CTF | 关于web的小伎俩

原创

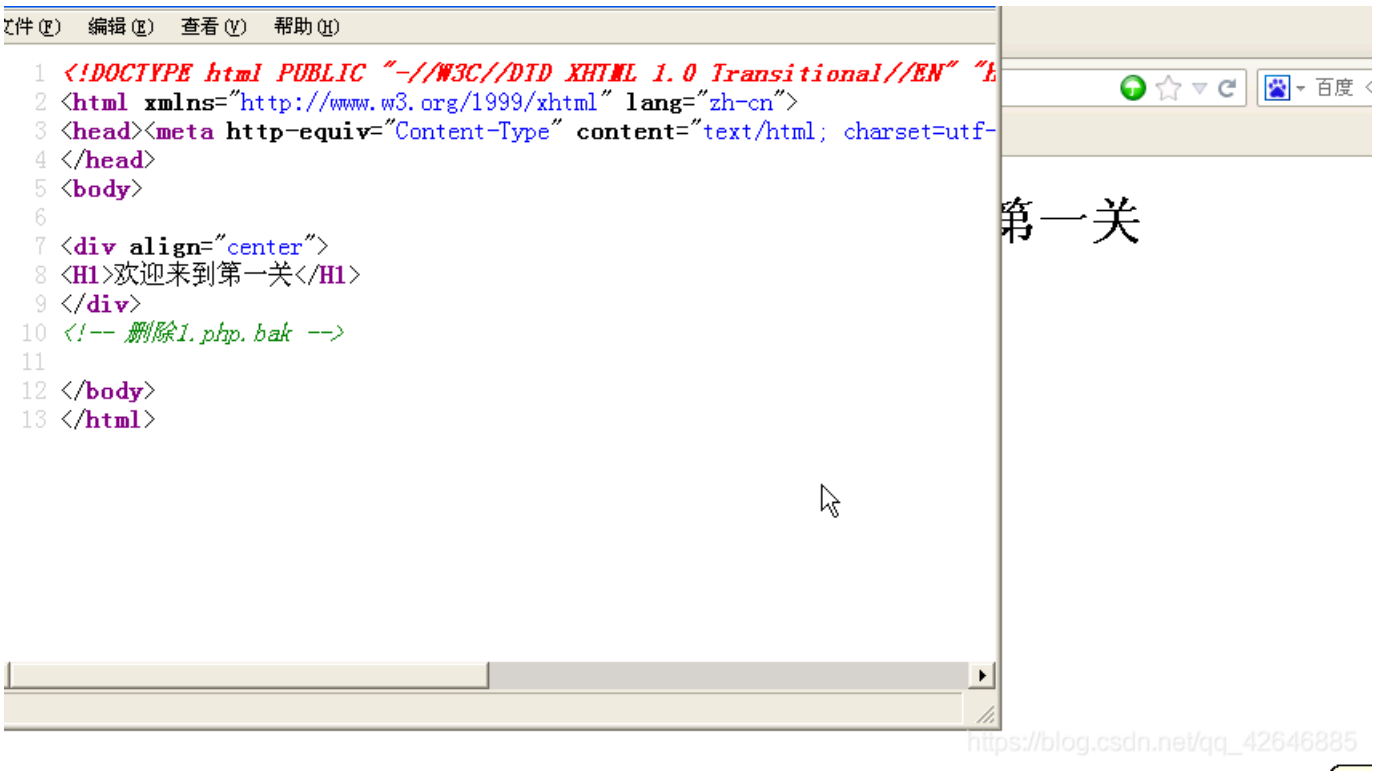
大青呐 于 2019-07-06 12:44:52 发布 800 收藏 6
分类专栏： CTF-Web实验 CTF-Web实验 文章标签： CTF WEB

打开服务器上的网页然后看到进入第一关的按钮，点击。

点击按钮，跳转到下一个页面。

欢迎来到第一关

查看源代码，看到有一行的注释：删除1.php.bak



在地址栏加上1.php.bak后，页面变化不大，多了几个符号。

';

欢迎来到第一关

';

再次查看源代码：

```
F)  编辑(E)  查看(V)  帮助(H)
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-cn">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-equiv="Conten
</head>
<body>

<div align="center">';
<H1>欢迎来到第一关</H1>';
</div>';
<!-- 删除1.php.bak>;
<button type="button" onclick="javascript:location.href='the2nd.php'">第二关</button>
</body>
</html>
```

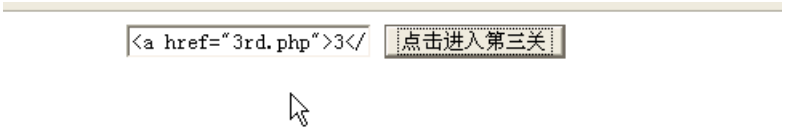

注释中给了第二关的地址，在地址栏访问：

点击“点击进入第三关”的按钮：

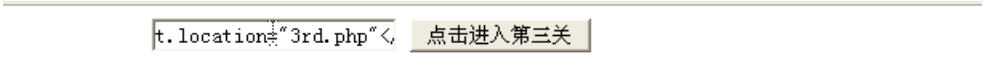
看到一个弹窗，以及第三关的页面是3rd.php，点击确定返回之前第二关的页面。

看到输入框，很容易想到xss，写个alert，居然弹框了。

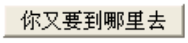
尝试构建一个a标签插进去。尝试后发现不行，构造出的链接闪一下就没了，使用了黑魔法。



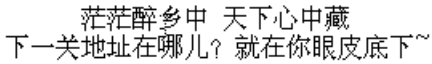
使用重定向跳转页面<script>document.location="3rd.php"</script>。



发现成功绕过验证，点击进入下一关。



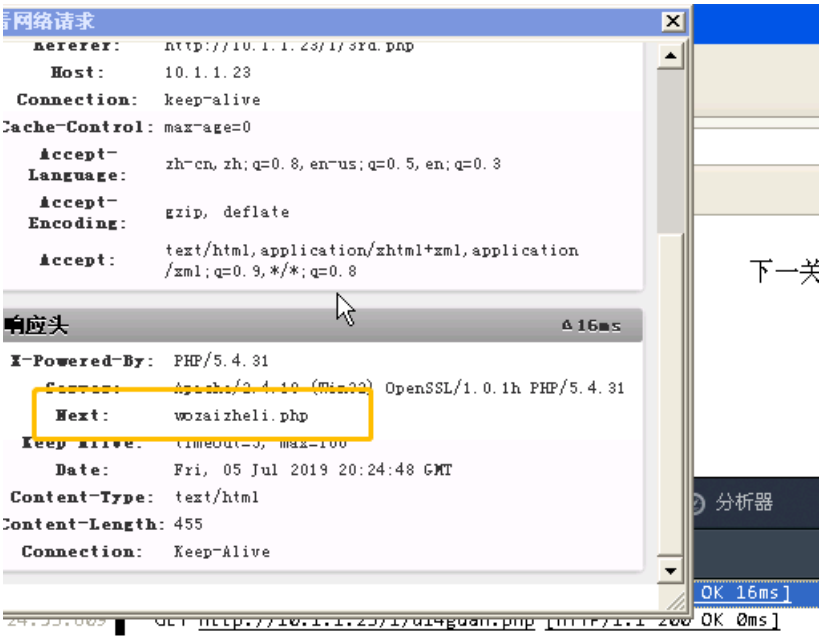
出现了只有文字的页面，再次查看页面的源代码。



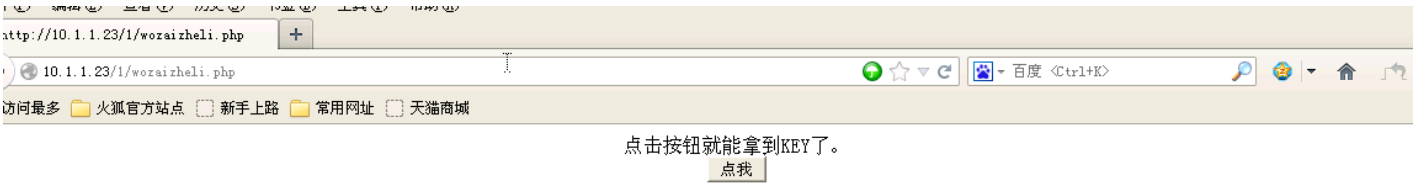
源代码中没有发现什么异常和线索。文字内容提示下一关地址就在眼皮底下，就查看下Http原始请求包和返回包。

```
(F) 编辑(E) 查看(V) 帮助(H)
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-cn">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-equiv="Content-Language" content="zh-CN" />
</head>
<body>
<div align="center">茫茫醉乡中 天下心中藏<br>下一关地址在哪儿？就在你眼皮底下~</div></body>
</html>
```

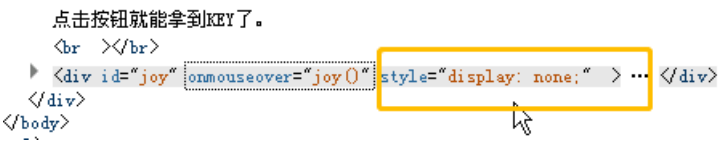

在返回的报文中有个next字段，提供了下一关的页面



调转到页面，看到提示：



可是在鼠标放到按钮上时，按钮消失了。审查元素看下:



发现使用了display:none的样式设置，将它设置为block，按钮出现。点击按钮，按钮还是消失了，看到按钮是有个joy()函数操作，看下其代码，发现是该脚本隐藏了按钮。再删除了按钮上的onmouseover该操作，按钮出现。

```
<script type="text/javascript">
function joy(){
    var joy = document.getElementById("joy");
    joy.style.display="none";
}
</script>
```

点击按钮，出现了key，结束。

总结：

1、该小游戏包含知识有：HTTP协议、XSS、HTML及CSS部分知识。

2、要仔细观察页面中的所有线索，包括地址栏，源代码，页面元素等。

3、不断在实战中积累经验，积累知识，路漫漫其修远兮。