由于没有对后缀名进行处理，可以有很多绕过姿势
POST时将后缀名利用大小写即可绕过
另外经过测试蚁剑可以连接phtml的，其他的如php3、php4、php5、phps、phtm没有成功，可能是环境的原因
另外加.、空格、.空格.也可以

也可以利用%00截断，由于传到目录的位置是由save_name控制的，因此将其设为20.php.+.gif，然后再将+改为16进制的00即可，但是由于php版本的问题没有办法实验

另外，可以使用move_upload_file函数的漏洞，会忽略文件末尾的/.将save_name写为20.php/.即可，会自动将/.忽略掉从而完成文件上传（经测试可以），这个适用于没有对后缀名处理并且没有规定白名单的情况
不过我查了一下关于PHP任意文件上传漏洞（CVE-2015-2348），即move_upload_file函数的漏洞，也是关于这个%00截断的，没有关于/.的说法
关于该漏洞的介绍如下：http://bobao.360.cn/news/detail/1383.html
简而言之就是move_upload_file函数的第二个参数destination不要通过get、post来传递，否则就会出现%00截断漏洞
适用版本为5.4.38~5.6.6，同时由于php 5.2版本本身就受到00截断漏洞的影响，所以也在受影响的行列之中。