

预期存在两处漏洞

Getshell 流程：

1.通过爆破或变量覆盖，使得 session[admin] == True

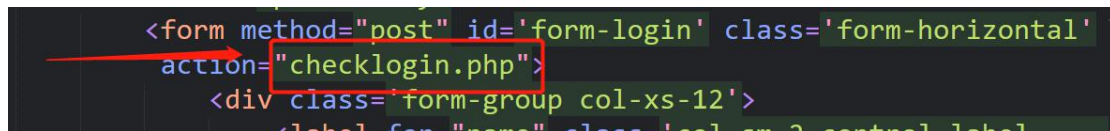
--->

2.Add\_photo.php 传文件到 upload.php 上传木马，看到 unicode 编码的 上传路径

--->

3.连接木马 getshell

在 index.html 中 看到 checklogin.php，并在多个文件中可以看到包含 checklogin.php，寻找 session[admin] == True 来判断当前用户是否登录。登录后，可从 Add\_photo.php 进行 php3 的后缀上传木马，upload.php 会打印 json 格式的文传路径。

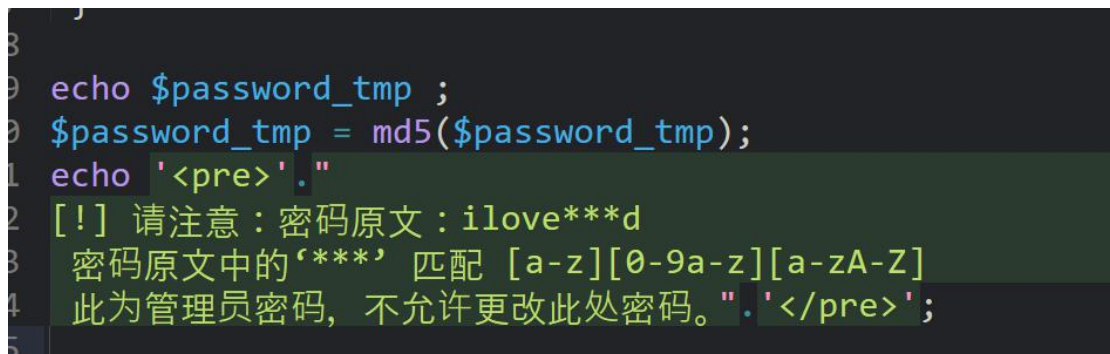


```
<form method="post" id='form-login' class='form-horizontal'
      action="checklogin.php">
  <div class='form-group col-xs-12'>
    <label for="name" class='col-sm-2 control-label'>
```

第一处：

Checklogin.php

虽然登录处有注入，但是没啥用。因为知道密文但是也没办法通过 md5 运算解密登录。在此文件中有正则提示，通过写脚本进行 md5 爆破即可得到明文密码： ilovef00d

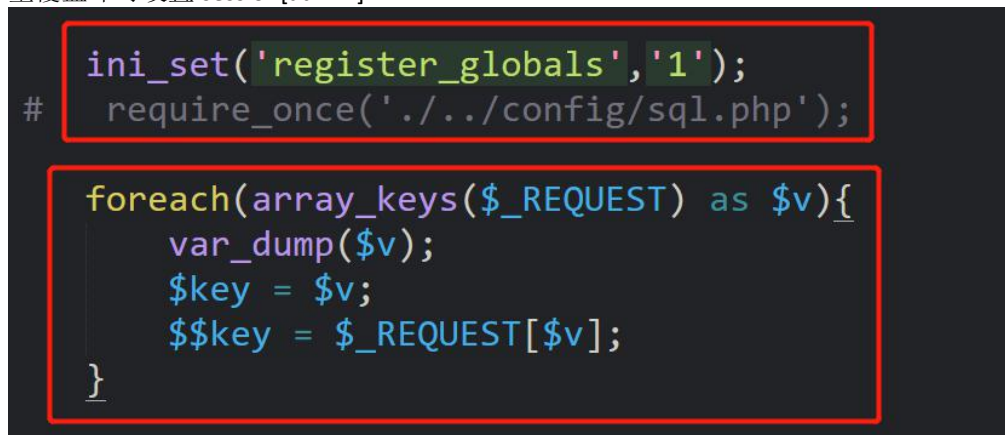


```
echo $password_tmp ;
$password_tmp = md5($password_tmp);
echo '<pre>' . "
[!] 请注意：密码原文：ilove***d
密码原文中的'***' 匹配 [a-z][0-9a-z][a-zA-Z]
此为管理员密码，不允许更改此处密码。" . "</pre>";
```

第二处：

Checklogin.php

还是这个文件，存在变量覆盖(PHP 5.4 以后不能直接变量覆盖，但是后面双\$导致的人为变量覆盖依然可以)或双\$变量覆盖。访问 “http://ip:port/checklogin.php?\_SESSION[admin]=true”或者双\$变量覆盖即可设置 session[admin]



```
ini_set('register_globals', '1');
# require_once('../config/sql.php');

foreach(array_keys($_REQUEST) as $v){
    var_dump($v);
    $key = $v;
    $$key = $_REQUEST[$v];
}
```