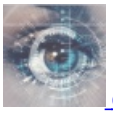
攻防世界PHP2

原创

听门外雪花飞 于 2022-01-25 18:55:12 发布 542 收藏

分类专栏： ctf刷题纪 文章标签： php 安全 web安全

本文链接：https://blog.csdn.net/weixin_52268949/article/details/122690545



PHP2

进入环境就一个英文其他啥都没有，英文也没啥提示信息

我们使用dirsearch扫描一下，一开始确实没扫到什么东西，到最后看了wp发现原来源码是在index.phps中，这里只提供一个思路，不必深究

```php
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>
```

分析代码通过get方式输入一个id值如果admin=id那就输出not allowed并退出php程序，然后进行一次url解码，然后再判断idadmin就可以输出flag

这题其实也很简单我们只需要将admin中任意一个字母进行url编码然后就可以绕过检测，因为程序中有个url解码，然后我们使用浏览器传参也会进行一次解码，所以我们那个字母要进行两次url编码，这里我就编码d了

```
?id=a%25%36%34min
```

到index.php中去传参

得到flag