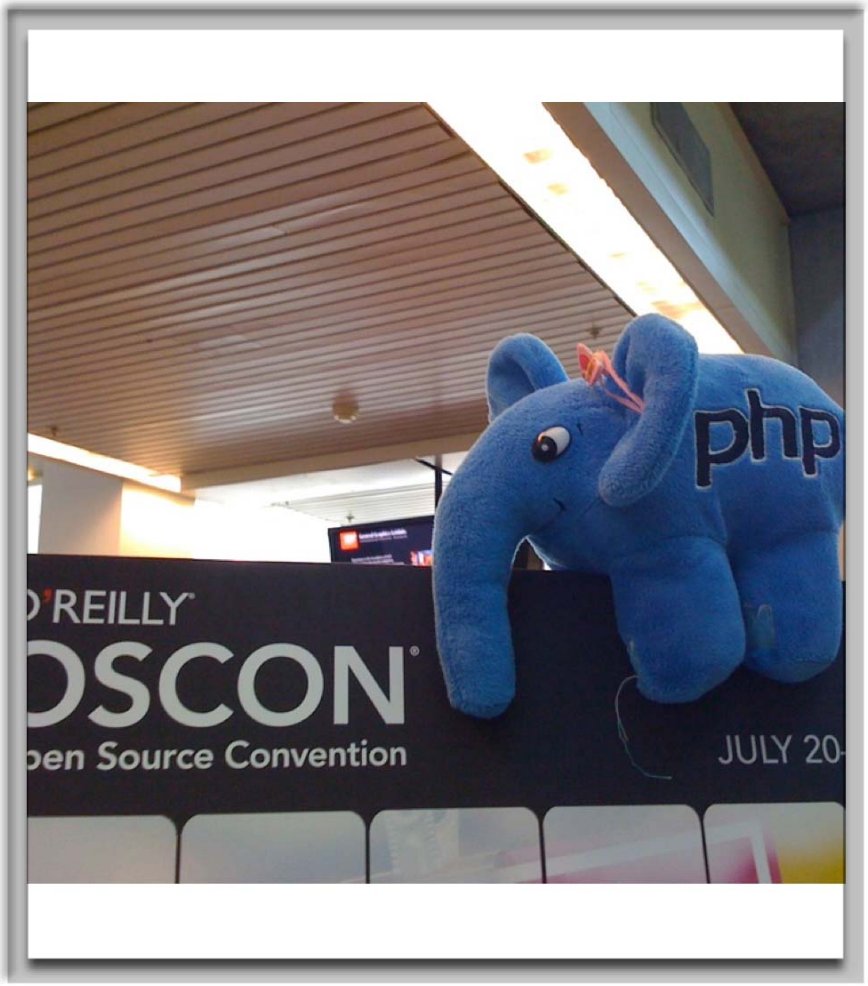
PHP code audits

OSCON 2009

San José, CA, USA

July 21th 2009



Agenda

Workshop presentation

Black box audit

Source code audit

Who speaks?

Philippe Gamache

Parler Haut, Interagir Librement : Web development, security audit, training

info@ph-il.ca

@SecureSymfony

Who speaks?

Damien Seguy

Alter Way Consulting :
Open sources expert services

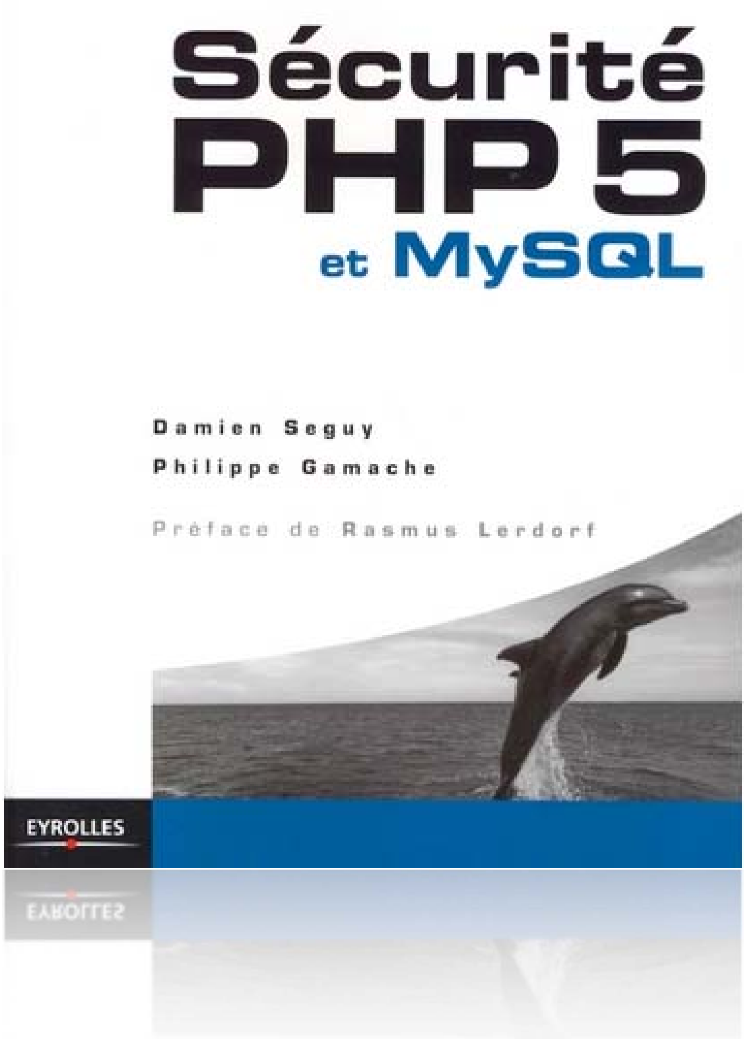
Father of the Elephpant

Calendar maker

damien.seguy@alterway.fr

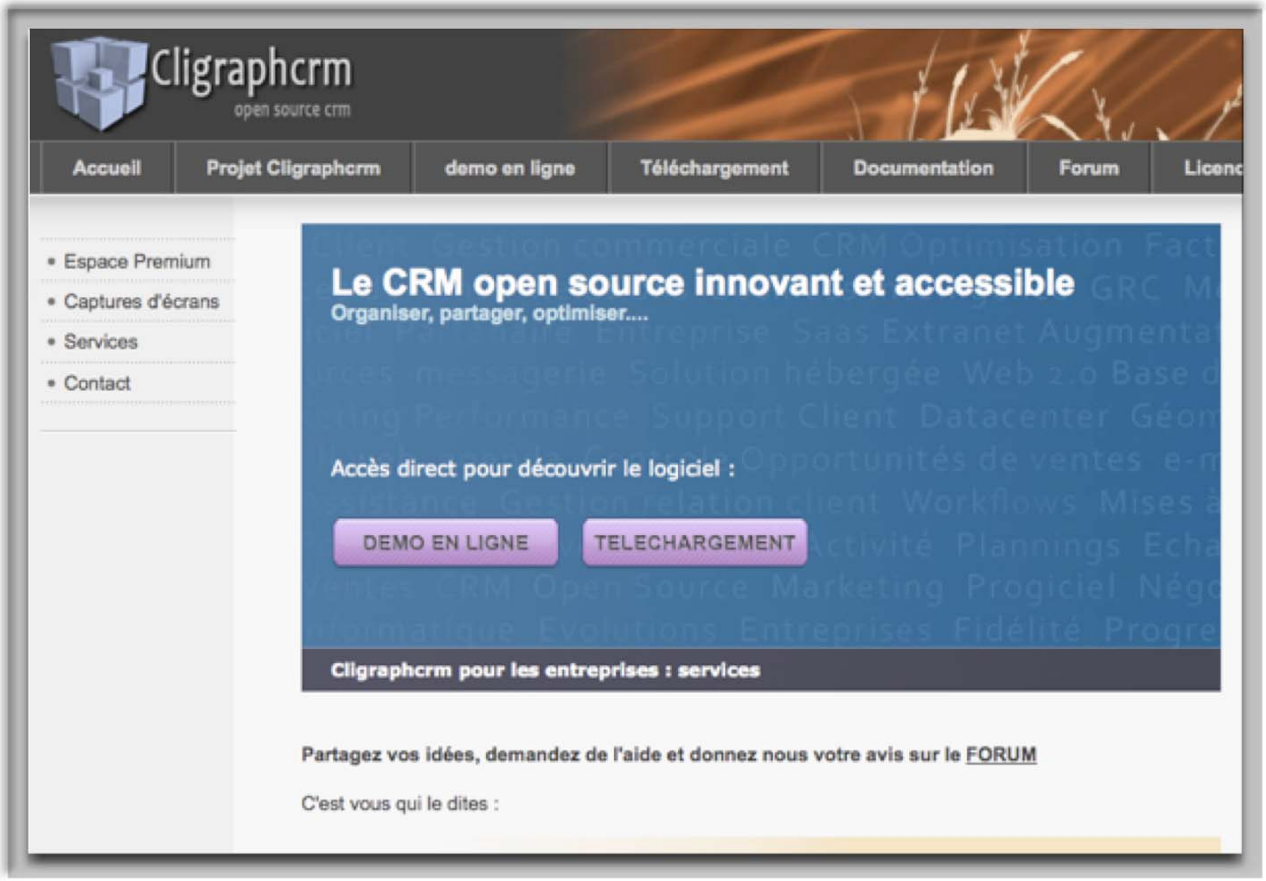
Security Book

- New 2009 edition
- Comprehensive review of security system for MySQL, PHP, etc.
- Published in French
  - Planning translation



The application

http://www.cligraphcrm.com/



Le CRM open source innovant et accessible

Organiser, partager, optimiser....

Accès direct pour découvrir le logiciel :

Cligraphcrm pour les entreprises : services

Partagez vos idées, demandez de l'aide et donnez nous votre avis sur le FORUM

C'est vous qui le dites :

Full audit synopsis

Identification of the audit goals

Interview with the dev teams

Black box testing

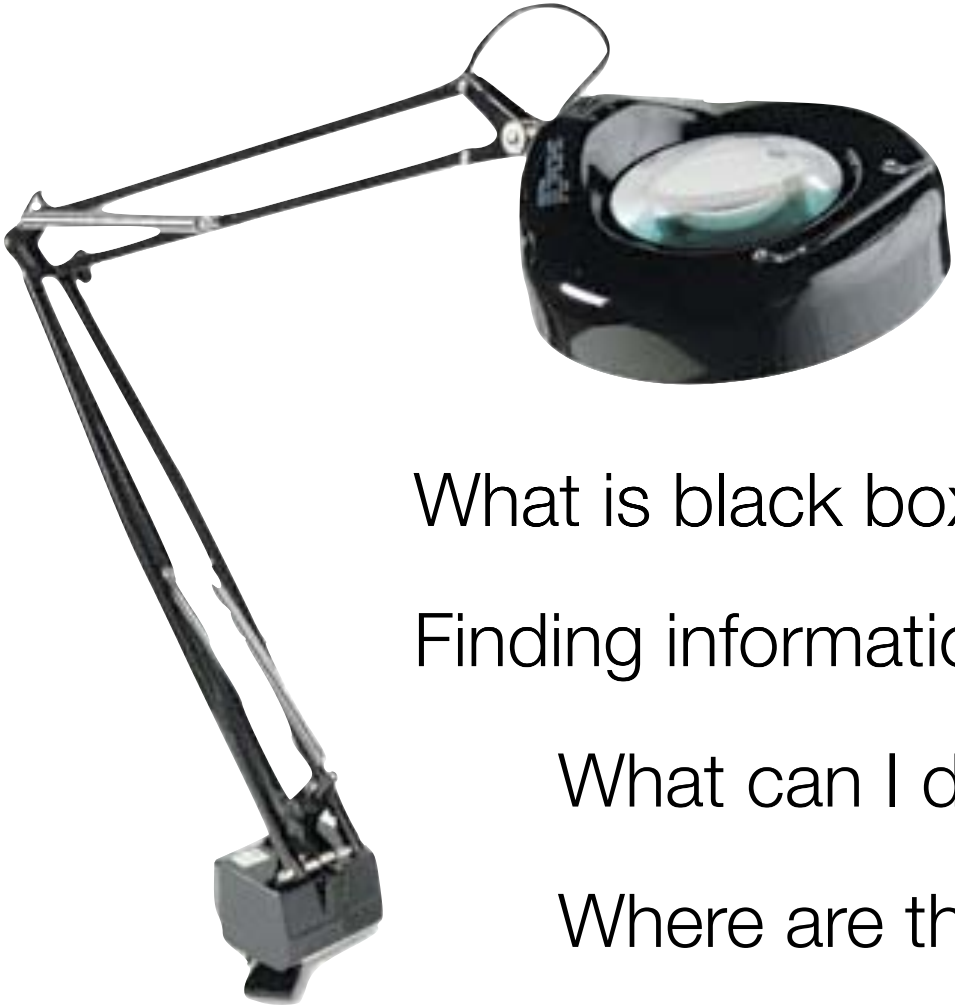
Open Code audit

Report

Yes,
we take
questions

Black box testing

Black box testing



What is black box testing?

Finding information

- What can I do with this application?
- Where are the most popular entry points?

Black box testing

- Look for vulnerabilities
  - Use different tools and technics
    - Automatic scanners
    - By hand
    - Fuzzing tools
    - Scenarios
  - How do I use to my advantage?

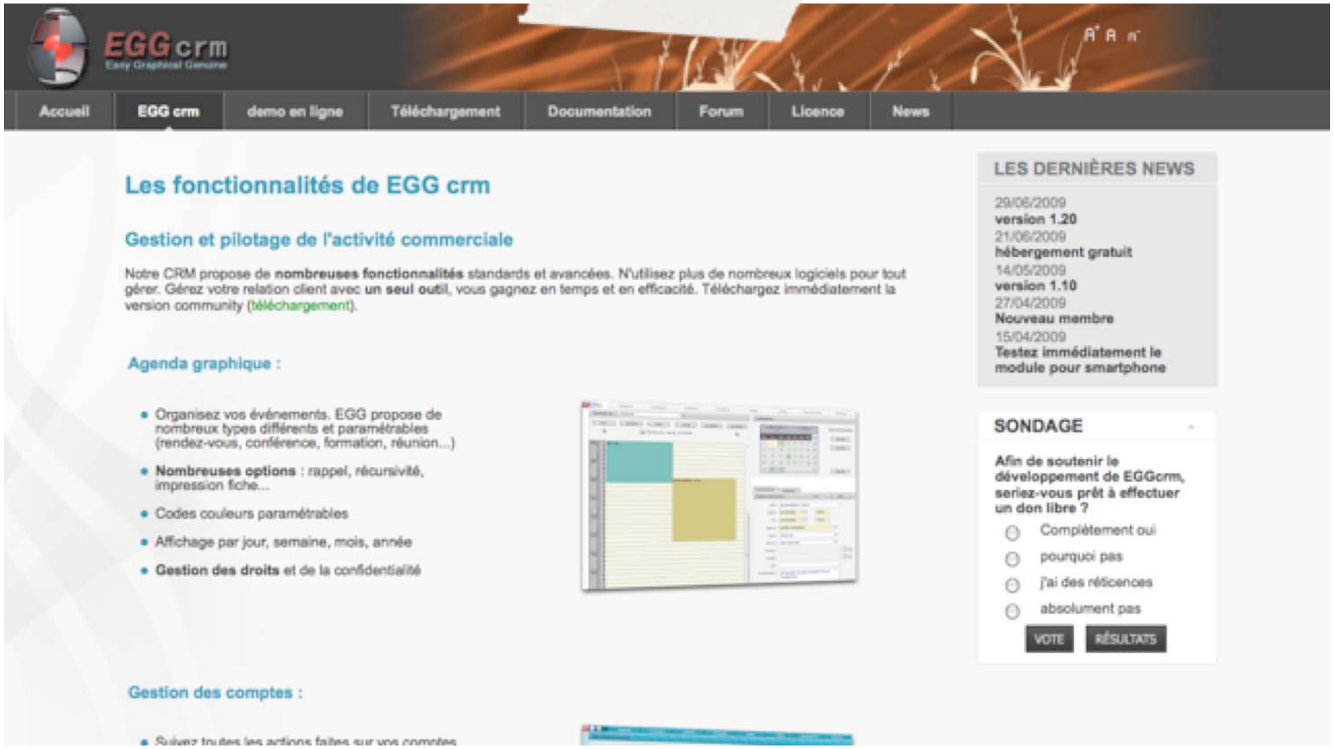
Black box testing

- Strike
  - Attacking a vulnerability with a specific purpose

Find Information

Look at the application web site

Features



Les fonctionnalités de EGG crm

Gestion et pilotage de l'activité commerciale

Notre CRM propose de **nombreuses fonctionnalités** standards et avancées. N'utilisez plus de nombreux logiciels pour tout gérer. Gérez votre relation client avec **un seul outil**, vous gagnez en temps et en efficacité. Téléchargez immédiatement la version community (téléchargement).

Agenda graphique :

- Organisez vos événements. EGG propose de nombreux types différents et paramétrables (rendez-vous, conférence, formation, réunion...)
- **Nombreuses options** : rappel, récursivité, impression fiche...
- Codes couleurs paramétrables
- Affichage par jour, semaine, mois, année
- **Gestion des droits** et de la confidentialité

Gestion des comptes :

- Suivez toutes les actions faites sur vos comptes

LES DERNIÈRES NEWS

29/06/2009
version 1.20
21/06/2009
hébergement gratuit
14/05/2009
version 1.10
27/04/2009
Nouveau membre
15/04/2009
Testez immédiatement le module pour smartphone

SONDAGE

Afin de soutenir le développement de EGGcrm, seriez-vous prêt à effectuer un don libre ?

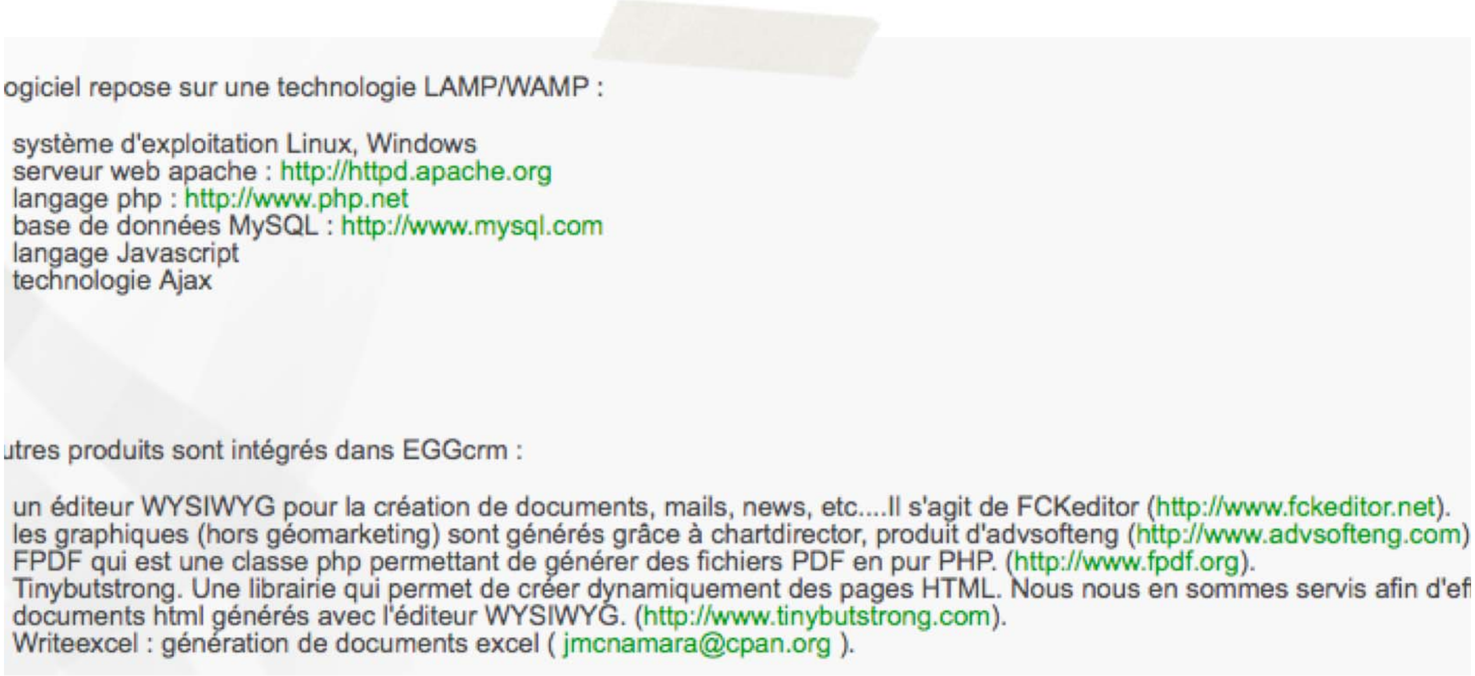
○ Complètement oui
○ pourquoi pas
○ j'ai des réticences
○ absolument pas

VOTE RÉSULTATS

Find Information

Look at the application web site

Technology



ogiciel repose sur une technologie LAMP/WAMP :

système d'exploitation Linux, Windows
serveur web apache : http://httpd.apache.org
langage php : http://www.php.net
base de données MySQL : http://www.mysql.com
langage Javascript
technologie Ajax

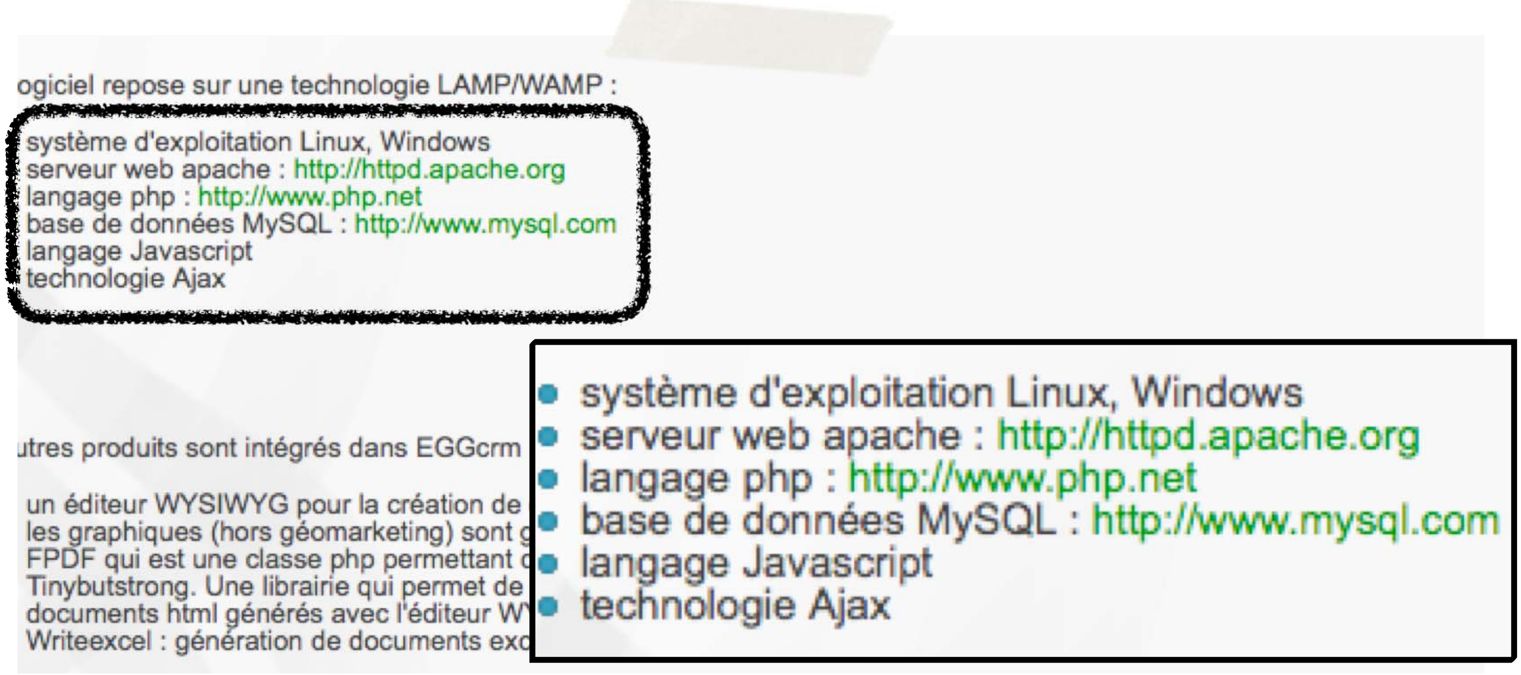
utres produits sont intégrés dans EGGcrm :

un éditeur WYSIWYG pour la création de documents, mails, news, etc....Il s'agit de FCKeditor (http://www.fckeditor.net).
les graphiques (hors géomarketing) sont générés grâce à chartdirector, produit d'advsofteng (http://www.advsofteng.com)
FPDF qui est une classe php permettant de générer des fichiers PDF en pur PHP. (http://www.fpdf.org).
Tinybutstrong. Une librairie qui permet de créer dynamiquement des pages HTML. Nous nous en sommes servis afin d'ef
documents html générés avec l'éditeur WYSIWYG. (http://www.tinybutstrong.com).
Writeexcel : génération de documents excel (jmcnamara@cpan.org).

Find Information

Look at the application web site

Technology



ogiciel repose sur une technologie LAMP/WAMP :

système d'exploitation Linux, Windows
serveur web apache : http://httpd.apache.org
langage php : http://www.php.net
base de données MySQL : http://www.mysql.com
langage Javascript
technologie Ajax

utres produits sont intégrés dans EGGcrm

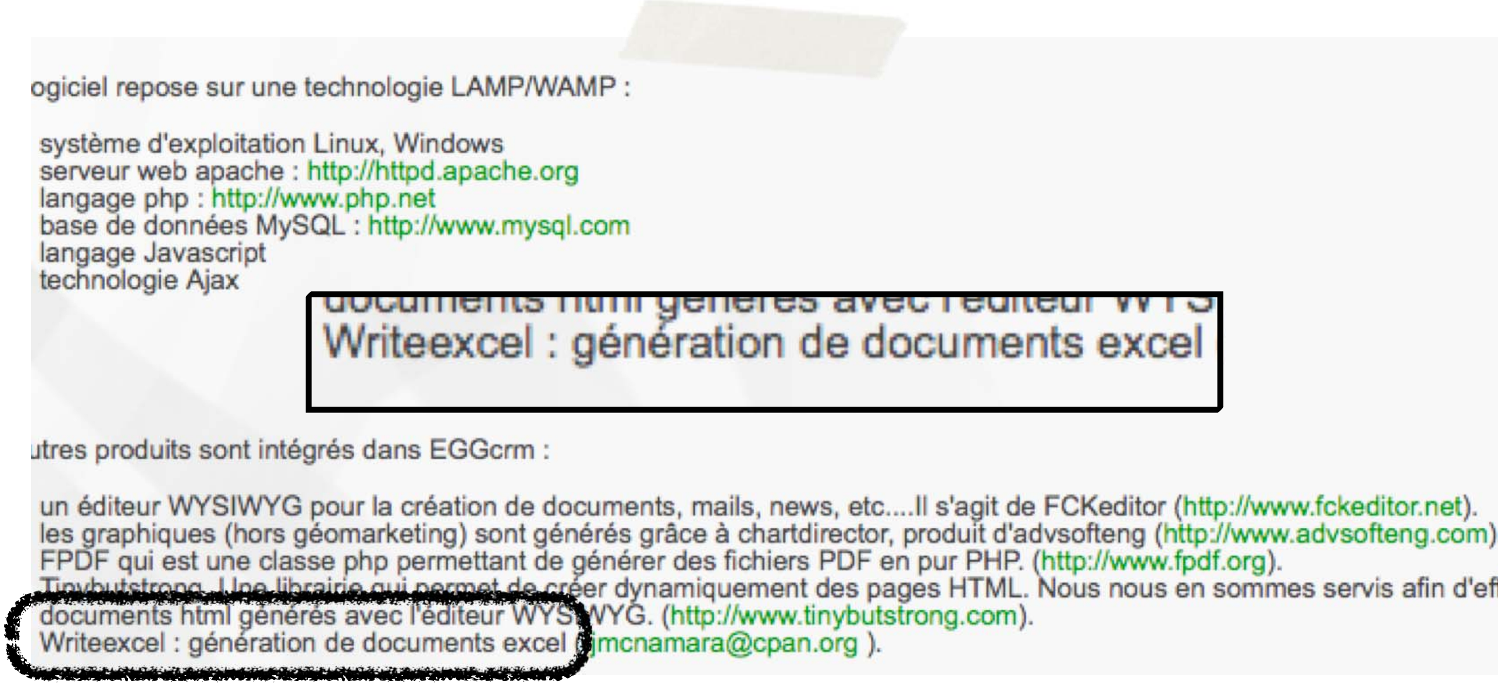
un éditeur WYSIWYG pour la création de
les graphiques (hors géomarketing) sont g
FPDF qui est une classe php permettant d
Tinybutstrong. Une librairie qui permet de
documents html générés avec l'éditeur W
Writeexcel : génération de documents exc

- système d'exploitation Linux, Windows
- serveur web apache : http://httpd.apache.org
- langage php : http://www.php.net
- base de données MySQL : http://www.mysql.com
- langage Javascript
- technologie Ajax

Find Information

Look at the application web site

Technology



ogiciel repose sur une technologie LAMP/WAMP :

système d'exploitation Linux, Windows
serveur web apache : http://httpd.apache.org
langage php : http://www.php.net
base de données MySQL : http://www.mysql.com
langage Javascript
technologie Ajax

documents html générés avec l'éditeur WYS
Writeexcel : génération de documents excel

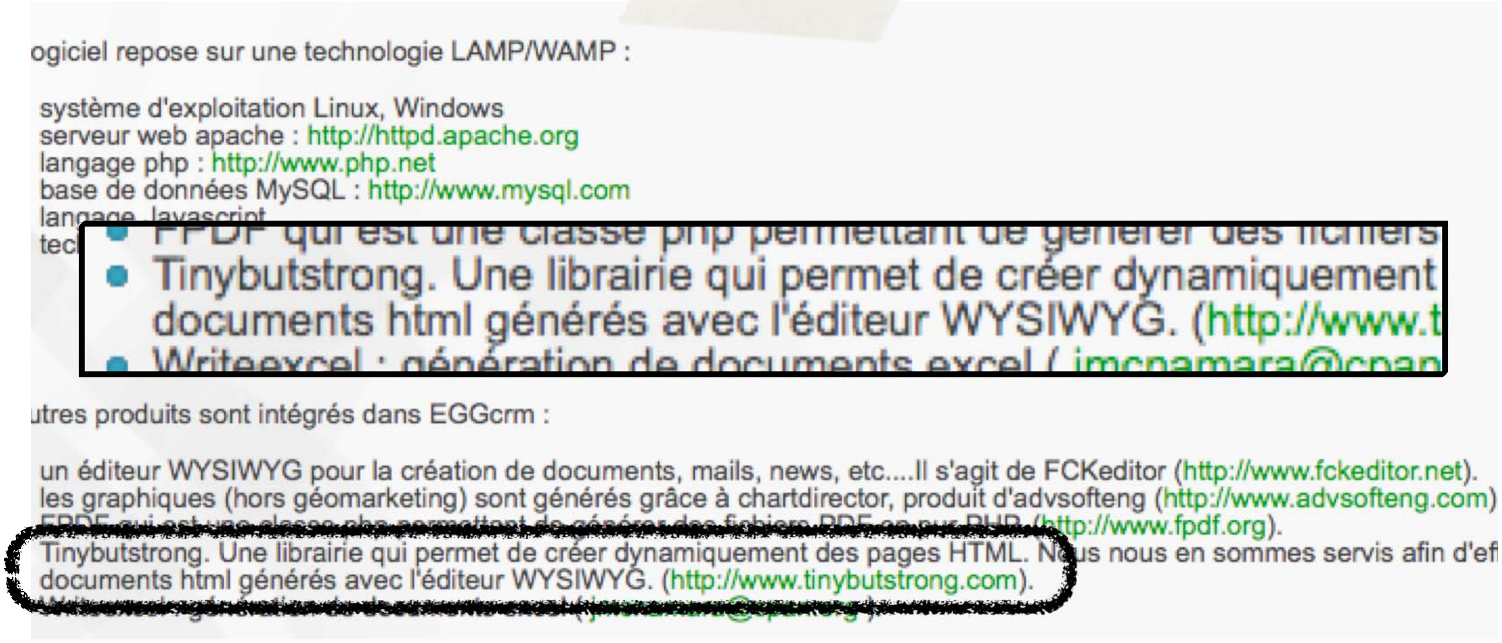
utres produits sont intégrés dans EGGcrm :

un éditeur WYSIWYG pour la création de documents, mails, news, etc....Il s'agit de FCKeditor (http://www.fckeditor.net).
les graphiques (hors géomarketing) sont générés grâce à chartdirector, produit d'advsofteng (http://www.advsofteng.com)
FPDF qui est une classe php permettant de générer des fichiers PDF en pur PHP. (http://www.fpdf.org).
Tinybutstrong. Une librairie qui permet de créer dynamiquement des pages HTML. Nous nous en sommes servis afin d'ef
documents html générés avec l'éditeur WYSIWYG. (http://www.tinybutstrong.com).
Writeexcel : génération de documents excel (jmcnamara@cpan.org).

Find Information

Look at the application web site

Technology



ogiciel repose sur une technologie LAMP/WAMP :

système d'exploitation Linux, Windows
serveur web apache : http://httpd.apache.org
langage php : http://www.php.net
base de données MySQL : http://www.mysql.com
langage Javascript
tec

- FPDF qui est une classe php permettant de générer des fichiers
- Tinybutstrong. Une librairie qui permet de créer dynamiquement
  documents html générés avec l'éditeur WYSIWYG. (http://www.t
- Writeexcel : génération de documents excel (jmcnamara@cpan

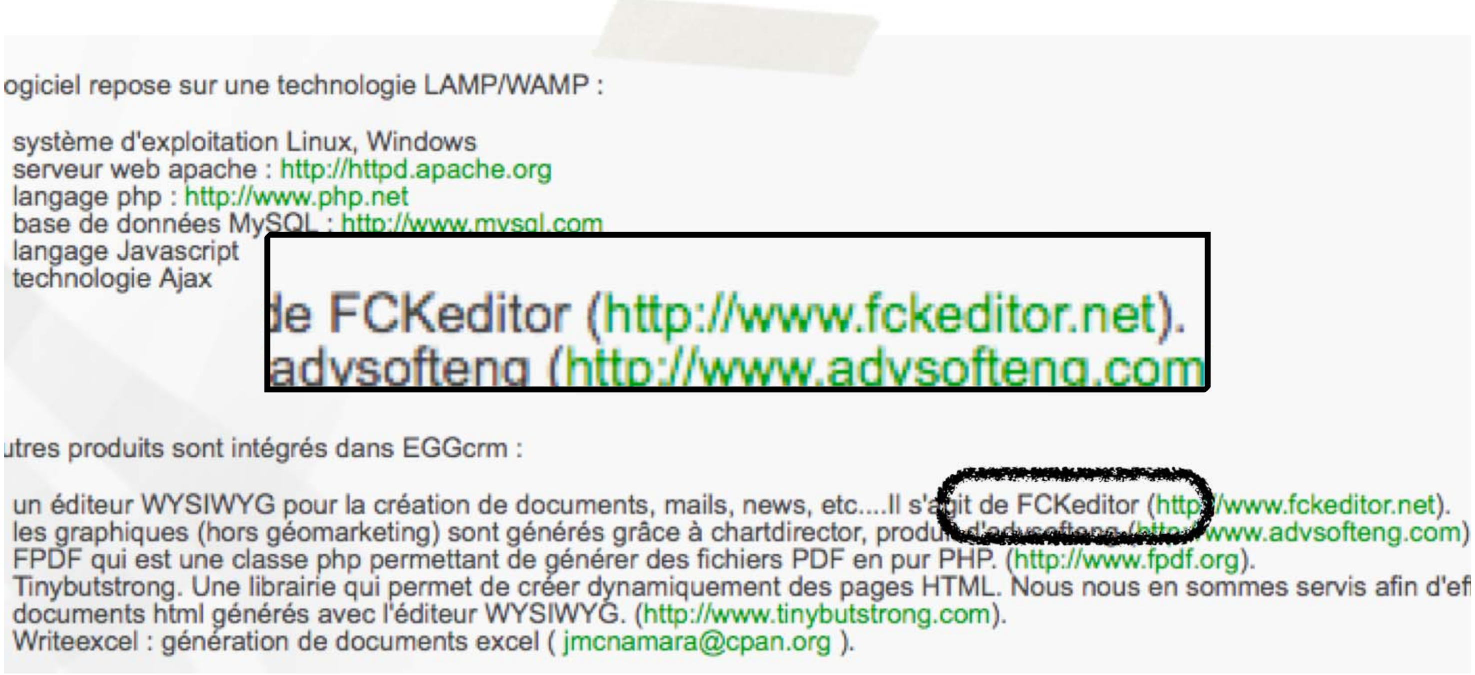
utres produits sont intégrés dans EGGcrm :

un éditeur WYSIWYG pour la création de documents, mails, news, etc....Il s'agit de FCKeditor (http://www.fckeditor.net).
les graphiques (hors géomarketing) sont générés grâce à chartdirector, produit d'advsofteng (http://www.advsofteng.com)
FPDF qui est une classe php permettant de générer des fichiers PDF en pur PHP (http://www.fpdf.org).
Tinybutstrong. Une librairie qui permet de créer dynamiquement des pages HTML. Nous nous en sommes servis afin d'ef
documents html générés avec l'éditeur WYSIWYG. (http://www.tinybutstrong.com).
Writeexcel : génération de documents excel (jmcnamara@cpan.org).

Find Information

Look at the application web site

Technology



ogiciel repose sur une technologie LAMP/WAMP :

système d'exploitation Linux, Windows
serveur web apache : http://httpd.apache.org
langage php : http://www.php.net
base de données MySQL : http://www.mysql.com
langage Javascript
technologie Ajax

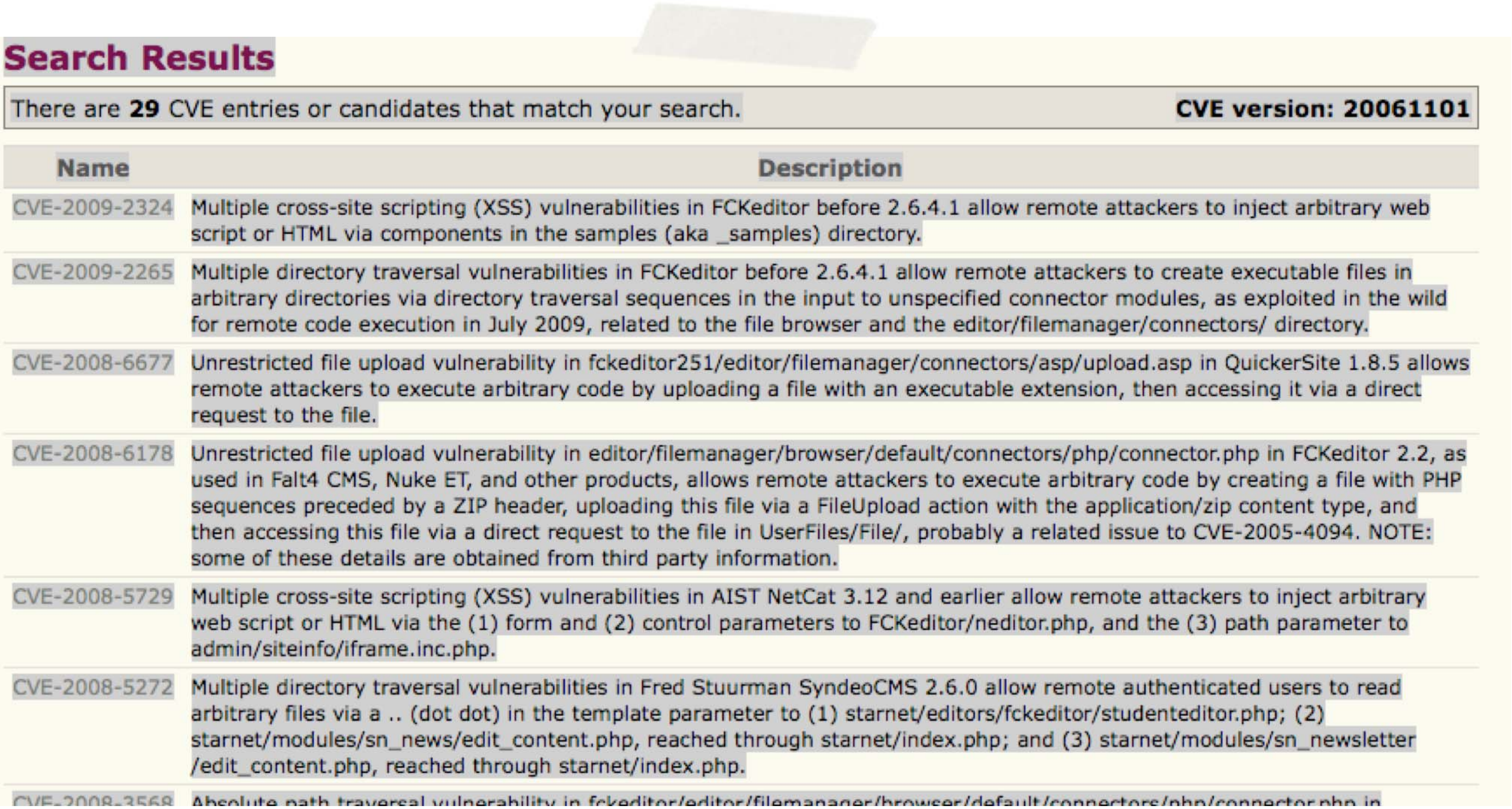
de FCKeditor (http://www.fckeditor.net).
advsofteng (http://www.advsofteng.com

utres produits sont intégrés dans EGGcrm :

un éditeur WYSIWYG pour la création de documents, mails, news, etc....Il s'agit de FCKeditor (http://www.fckeditor.net).
les graphiques (hors géomarketing) sont générés grâce à chartdirector, produit d'advsofteng (http://www.advsofteng.com)
FPDF qui est une classe php permettant de générer des fichiers PDF en pur PHP. (http://www.fpdf.org).
Tinybutstrong. Une librairie qui permet de créer dynamiquement des pages HTML. Nous nous en sommes servis afin d'ef
documents html générés avec l'éditeur WYSIWYG. (http://www.tinybutstrong.com).
Writeexcel : génération de documents excel (jmcnamara@cpan.org).

18

Where did I hear about this?



Search Results

There are **29** CVE entries or candidates that match your search. **CVE version: 20061101**

Name	Description
CVE-2009-2324	Multiple cross-site scripting (XSS) vulnerabilities in FCKeditor before 2.6.4.1 allow remote attackers to inject arbitrary web script or HTML via components in the samples (aka _samples) directory.
CVE-2009-2265	Multiple directory traversal vulnerabilities in FCKeditor before 2.6.4.1 allow remote attackers to create executable files in arbitrary directories via directory traversal sequences in the input to unspecified connector modules, as exploited in the wild for remote code execution in July 2009, related to the file browser and the editor/filemanager/connectors/ directory.
CVE-2008-6677	Unrestricted file upload vulnerability in fckeditor251/editor/filemanager/connectors/asp/upload.asp in QuickerSite 1.8.5 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file.
CVE-2008-6178	Unrestricted file upload vulnerability in editor/filemanager/browser/default/connectors/php/connector.php in FCKeditor 2.2, as used in Falt4 CMS, Nuke ET, and other products, allows remote attackers to execute arbitrary code by creating a file with PHP sequences preceded by a ZIP header, uploading this file via a FileUpload action with the application/zip content type, and then accessing this file via a direct request to the file in UserFiles/File/, probably a related issue to CVE-2005-4094. NOTE: some of these details are obtained from third party information.
CVE-2008-5729	Multiple cross-site scripting (XSS) vulnerabilities in AIST NetCat 3.12 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) form and (2) control parameters to FCKeditor/neditor.php, and the (3) path parameter to admin/siteinfo/iframe.inc.php.
CVE-2008-5272	Multiple directory traversal vulnerabilities in Fred Stuurman SyndeoCMS 2.6.0 allow remote authenticated users to read arbitrary files via a .. (dot dot) in the template parameter to (1) starnet/editors/fckeditor/studenteditor.php; (2) starnet/modules/sn_news/edit_content.php, reached through starnet/index.php; and (3) starnet/modules/sn_newsletter /edit_content.php, reached through starnet/index.php.
CVE-2008-3568	Absolute path traversal vulnerability in fckeditor/editor/filemanager/browser/default/connectors/php/connector.php in

Find vulnerabilities

We look in Common Vulnerabilities and Exposures

Also in bugtrack, xssed.com, etc...

We could have look in Google, Bing, etc...

No published vulnerabilities for cliGraph

Find Information

```
HTTP/1.x 200 OK
Date: Mon, 20 Jul 2009 17:29:25 GMT
Server: Apache/2.2.3 (Debian) PHP/5.2.0-8+etch11 mod_ssl/2.2.3
OpenSSL/0.9.8c
X-Powered-By: PHP/5.2.0-8+etch11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 586
Content-Type: text/html; charset=UTF-8
X-Cache: MISS from Colossus
Connection: close
```

- HTTP headers
  - curl, wget, Firefox
  - Rex Swain's HTTP Viewer

Typical files

Usual directories

includes, include, inc, com,

classes, lib, library

admin, adm, administrator,

tmp, TMP, ext, var

data, db, conf, config

uploads, install,

Typical files

.phps, .inc, .class,

xml, ini, yaml, cfg

Apache Alias : /icons/

robots.txt

Security dilema

robots.txt

```
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Disallow: /xmlrpc/
```

External testing

Get the list of the scripts (find .)

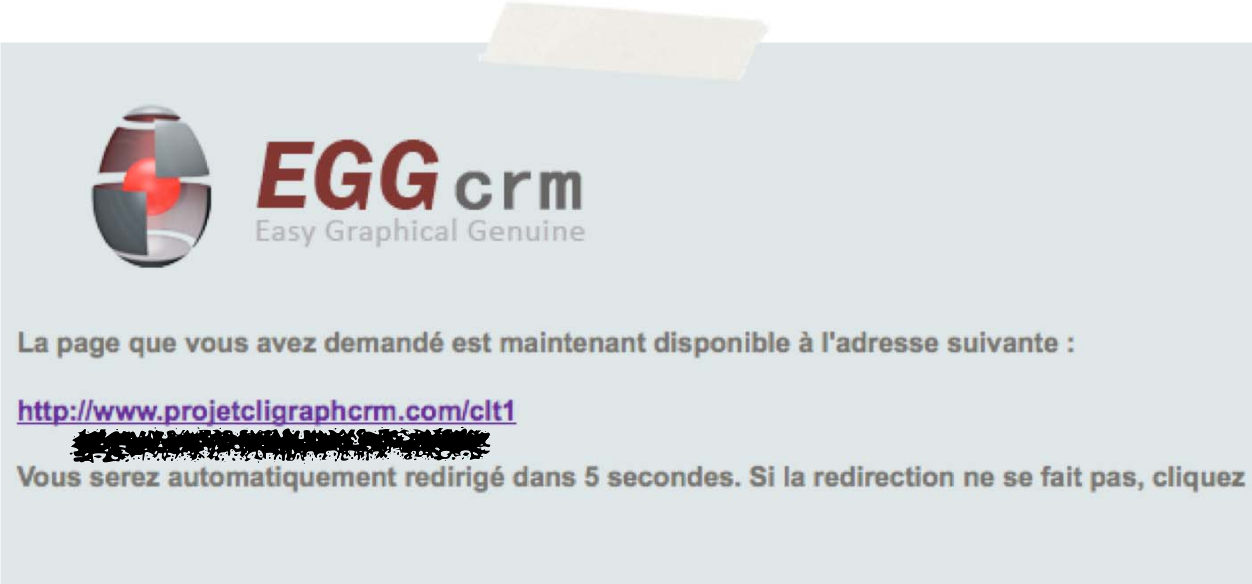
Turn that into URLs

Fetch them directly on the web site

Study what’s coming back

Maybe you gonna need to install it yourself

Typical files



La page que vous avez demandé est maintenant disponible à l'adresse suivante :

http://www.projetcligraphcrm.com/clt1

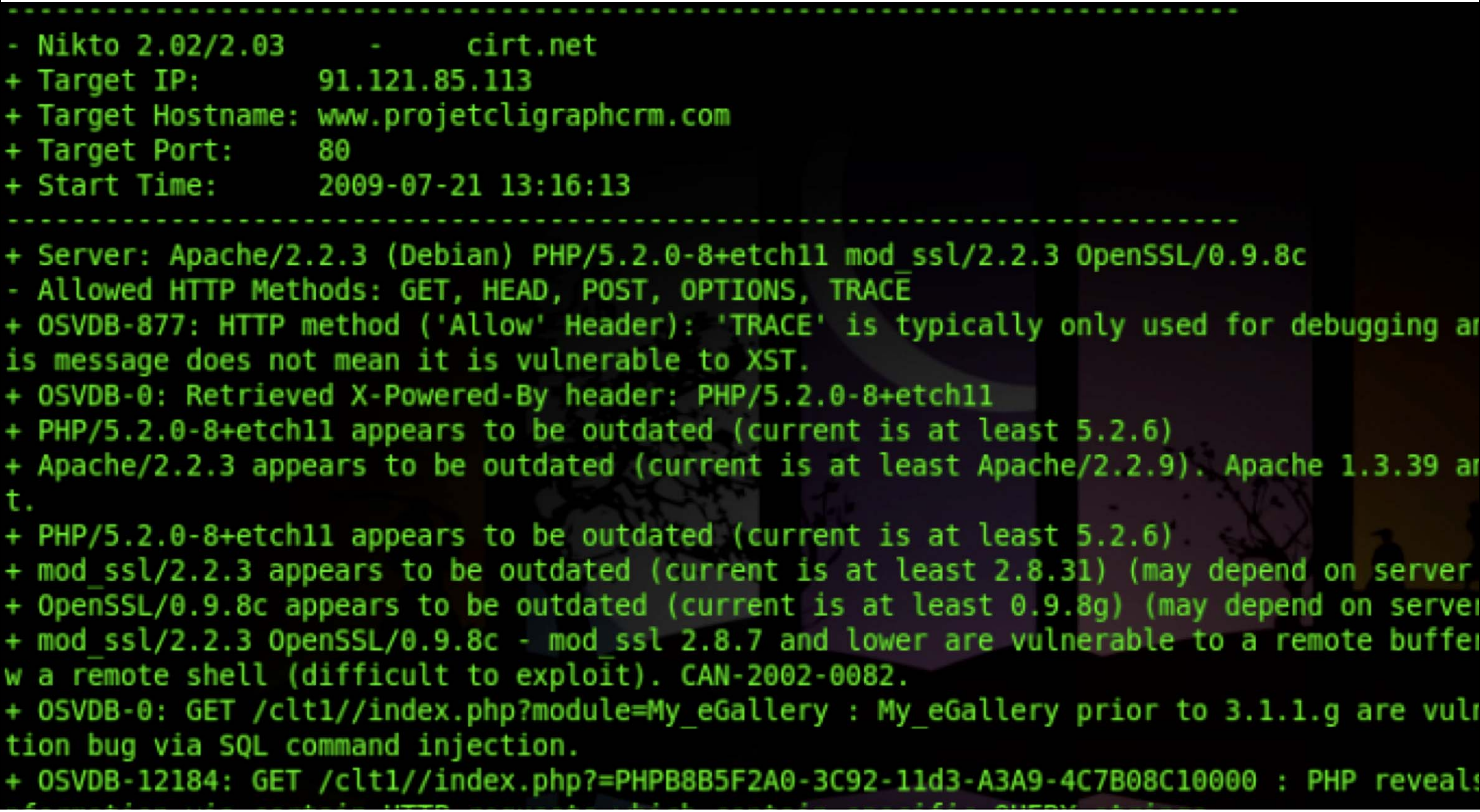
[redacted]

Vous serez automatiquement redirigé dans 5 secondes. Si la redirection ne se fait pas, cliquez

- https
- 404 and 5xx pages
- Blank page
  - Bad code without error posting

Automatic scanners

Nikto http://www.cirt.net/



```
---------------------------------------------------------------------------
- Nikto 2.02/2.03      -     cirt.net
+ Target IP:          91.121.85.113
+ Target Hostname:    www.projetcligraphcrm.com
+ Target Port:        80
+ Start Time:         2009-07-21 13:16:13
---------------------------------------------------------------------------
+ Server: Apache/2.2.3 (Debian) PHP/5.2.0-8+etch11 mod_ssl/2.2.3 OpenSSL/0.9.8c
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging ar
is message does not mean it is vulnerable to XST.
+ OSVDB-0: Retrieved X-Powered-By header: PHP/5.2.0-8+etch11
+ PHP/5.2.0-8+etch11 appears to be outdated (current is at least 5.2.6)
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.9). Apache 1.3.39 ar
t.
+ PHP/5.2.0-8+etch11 appears to be outdated (current is at least 5.2.6)
+ mod_ssl/2.2.3 appears to be outdated (current is at least 2.8.31) (may depend on server
+ OpenSSL/0.9.8c appears to be outdated (current is at least 0.9.8g) (may depend on serve
+ mod_ssl/2.2.3 OpenSSL/0.9.8c - mod_ssl 2.8.7 and lower are vulnerable to a remote buffe
w a remote shell (difficult to exploit). CAN-2002-0082.
+ OSVDB-0: GET /clt1//index.php?module=My_eGallery : My_eGallery prior to 3.1.1.g are vul
tion bug via SQL command injection.
+ OSVDB-12184: GET /clt1//index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 : PHP reveals
```

Find vulnerabilities

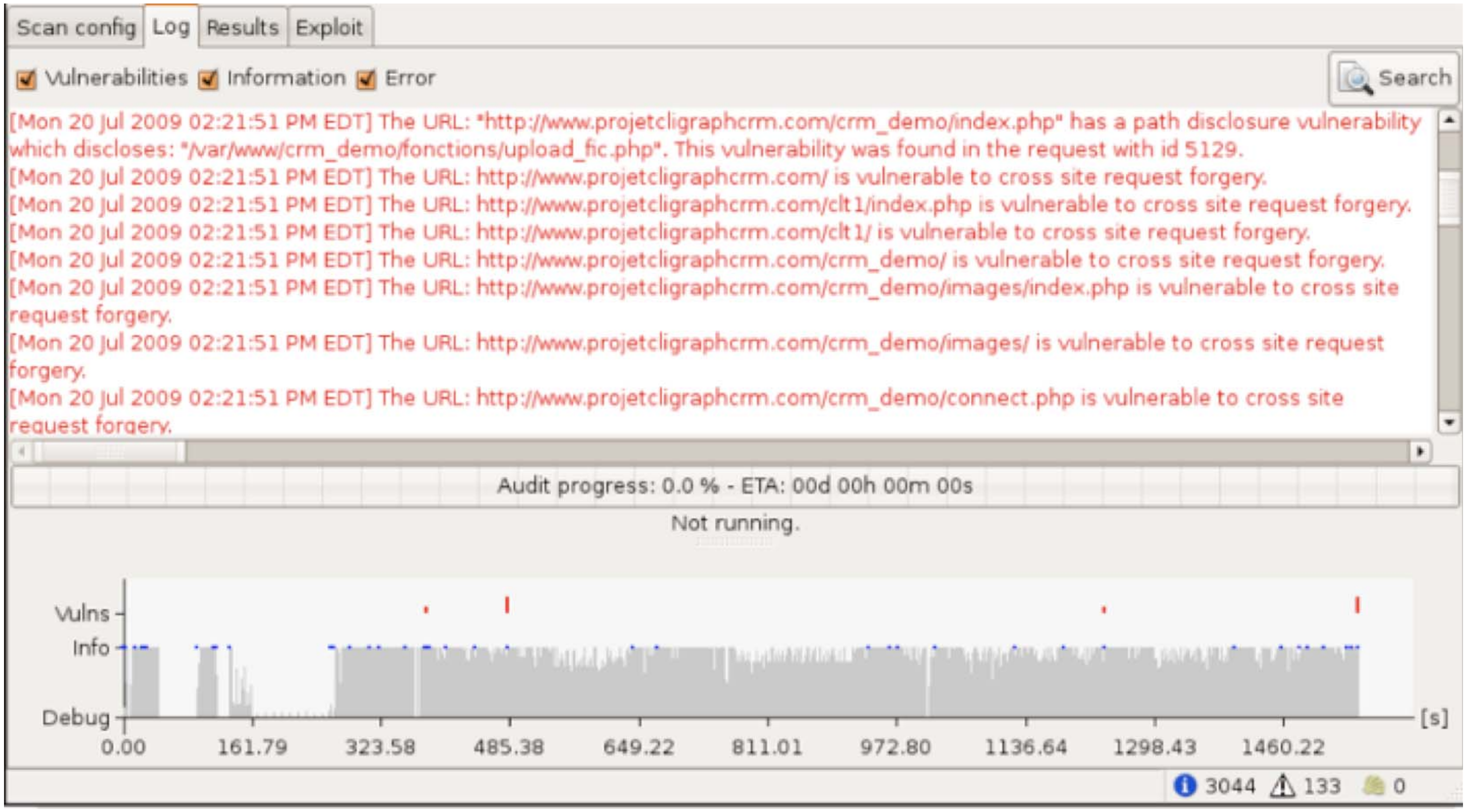
What to look for ?

- XSS
- CSRF
- Injections
- Files overwrite

Automatic scanners

Web Application Attack and Audit Framework (W3AF)

http://w3af.sourceforge.net/



```
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: "http://www.projetcligraphcrm.com/crm_demo/index.php" has a path disclosure vulnerability
which discloses: "/var/www/crm_demo/fonctions/upload_fic.php". This vulnerability was found in the request with id 5129.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/ is vulnerable to cross site request forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/clt1/index.php is vulnerable to cross site request forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/clt1/ is vulnerable to cross site request forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/crm_demo/ is vulnerable to cross site request forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/crm_demo/images/index.php is vulnerable to cross site
request forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/crm_demo/images/ is vulnerable to cross site request
forgery.
[Mon 20 Jul 2009 02:21:51 PM EDT] The URL: http://www.projetcligraphcrm.com/crm_demo/connect.php is vulnerable to cross site
request forgery.
```

Audit progress: 0.0 % - ETA: 00d 00h 00m 00s

Not running.

Manual tools

- Firefox
  - Access Me
  - Firebug
  - SQL Inject Me
  - Web Developer
  - XSS Me Data

Manual tools

Arrays

```
c[]=1
```

Surplus variables

```
debug=1, task=view
```

Missing variables

Manual tools

```
action/facture_fiche.php?
exp_typedoc=facture&exp_id=
2009N000196&exp_formdoc=pdf
```

```
action/facture_fiche.php?
exp_typedoc=facture&exp_id=2009
N000196&exp_formdoc=fiche
```

```
Fatal error: Cannot redeclare fct_redimension_img()
(previously declared in /var/www/crm_demo/fonctions/
fonction_img.php:68) in /var/www/crm_demo/fonctions/
fonction_img.php on line 134
```

Fuzzing

Test by random value

Stress forms

Database

All characters from \0 to \x255

All Unicode characters

The numbers 1, 0, -1, 0.99, extreme, infinite

Fuzzing

- Strings
    - Long
    - Short
- Dictionaries of values
    - of vulnerabilities
- GET, POST, COOKIE

Fuzzing

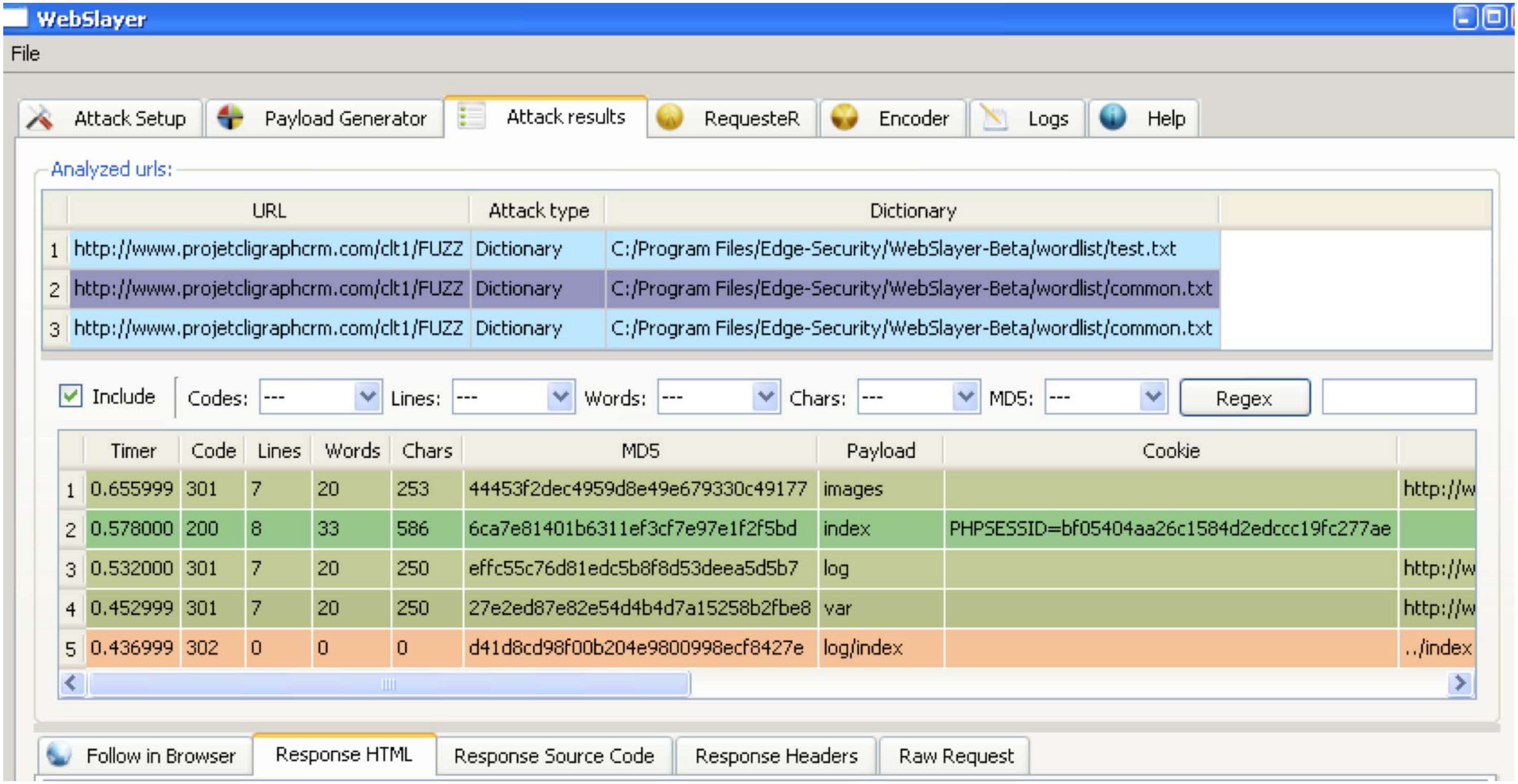
Wfuzz

http://www.edge-security.com/wfuzz.php

WebSlayer

http://www.edge-security.com/webslayer.php

Exemple Fuzzing



	URL	Attack type	Dictionary
1	http://www.projetcligraphcrm.com/clt1/FUZZ	Dictionary	C:/Program Files/Edge-Security/WebSlayer-Beta/wordlist/test.txt
2	http://www.projetcligraphcrm.com/clt1/FUZZ	Dictionary	C:/Program Files/Edge-Security/WebSlayer-Beta/wordlist/common.txt
3	http://www.projetcligraphcrm.com/clt1/FUZZ	Dictionary	C:/Program Files/Edge-Security/WebSlayer-Beta/wordlist/common.txt

☑ Include Codes: --- Lines: --- Words: --- Chars: --- MD5: --- Regex

	Timer	Code	Lines	Words	Chars	MD5	Payload	Cookie	
1	0.655999	301	7	20	253	44453f2dec4959d8e49e679330c49177	images		http://w
2	0.578000	200	8	33	586	6ca7e81401b6311ef3cf7e97e1f2f5bd	index	PHPSESSID=bf05404aa26c1584d2edccc19fc277ae	
3	0.532000	301	7	20	250	effc55c76d81edc5b8f8d53deea5d5b7	log		http://w
4	0.452999	301	7	20	250	27e2ed87e82e54d4b4d7a15258b2fbe8	var		http://w
5	0.436999	302	0	0	0	d41d8cd98f00b204e9800998ecf8427e	log/index		../index

Scenarios

More realistic tests

- fragile

Automate your tests

Complete with fuzzing

Use proxy servers

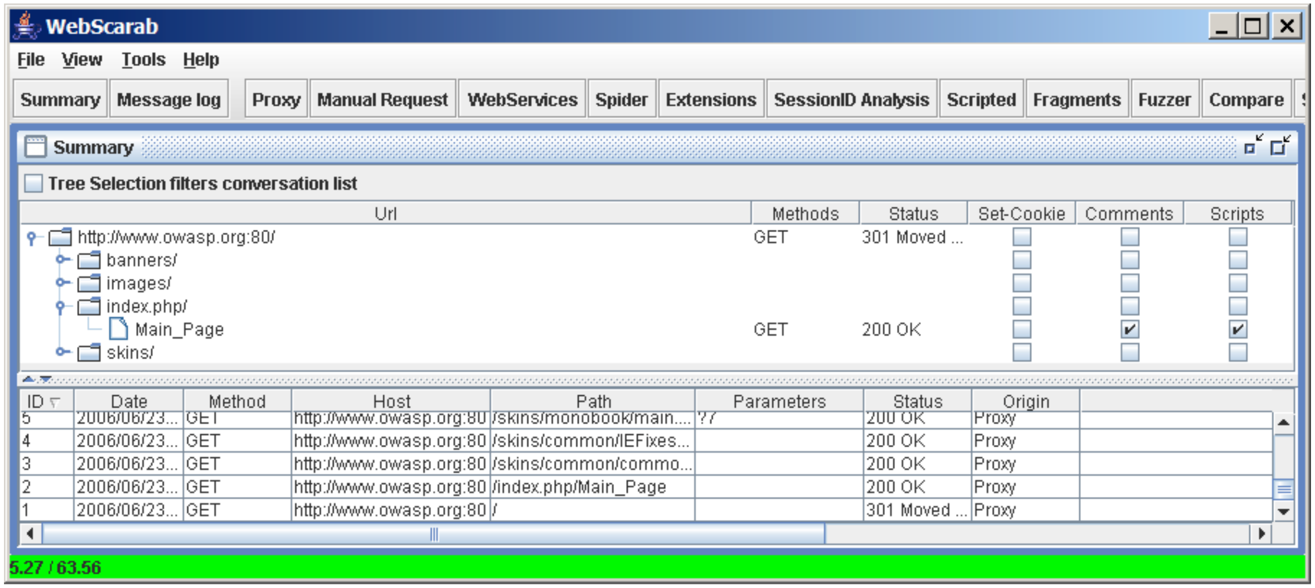
Scenarios

Firefox

Selenium IDE

WebScarab

http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project



□ Tree Selection filters conversation list

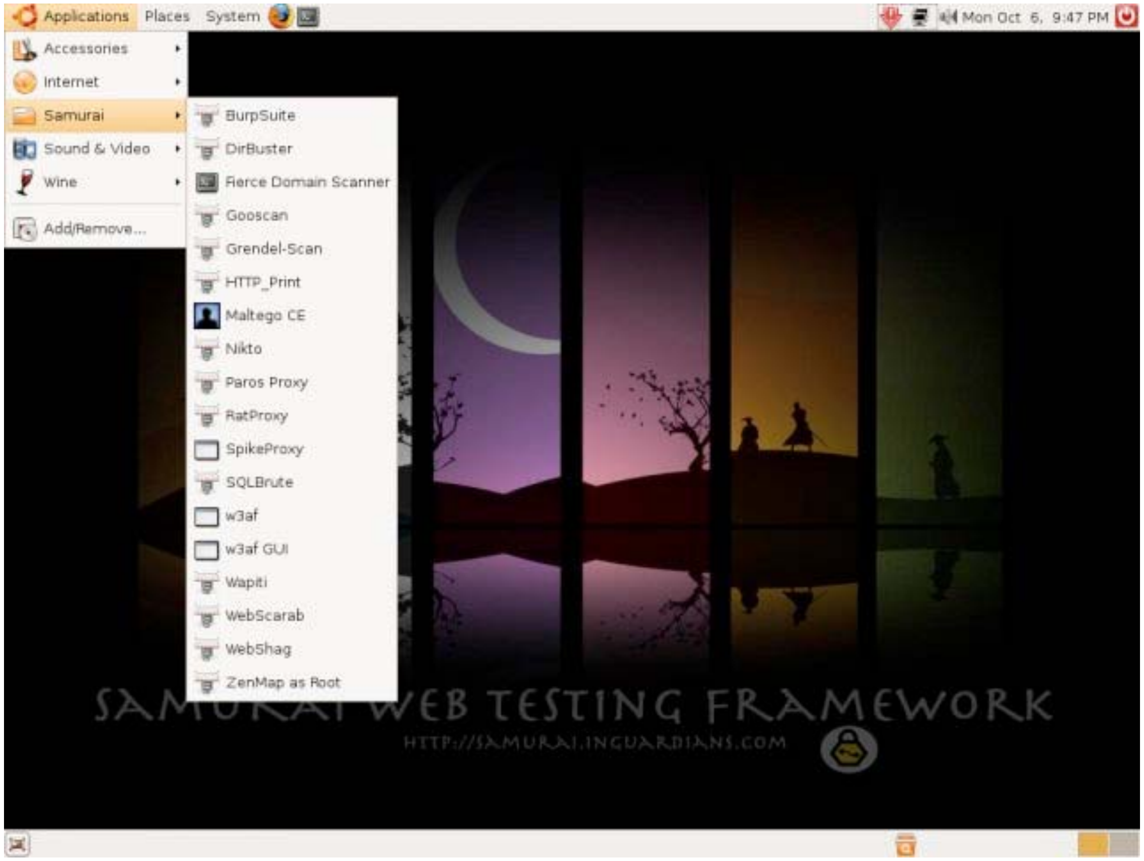
Url	Methods	Status	Set-Cookie	Comments	Scripts
http://www.owasp.org:80/	GET	301 Moved ...	□	□	□
banners/			□	□	□
images/			□	□	□
index.php/			□	□	□
Main_Page	GET	200 OK	□	☑	☑
skins/			□	□	□

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main....	?7	200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy

Simplify your life

Samurai Web Testing Framework

http://samurai.inguardians.com/



Conclusion

- Black box
    - Easy to set up
    - Take into account the context of the application
    - Often spectacular
    - Generally shallow

Open code audit

Code audits

Look into the PHP code

Search for hidden problems

Usually less spectacular than black box

From the interview

- Check if dev teams knows that to secure
- Have it explains their approach
  - Check what they say
  - Check what they don’t say

The shy version

We know there are security problems

- but we have no time to secure them
- this app has been written years ago
- we can’t keep up with the threats

The strong version

We have secured the application

- We use SSL, and webwasher and crypto
- All content is validated and filtered
- We don’t do any dynamical include
- Our frameworks doesn’t allow this

Approach

What to search for?

What are the entry points?

How can they be exploited

Or protected ?

What to search for?

- Injections
  - PHP
  - SQL
  - HTML
  - system

Keep focused

Easy to loose focus

Tempting to audit everything

PHP injections

- PHP injections
  - dynamical inclusion
    - include, require and *_once
  - back ticks
  - eval

Eval

- Easy to look for
- grep
  - Fast, available, convenient
  - 853 occurences
- Tokenizer
  - Semantic, accurate
  - 37 occurrences

Tokenizer

```
<?php print ("hello $world! "); ?>
```

```
    [1] => Array
        (
            [0] => 266
            [1] => print
            [2] => 1
        )

    [2] => Array
        (
            [0] => 370
            [1] =>
            [2] => 1
        )

    [3] => (
    [4] => "
    [5] => Array
        (
            [0] => 314
            [1] => hello
            [2] => 1
        )
```

```
[6] => Array
    (
        [0] => 309
        [1] => $world
        [2] => 1
    )

[7] => Array
    (
        [0] => 314
        [1] => !
        [2] => 1
    )

[8] => "
[9] => )
[10] => ;
        [1] => Array
            (
                [0] => PHP token
                [1] => PHP code
                [2] => Script line
            )
        [2] => "
```

Evals

- **`eval('$retour=$GLOBALS["'.$matches[1].'"];')`**
  - Variable variables.
- **`eval($contenu_thjipk);`**
- **`eval($contents_essai);`**
  - Content is read into variable, then executed : an include?
- **`eval('$hexdtime = "'.$hexdtime.'";')`**
  - Long way to cast a string into a string
- **`eval('$retour2.= '.var_dump($recept->erreur).';')`**
  - This doesn’t even work

Assessing the code

- One liners
  - One line of code is sufficiently to be bad
- Even though
  - you must follow the code
  - In reverse

Inclusion

- **`require("../params_frm.php")`**
- **`require(fct_lien_page_custom(TYPE_DOMAINE."/".TYPE_DOC."_custom.php","abs"))`**
- **`require(fct_lien_page_custom("params_footer.php","abs"))`**
  - Pretty secure inclusions

- But 96 variables used in includes
- **`include(fct_lien_page_custom("action/facture_".$format.".php","abs"))`**
  - $format, anyone?
- **`require_once("etat_simple_".$choix_page."_trt.php")`**
  - $choix_page, anyone ?

$format ?

```
<?php require("../params_trt.php");

$format=htmlentities($_REQUEST['exp_formdoc']);
if(empty($_REQUEST['exp_affiche'])) $affichage=0;
  else $affichage=$_REQUEST['exp_affiche'];
if(empty($_REQUEST['exp_stockdoc'])) $stockage=0;
  else $stockage=$_REQUEST['exp_stockdoc'];
$cde_id=$_REQUEST['exp_id'];
$type_doc=$_REQUEST['exp_typedoc'];

require(fct_lien_page_custom("fonctions/
fonction_img.php","abs"));

include(fct_lien_page_custom("action/facture_".
$format.".php","abs"));
?>
```

$choix_format ?

```
switch($choix) {
  case 0 : $choix_page="tabl";
  break;
  case 1 : $choix_page="histo1";
        if ($gfx_sens_graph=="1") $gfx_margegauche_dft="90";
  break;
  case 2 : $choix_page="histo2";
        if ($gfx_sens_graph=="1") $gfx_margegauche_dft="90";
  break;
  case 3 : $choix_page="histo3";
        if ($gfx_sens_graph=="1") $gfx_margegauche_dft="90";
  break;
  case 4 : $choix_page="histo4";
        if ($gfx_sens_graph=="1") $gfx_margegauche_dft="90";
  break;
  case 5 : $choix_page="histo5";
        if ($gfx_sens_graph=="1") $gfx_margegauche_dft="90";
  break;  }

  ###...Way below
  require_once("etat_simple_".$choix_page."_trt.php");
```

Statistical audit

Extract one type of information

Review it out of context

Use this as a starting point for more questions

Comments

//echo "<div><a class=\"texte1\" style=...

#echo "<pre>";

Left overs

#print_r($_REQUEST);

Main code is not cleaned of debug?

// hack for mozilla sunbird's extra = signs

Look for swearing, TODO, hack

Variables

6883 different variables names

All one possible one letter variable

32 chars : $cache_maxsize_UTF8StringToArray

Most used : $i (2586 times)

$_1904, $samedi, $dummy, $sss, 19 $unknowns

711 variables used only once in the codes

Other ideas

- name of functions
- name of classes
- name of constants
- literal
  - strings, numbers
- Condition (if, while)

register_globals strikes back

Foreach and $$

extract

import_request_var

$GLOBALS

parse_str

register_globals (ini_get(‘register_globals’))

Found!

- ./install/identification.php
- **`extract($_POST)  : 1`**
    - Injection by $_POST

- ./eggcrm/fonctions/fonctions_gen.php
- **`$GLOBALS[$k] = $chaine[$k]`**
- **`$GLOBALS[$this->mode] [$k] = $chaine[$k]`**

    - In the fct_urldecode, the values are stripslashed, and then injected in the $GLOBALS, resulting in variable creation

SQL injections

Point of entry

- mysql_query
- mysqli_real_escape_string
- SQL query :
    - string with SELECT, UPDATE, ...

Found!

-
  ```
  'UPDATE param_suivi SET      param_suivi_nom="'.str_replace($tr
  ansf_sp,$transf_fr,$_POST["suivi_nom"])  : 1
  ```
  - Direct injection via POST

-
  ```
  WHERE campagne_nom LIKE '%".addslashes($_REQUEST['rech_nom'])
  ```
  - Injection from $_REQUEST

-
  ```
  "UPDATE even_spl SET even_spl_fait='".
  $even_fait."',even_spl_modification='".$date_du_jour."'
  WHERE even_spl_id='".$even_id."' AND even_spl_affaire_id='".
  $even_aff_id."'";  : 1
  ```

-
  ```
  "INSERT INTO ".$type_doc."_suivi    (".
  $type_doc."_suivi_param_suivi_id, ".$type_doc."_suivi_".
  $type_doc."_id, ".$type_doc."_suivi_canal_id,    ".
  $type_doc."_suivi_action, ".$type_doc."_suivi_commentaire, ".
  $type_doc."_suivi_creation)    VALUES ('".$id_suivi."', '".
  $id_doc."', '".$id_canal."', '".
  $suivi_date."', '".addslashes($suivi_commentaire)
  ```

And also

- Header injection
  - Look for header()
- XSS
  - look for Echo, or concatenation with tags
- Etc...

Report

Vulnerability	Critical	Load
register_globals	High	High
Injections	High	Medium
SQL injection	Medium	High
headers	Low	Low

Team organization

Team Work

- Continuous audit?
  - Once
  - When necessary
  - Regularly
  - Continuously

PHP Mantra

List your mantra

The five most important rules you agree upon

Have them printed and visible to everyone

Cross audit

- Group developers by two
    - Have each one review the code of the other
    - Based on the mantra
- Light weight process
- Doesn’t have to be in the same project

PHP audit tools

groogle

Groogle (http://groogle.sourceforge.net)

Review Board (http://www.review-board.org/)

Rietveld http://codereview.appspot.com/

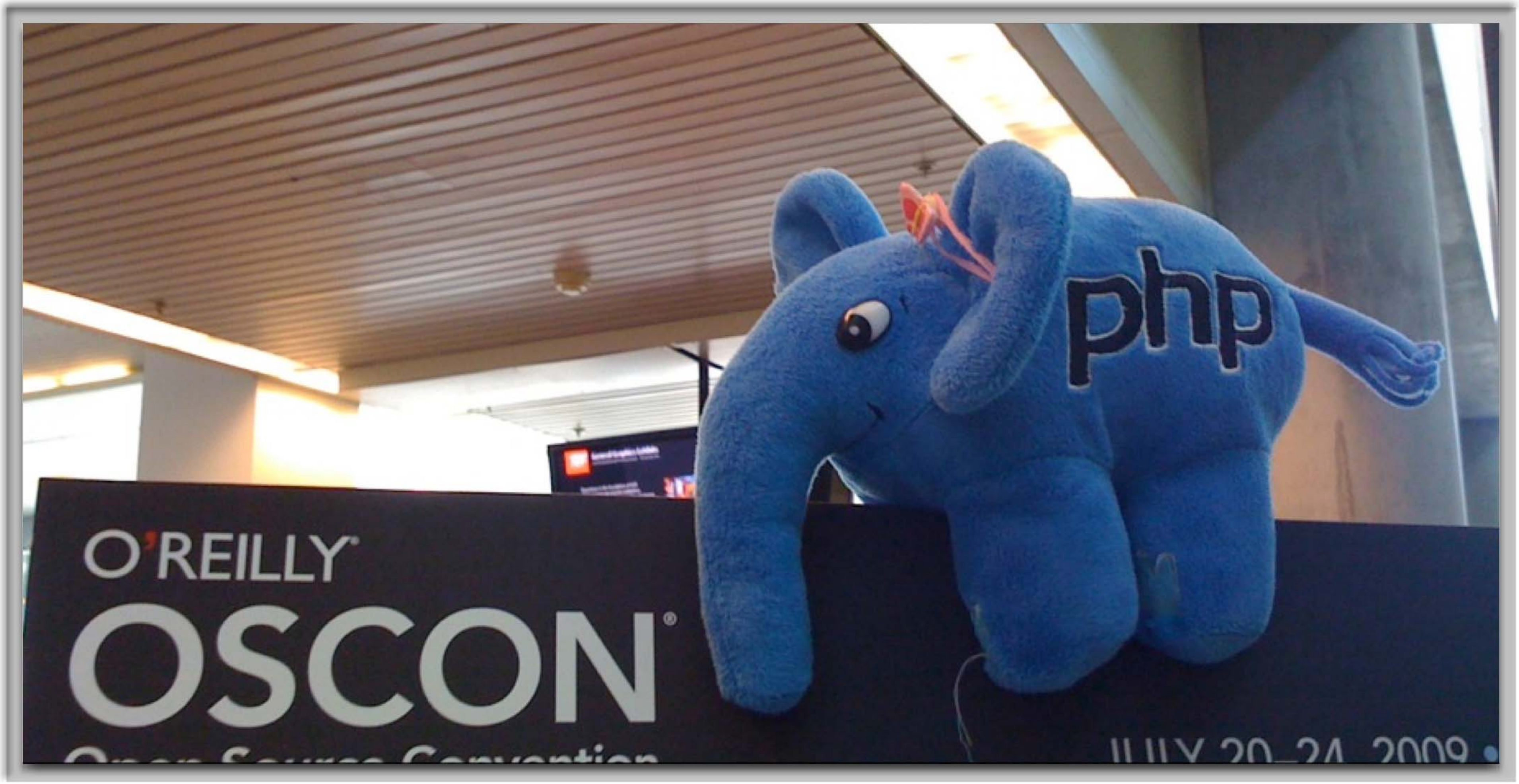
rietveld
Code Review for

SmartBear (http://www.smartbear.com/)

SmartBear
SOFTWARE

Community step up

- Mantra, cross audits
  - go beyond services and departements
- Open this outside ?
  - External review?
- New way of coding ?



Thank you!

Philippe Gamache : info@ph-il.ca

Damien Seguy : damien.seguy@alterway.fr