Admins - Anomalie #2861

Photos.april.org : la page search vérolée par du spam

21/12/2017 09:52 - Quentin Gibeaux

Statut:	Fermé	**Début:**	07/03/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Quentin Gibeaux	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Février 2018	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Un membre vigilant a remarqué que photos.april.org était référencé sur les moteurs de recherche avec des urls contenant des mots (viagra, etc), qui mènent vers des sites douteux.

Exemple : https://photos.april.org/index.php?search=cialis-5mg-prix-pharmacie

Difficile à analyser, la faille a l'air de flusher l'historique réseau de l'outil de debug de firefox…

Sous-tâches:

Demande # 2996: Faire en sorte que piwigo ne soit plus vérolable	**Fermé**
Demande # 2998: Migrer photos.april.org sur une vm pour l'isoler	**Fermé**

Historique

#1 - 21/12/2017 09:59 - François Poulain

Chez moi ça marche :

```
$ curl 'https://photos.april.org/index.php?search=cialis-5mg-prix-pharmacie' -H 'Host: photos.april.org' -H 'U
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0' -H 'Accept: text/html,applica
tion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' -H 'Accept-Language: fr-FR,fr;q=0.5' --compressed -H 'DNT: 1'
-H 'Connection: keep-alive' -I
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 21 Dec 2017 08:58:11 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: http://365-rx.com/search?id=1111&q=cialis
```

#2 - 21/12/2017 10:04 - Quentin Gibeaux

Avec un -L :

```
root@raspberrypi:~# curl 'https://photos.april.org/index.php?search=cialis-5mg-prix-pharmacie' -H 'Host: photo
s.april.org' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0' -H 'Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' -H 'Accept-Language: fr-FR,fr;q=0.5' --compr
essed -H 'DNT: 1' -H 'Connection: keep-alive' -IL
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 21 Dec 2017 09:01:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: http://365-rx.com/search?id=1111&q=cialis

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 21 Dec 2017 08:55:41 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.8
Set-Cookie: no_mobile=1
Set-Cookie: RNPS=UXHW9ADA0HFBJQP1QAVV6
Set-Cookie: id=1111; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: unique=1; expires=Fri, 22-Dec-2017 08:55:40 GMT; path=/
Set-Cookie: country_name=France; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
```

```
Set-Cookie: country_code=FR; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: lang=fr; expires=Sat, 26-Dec-2065 05:51:20 GMT; path=/
Set-Cookie: currency=EUR; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: ban_check=1; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: bonus=Viagra; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: uniq_flag=1; expires=Fri, 22-Dec-2017 08:55:40 GMT; path=/
Set-Cookie: shipping=AirMail; expires=Fri, 21-Dec-2018 08:55:40 GMT; path=/
Set-Cookie: b_test=1; expires=Thu, 28-Dec-2017 08:55:40 GMT; path=/
Set-Cookie: xspy=W10%3D; expires=Thu, 28-Dec-2017 08:55:40 GMT; path=/
```

#3 - 21/12/2017 10:31 - Quentin Gibeaux

J'ai cloné des sources propres de piwigo sur lamp et tenté un diff :

```
root@lamp:~/Piwigo# diff -ru --exclude=.git --exclude=language /var/www/photos.april.org/piwigo/ .   | less
```

Je n'ai rien remarqué de probant.

#4 - 21/12/2017 10:33 - François Poulain

J'ai pas mal greppé et rien trouvé de probant. Ni dans les sources, ni dans la DB.

#5 - 21/12/2017 10:38 - François Poulain

On n'est pas seuls : https://www.google.fr/search?q=cialis-5mg-prix-pharmacie+piwigo

#6 - 21/12/2017 10:54 - François Poulain

Une piste :

```
francois@renard:~$ curl 'https://photos.april.org/index.php?search=cialis-5mg-prix-pharmacie' -I
HTTP/1.1 400 Bad request
Server: nginx/1.10.3
Date: Thu, 21 Dec 2017 09:53:29 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: pwg_id=tr9ojtffctoosjr0m7p11corh0; path=/; HttpOnly
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

francois@renard:~$ curl 'https://photos.april.org/index.php?search=cialis-5mg-prix-pharmacie' -I -H 'Accept-La
nguage: fr-FR,fr;q=0.5'
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 21 Dec 2017 09:53:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: http://365-rx.com/search?id=1111&q=cialis
```

#7 - 21/12/2017 12:08 - François Poulain

mv _data _data.owned a coupé la chose.

#8 - 21/12/2017 12:18 - François Poulain

```
root@lamp:/var/www/photos.april.org/piwigo/_data.pwned# base64 -d settings/0cca657fdc146e4859ab4fe5bbbacd65 |
head
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <title>Ou Trouver Viagra - Pharmacie En Ligne</title>
<meta name="description" content="Ou trouver viagra. La Poste aérienne gratuite est disponible pour les comman
des plus de 150 €. 10% de la réduction pour tous d'autres commandes, Des offres spéciales dans notre pharmacie
!" />
<meta name="keywords" content="ou trouver viagra" />
  <meta name="generator" content="Piwigo (aka PWG), see piwigo.org">
```

#9 - 21/12/2017 12:34 - François Poulain

J'ai ouvert https://github.com/Piwigo/Piwigo/issues/827

#10 - 22/12/2017 09:40 - François Poulain

- Fichier _data.pwned.tar.gz ajouté

Upload du dossier _data, sans _data/i (qui fait 1.5 Go).

#11 - 22/12/2017 09:54 - François Poulain

Le plus intéressant semble être ici :

```
_data.pwned$ for file in $(file settings/decoded/* | grep ASCII | awk -F: '{print $1}'); do echo "" && echo ==
============== && cat $file; done

================
/index.php?search=achat-cialis-pas-cher
/index.php?search=acheter-cialis-tadalafil
/index.php?search=acheter-clomid-50mg
/index.php?search=acheter-du-vrai-cialis
/index.php?search=acheter-lioresal-baclofen
/index.php?search=acheter-viagra-pour-femme
/index.php?search=cialis-10-prix
/index.php?search=cialis-5mg-prix-pharmacie
/index.php?search=cialis-sans-ordonnance-belgique
/index.php?search=commande-de-cialis
/index.php?search=comment-trouver-du-viagra
/index.php?search=dapoxetine-acheter
/index.php?search=faut-il-une-ordonnance-pour-du-cialis
/index.php?search=le-prix-du-cialis-en-pharmacie
/index.php?search=le-viagra-pour-femme
/index.php?search=levitra-moins-cher
/index.php?search=lioresal-acheter
/index.php?search=meilleur-prix-cialis
/index.php?search=nolvadex-acheter
/index.php?search=orlistat-sandoz-pas-cher
/index.php?search=ou-trouver-viagra
/index.php?search=priligy-en-suisse
/index.php?search=prix-du-cialis-en-espagne
/index.php?search=propecia-pour-femme
/index.php?search=vente-cialis-belgique
/index.php?search=vente-de-cialis-sans-ordonnance
/index.php?search=vente-de-viagra-en-suisse
/index.php?search=vente-de-viagra-sans-ordonnance
/index.php?search=vente-en-ligne-cialis
/index.php?search=vrai-cialis-moins-cher
================
2592000
================
a:7:{s:17:"SMART_SERVICE_URL";s:35:"http://37.1.205.230/Smart/Smart.php";s:15:"TDS_SERVICE_URL";s:32:"http://3
7.1.205.230/Smart/Go.php";s:19:"SEARCHENGINE_AGENTS";s:39:"google|slurp|msnbot|bingbot|baiduspider";s:13:"MOBI
LE_AGENTS";s:35:"android|iphone|windows phone|mobile";s:18:"DONOR_CACHE_EXPIRE";i:157680000;s:20:"DOORWAY_CACH
E_EXPIRE";i:157680000;s:17:"SITE_CACHE_EXPIRE";i:604800;}
================
/picture.php?/2569/categories
/picture.php?/2733/categories
/picture.php?/1312/category/94
/picture.php?/3468/categories
/picture.php?/1195/category/12
/picture.php?/159/categories&slideshow=
/action.php?id=3663&part=e
/
/index.php?/category/44
/index.php?/category/72
/picture.php?/632
/index.php?/category/7/start-16
/picture.php?/3446/categories&slideshow=
/picture.php?/840
/picture.php?/1451
/picture.php?/3425/category/76
/picture.php?/2935/category/69
/piwigo/index.php?/category/23
/picture.php?/3691/categories&slideshow=
/piwigo/comments.php
/picture.php?/3804/categories
/index.php?/categories/created-monthly-calendar-2011-5-29
```

/picture.php?/1219
/picture.php?/683
/index.php?/category/35/start-16
/picture.php?/3683/categories
/picture.php?/3056/categories&slideshow=
/picture.php?/1690
/picture.php?/3472/category/3
/picture.php?/2398/category/66
/picture.php?/1555/categories&slideshow=
/index.php?/categories/posted-monthly-calendar-2013-6-07
/picture.php?/319/category/56
/picture.php?/1646/category/47
/index.php?/categories/posted-monthly-calendar-2013-7-10
/picture.php?/3444/categories&slideshow=
/picture.php?/3735/category/95
/picture.php?/1949/category/20
/picture.php?/3815/category/108
/picture.php?/1438/categories&slideshow=
/picture.php?/3673/categories&slideshow=
/picture.php?/988/categories&slideshow=
/index.php?/categories/posted-monthly-calendar-2014-6-30
/index.php?/category/101/start-32
/picture.php?/2238/category/62
/index.php?/posted-monthly-list-2012-10-27
/index.php?/categories/created-monthly-list-2013-5
/index.php?/categories/created-monthly-calendar-2012-2-26
/index.php?/categories/posted-monthly-list-2012-3-12
/picture.php?/23/category/93
/picture.php?/3301/categories
/picture.php?/251/categories
/index.php?/category/5
/picture.php?/3188/categories
/picture.php?/1256/category/101
/picture.php?/1236/category/101
/picture.php?/1304/categories&slideshow=
/picture.php?/1865/categories&slideshow=
/picture.php?/3769/category/95
/picture.php?/514/categories&slideshow=
/index.php?/categories/created-monthly-list-2014-any
/picture.php?/1218/categories
/picture.php?/880/category/73
/picture.php?/864/categories
/picture.php?/1260/categories&slideshow=
/picture.php?/342/categories
/index.php?/category/64
/index.php?/category/58
/picture.php?/1305/categories
/picture.php?/3922/category/123
/picture.php?/3868/categories
/picture.php?/1969/categories
/picture.php?/3450/categories
/index.php?/category/18
/index.php?/created-monthly-list-2015-02-27
/index.php?/category/51/start-32
/index.php?/category/125
/picture.php?/3309/category/76
/picture.php?/1426/categories
/index.php?/category/93/start-32
/picture.php?/3590/categories
/picture.php?/3212/categories
/picture.php?/458/category/52
/picture.php?/3661/categories
/picture.php?/3754/categories
/picture.php?/248/categories
/picture.php?/296/categories&slideshow=
/index.php?/posted-monthly-list-2010-09-12
/picture.php?/852/categories
/picture.php?/1354/categories
/picture.php?/138/categories&slideshow=
/picture.php?/3233/categories
/piwigo/index.php?/category/103
/index.php?/category/48
/picture.php?/694/categories&slideshow=
/picture.php?/1275/categories
/index.php?/category/130

```
/index.php?/category/38
/picture.php?/699/categories&slideshow=
/picture.php?/1347/category/9
/index.php?/created-monthly-list-2008-06-01
================
2592000
================
1434731894
================
2592000
================
/index.php?search=achat-cialis-pas-cher
/index.php?search=acheter-cialis-tadalafil
/index.php?search=acheter-clomid-50mg
/index.php?search=acheter-du-vrai-cialis
/index.php?search=acheter-lioresal-baclofen
/index.php?search=acheter-viagra-pour-femme
/index.php?search=cialis-10-prix
/index.php?search=cialis-5mg-prix-pharmacie
/index.php?search=cialis-sans-ordonnance-belgique
/index.php?search=commande-de-cialis
/index.php?search=comment-trouver-du-viagra
/index.php?search=dapoxetine-acheter
/index.php?search=faut-il-une-ordonnance-pour-du-cialis
/index.php?search=le-prix-du-cialis-en-pharmacie
/index.php?search=le-viagra-pour-femme
/index.php?search=levitra-moins-cher
/index.php?search=lioresal-acheter
/index.php?search=meilleur-prix-cialis
/index.php?search=nolvadex-acheter
/index.php?search=orlistat-sandoz-pas-cher
/index.php?search=ou-trouver-viagra
/index.php?search=priligy-en-suisse
/index.php?search=prix-du-cialis-en-espagne
/index.php?search=propecia-pour-femme
/index.php?search=vente-cialis-belgique
/index.php?search=vente-de-cialis-sans-ordonnance
/index.php?search=vente-de-viagra-en-suisse
/index.php?search=vente-de-viagra-sans-ordonnance
/index.php?search=vente-en-ligne-cialis
/index.php?search=vrai-cialis-moins-cher
================
<table border="0">
<tr><td><a href="http://photos.april.org/index.php?search=achat-cialis-pas-cher">achat cialis pas cher</a></td
></tr>
<tr><td><a href="http://photos.april.org/index.php?search=vrai-cialis-moins-cher">vrai cialis moins cher</a></
td></tr>
<tr><td><a href="http://photos.april.org/index.php?search=cialis-10-prix">cialis 10 prix</a></td></tr>
<tr><td><a href="http://photos.april.org/index.php?search=nolvadex-acheter">nolvadex acheter</a></td></tr>
<tr><td><a href="http://www-lsm.in2p3.fr/gallery/index.php?id=91165">acheter viagra pfizer</a></td></tr>
<tr><td><a href="http://www.patrimoineculturel.org/?search=buy-baclofen">buy baclofen</a></td></tr>
<tr><td><a href="http://www-lsm.in2p3.fr/gallery/index.php?id=62794">cialis pharmacie en ligne</a></td></tr>
<tr><td><a href="http://www.unmarried.org/limesurvey/index.php?id=62629">viagra cialis levitra online</a></td>
</tr>
</table>
```

#12 - 01/02/2018 09:50 - Quentin Gibeaux

- Assigné à mis à Quentin Gibeaux

- Version cible changé de Backlog à Février 2018

Vérifier l'intégrité du code et coder une sonde qui cherche la réapparition

#13 - 15/02/2018 14:08 - Quentin Gibeaux

J'ai installé le module suivant : http://piwigo.org/ext/extension_view.php?eid=844
Après exécution :

```
Piwigo 2.9.2, 583 files scanned in 0.901 seconds
    Well done! Everything seems good :-)
```

Ça a l'air ok.

#14 - 15/02/2018 14:41 - Quentin Gibeaux

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

J'ai rajouté un check icinga qui va greper des mots "spam" dans le dossier _data de piwigo pour détecter l'apparition.

#15 - 07/03/2018 13:03 - Quentin Gibeaux

- Statut changé de Résolu à Confirmé

le _data n'est pas seul, le problème est revenu…
-> Modifier le monitoring pour vérifier que la réponse HTTP ne mène pas à une redirection vers du spam

#16 - 07/03/2018 13:35 - Quentin Gibeaux

J'ai corrigé le check icinga, il ne détectait pas bien le spam.

#17 - 07/03/2018 14:06 - François Poulain

Je propose de couper photos.april.org jusque ce qu'on ait la certitude que ça ne se reproduise pas.

Si l'uptream n'a pas idée de comment ça arrive, vu que ça arrive sur des dizaines d'instances, je propose de migrer vers autre chose.

#18 - 07/03/2018 14:24 - Quentin Gibeaux

Si l'on coupe, on aura jamais la certitude que ça se reproduise pas car on ne saura pas comment c'est réalisé.
Là le check icinga est réparé, au prochain pown on détectera l'horodatage de l'infection, ce qui aidera à trouver l'origine du problème.

-> Laissons notre piwigo en honey-pot pour détecter une piste d'infection ?

Pour depowner il suffit juste de supprimer le dossier _data dans le dossier de piwigo.

#19 - 07/03/2018 14:30 - Quentin Gibeaux

- Statut changé de Confirmé à Résolu

#20 - 07/03/2018 22:08 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

Fichiers

_data.pwned.tar.gz	4,16 Mo	22/12/2017	François Poulain