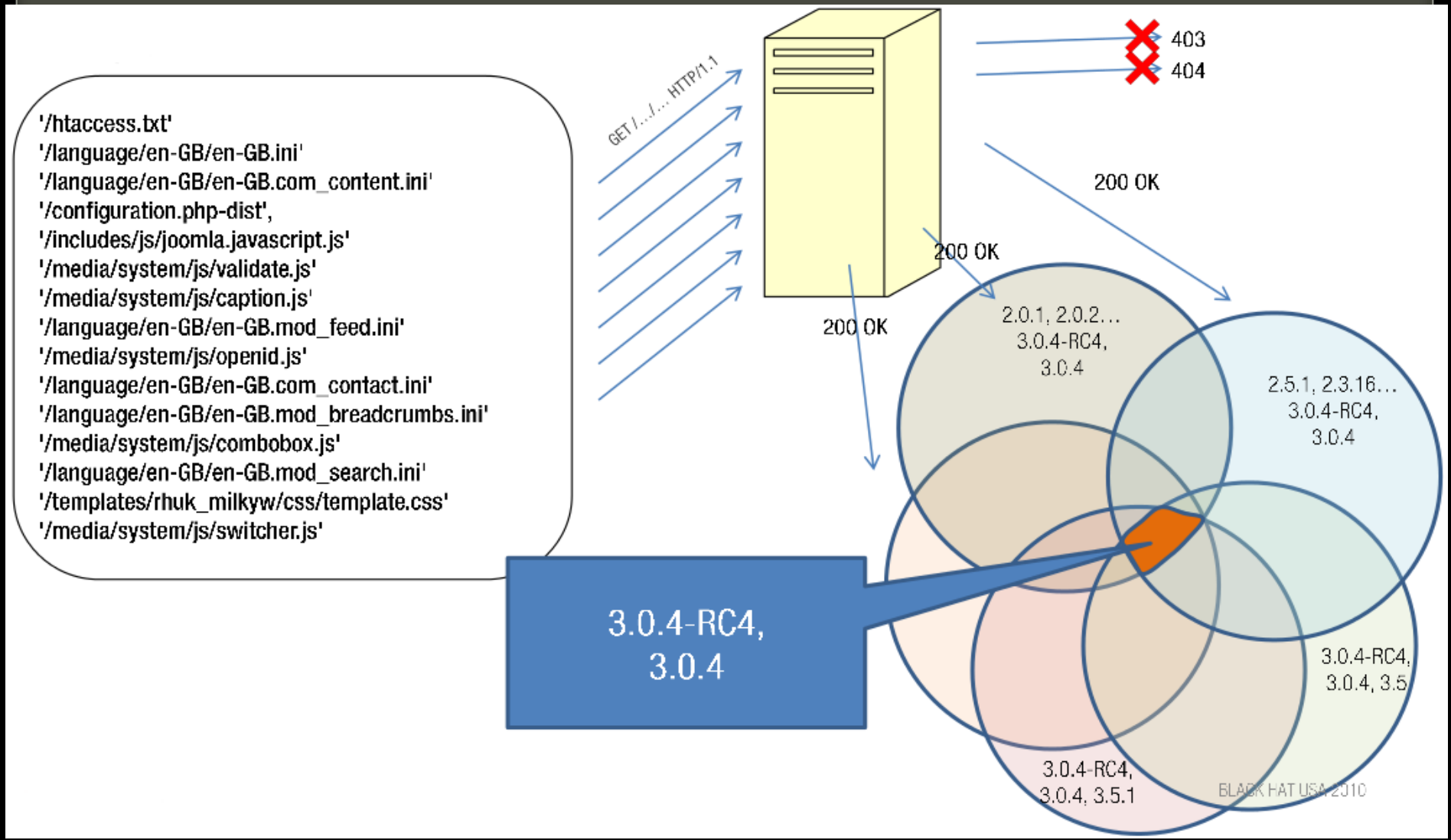
Fichiers statiques

Joomla-1.5.15

./language/index.html	dd5d02cc750d2855cf6f6c5bf5bea587
./language/pdf_fonts/index.html	1c7b413c3fa39d0fed40556d2658ac73
./language/en-GB/index.html	1c7b413c3fa39d0fed40556d2658ac73
./language/en-GB/en-GB.xml	b014471a7dd7abcb9480fc1d149b96ef
./templates/index.html	1c7b413c3fa39d0fed40556d2658ac73
./templates/rhuk_milkyway/index.html	1c7b413c3fa39d0fed40556d2658ac73
./templates/rhuk_milkyway/templateDetails.xml	56fb6df9bbdea9efcbc93d638cd070ba
./templates/rhuk_milkyway/html/index.html	1c7b413c3fa39d0fed40556d2658ac73
./templates/rhuk_milkyway/favicon.ico	63b982eddd64d44233baa25066db6bc1
./templates/rhuk_milkyway/css/index.html	1c7b413c3fa39d0fed40556d2658ac73

(…)

Fichiers statiques



Fichiers statiques

Outils : BlindElephant, WAFP, ...

- Pas résistant au changement de racine
- Fichiers statiques sur un autre domaine

Fichiers statiques

Deuxième approche : spider + comparaison

1) Récupération d'un mirroir (partiel)
2) Calcul des hash et comparaison
3) Récupération de l'application et de la version

Outils : WhatWeb, ...

Agenda

- Comprendre les risques
- Serveur Web
- Fichiers statiques
- Frameworks
- Questions

Frameworks

3 manières de faire une application Web :

- Tout à la main : old school
- Frameworks outils : symfony, cakephp, struts,..
- Frameworks clés en main (CMS) : Joomla, Drupal, ...

Frameworks

```
$ python BlindElephant.py -l
Currently configured web apps: 15
confluence with 0 plugins
drupal with 16 plugins
joomla with 0 plugins
liferay with 0 plugins
mediawiki with 0 plugins
moodle with 0 plugins
movabletype with 0 plugins
oscommerce with 0 plugins
phpbb with 0 plugins
phpmyadmin with 0 plugins
phpnuke with 0 plugins
spip with 0 plugins
tikiwiki with 0 plugins
twiki with 0 plugins
wordpress with 26 plugins
```

```
./wafp.rb -P
drupal
fluxbb
joomla
phpBB
phpmyadmin
punbb
serendipity
smf
typo3
wordpress
```

Frameworks

Objectif :

- Gérer les 2 approches
- Maintenance très simplifiée
- Détecter les frameworks outils

1) From scratch
2) BlindElephant :
   - Rapide
   - Efficace
   - Choix d'implémentations contraignants (BDD, checksums,...)
   - Intervention manuelle dans la maintenance
3) WAFP :
   - Pas de gestion des plugins
   - Moins efficace que BE mais maintenance très simplifiée
   - SQLite
4) WhatWeb :
   - Maintenance très complexe

Frameworks

Frameworks outils :

La plupart de temps, il existe des fichiers statiques ! Quel chemin final ?

Symfony :
$ find ./RELEASE_1_4_9/ -name *.js
./RELEASE_1_4_9/data/web/sf/sf_admin/js/collapse.js
./RELEASE_1_4_9/data/web/sf/sf_admin/js/double_list.js

Struts :
$ find ./struts-2.2.1.1/ -name *.js
./struts-2.2.1.1/src/plugins/dojo/src/main/resources/org/apache/struts2/static/dojo/dojo.js
(...)

Frameworks

```
$ ./wafp.rb http://www.articlegold.com
Collecting and fetching the files we need to identify the product ...

Identified Product: symfony (110.00 %)

 found the following matches (limited to 10):
+-----------------------------------------------------------+
 symfony-1.4.1                    52 / 52   (100.00%)
 symfony-1.4.8                    52 / 52   (100.00%)
 symfony-1.4.7                    52 / 52   (100.00%)
 symfony-1.4.9                    52 / 52   (100.00%)
 symfony-1.4.6                    52 / 52   (100.00%)
 symfony-1.4.2                    52 / 52   (100.00%)
 symfony-1.4.5                    52 / 52   (100.00%)
 symfony-1.4.3                    52 / 52   (100.00%)
 symfony-1.4.0                    52 / 52   (100.00%)
 symfony-1.4.4                    52 / 52   (100.00%)
+-----------------------------------------------------------+
 WAFP 0.01-26c3  - - - - - - - - -  http://mytty.org/wafp/
```

Frameworks

$ ./wafp.rb http://www.merchantpilot.com/

Collecting and fetching the files we need to identify the product ...

```
 found the following matches (limited to 10):
+-----------------------------------------------------------+
 symfony-1.2.1                          99 / 101  (98.02%)
 symfony-1.2.12                         99 / 101  (98.02%)
 symfony-1.2.6                          99 / 101  (98.02%)
 symfony-1.2.4                          99 / 101  (98.02%)
 symfony-1.2.9                          99 / 101  (98.02%)
 symfony-1.2.11                         99 / 101  (98.02%)
 symfony-1.2.3                          99 / 101  (98.02%)
 symfony-1.2.0                          99 / 101  (98.02%)
 symfony-1.2.7                          99 / 101  (98.02%)
 symfony-1.2.2                          99 / 101  (98.02%)
+-----------------------------------------------------------+
 WAFP 0.01-26c3  - - - - - - - - -  http://mytty.org/wafp/
```

Frameworks

```
$ ./wafp.rb http://www.thedailysave.com/
Collecting and fetching the files we need to identify the product ...

Identified Product: cakephp (20.00 %)
Collecting the files we need to fetch ...

 found the following matches (limited to 10):
+-----------------------------------------------------------+
 cakephp-1.3.4                          2 / 4    (50.00%)
 cakephp-1.3.0                          2 / 4    (50.00%)
 cakephp-1.3.7                          2 / 4    (50.00%)
 cakephp-1.3.1                          2 / 4    (50.00%)
 cakephp-1.3.6                          2 / 4    (50.00%)
 cakephp-1.3.2                          2 / 4    (50.00%)
 cakephp-1.3.5                          2 / 4    (50.00%)
 cakephp-1.3.3                          2 / 4    (50.00%)
 cakephp-1.2.0                          1 / 4    (25.00%)
 cakephp-1.2.4                          1 / 4    (25.00%)
+-----------------------------------------------------------+
 WAFP 0.01-26c3  - - - - - - - - -  http://mytty.org/wafp/
```

Frameworks

```
$ ./wafp.rb http://scratch.mit.edu
Collecting and fetching the files we need to identify the product ...

Identified Product: cakephp (20.00 %)
Collecting the files we need to fetch ...

 found the following matches (limited to 10):
+-----------------------------------------------------------+
 cakephp-1.2.0                    2 / 4    (50.00%)
 cakephp-1.2.8                    2 / 4    (50.00%)
 cakephp-1.2.1                    2 / 4    (50.00%)
 cakephp-1.2.7                    2 / 4    (50.00%)
 cakephp-1.2.2                    2 / 4    (50.00%)
 cakephp-1.2.6                    2 / 4    (50.00%)
 cakephp-1.2.3                    2 / 4    (50.00%)
 cakephp-1.2.5                    2 / 4    (50.00%)
 cakephp-1.2.4                    2 / 4    (50.00%)
 cakephp-1.2.9                    2 / 4    (50.00%)
+-----------------------------------------------------------+
 WAFP 0.01-26c3  - - - - - - - - -  http://myttv.org/wafp/
```

Frameworks

Et sinon ? Les « plugins » ! ou tout package de code communautaire développé pour pallier les « manques » du framework :

```
$ ls -l svn.symfony-project.com/plugins/ | wc -l
1028

sqlite> select * from tbl_product where name='symfony_plugins';
753 | symfony_plugins | XXX | 1299519173 | not used, yet.
sqlite> select count(*) from tbl_fprint where product_id = 753;
52221
```

Frameworks

En fait, peu intéressant tel quel :

- Nombre de fichiers,
- Pas/très peu de corrélation entre les plugins

Mais très intéressant avec le spidering !

Frameworks

Spidering avec HTTrack mais possible avec wget

Mirroir partiel créé en local puis comparaison avec les produits et versions stockés dans la base de données.
Détection du changement de racine éventuel

Frameworks

```
./wafp.rb --spider http://hackitoergosum.org
Collecting and fetching the files we need to identify the product ...
Fetching mirror
....
[...]
Found files in unusual location for wordpress-2.9-RC1 :
./wp-includes/images/crystal/document.png.pagespeed.ce.5ter9w_jZT.png should be at
./wp-includes/images/crystal/document.png
Found files in unusual location for wordpress-2.9-beta-1 :
./wp-includes/images/crystal/document.png.pagespeed.ce.5ter9w_jZT.png should be at
./wp-includes/images/crystal/document.png
Found files in unusual location for wordpress-2.9-beta-2 :
./wp-includes/images/crystal/document.png.pagespeed.ce.5ter9w_jZT.png should be at
./wp-includes/images/crystal/document.png
Found files in unusual location for wordpress-2.9.1-beta1 :
./wp-includes/images/crystal/document.png.pagespeed.ce.5ter9w_jZT.png should be at
./wp-includes/images/crystal/document.png
```

Limites

Zend
Mises à jour incomplètes
Hardening trivial : peut être intégré au déploiement par défaut des frameworks

Questions ?