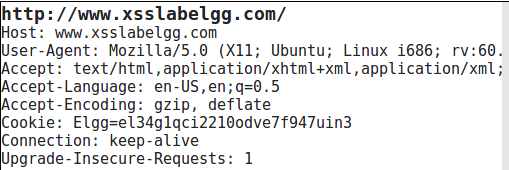
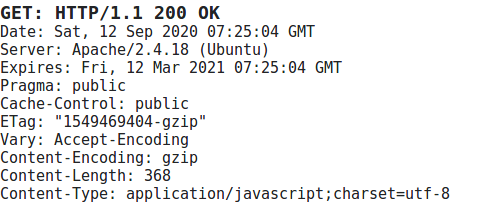
Task1：

安装HTTP Header Live插件，在左侧窗口查看已捕获的请求。登陆elgg，捕获到get请求和响应报文，在网站中注册或者发布内容等更改数据库的内容时，即能捕获到post请求和响应报文、

Get请求报文捕获如下



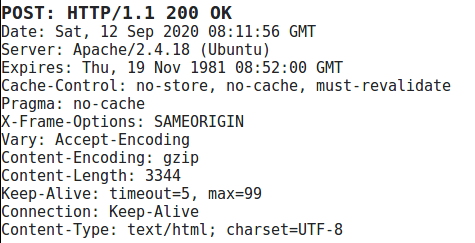
Get响应报文捕获如下



Post请求报文捕获如下



Post响应报文捕获如下



请求报文中

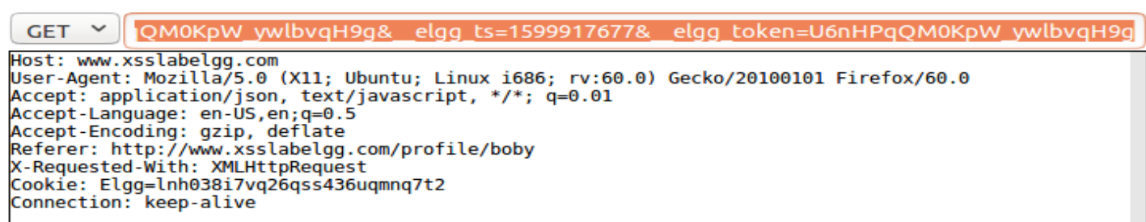
1. Accept表示指定客户端能够接收的内容类型（其中text/xml表示XML格式，application/xhtml+xml表示XHTML格式，application/xml表示XML数据格式和一些其他格式的内容类型）；
2. Accept-Encoding表示指定浏览器可以支持的web服务器返回内容压缩编码类型
3. Accept-Language表示浏览器可接受的语言
4. Cookie 是HTTP请求发送时，会把保存在该请求域名下的所有cookie值一起发送给web服务器。
5. Connection表示是否需要持久连接。（HTTP 1.1默认进行持久连接）
6. Referer表示先前网页的地址，当前请求网页紧随其后,即来路

响应报文中

1. Expires表示响应过期的日期和时间
2. Pragma包括实现特定的指令，它可应用到响应链上的任何接收方
3. Cache-Control告诉所有的缓存机制是否可以缓存及哪种类型
4. ETag表示请求变量的实体标签的当前值
5. Vary是告诉下游代理是使用缓存响应还是从原始服务器请求
6. Content-Encoding是web服务器支持的返回内容压缩编码类型。
7. Content-Length是响应体的长度
8. Content-Language是响应体的语言
9. Content-Type是返回内容的MIME类型
10. Server表示web服务器软件名称

Task2：

先登陆Alice的账号，并添加boby为好友，用HTTP Header Live插件捕获GET报文，并将url复制下来



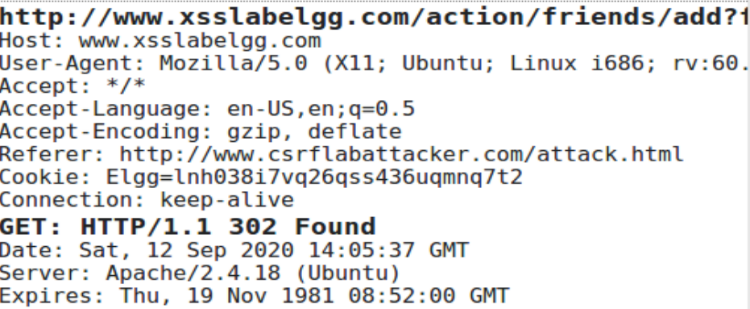
在var/www/CSRF/Attack文件目录下用管理员权限创建attack.html文件，并输入以下代码



其中url部分直接粘贴

以boby的名义发布包含[www.csrflabattacker.com/attack.html](http://www.csrflabattacker.com/attack.html)网址链接的博客

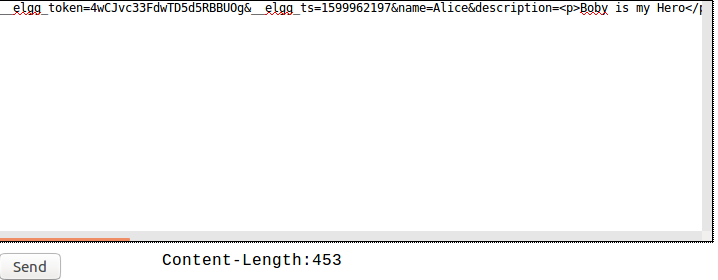
Alice登录后点击链接后，用HTTP Header Live插件捕获报文发现已经url发送过去



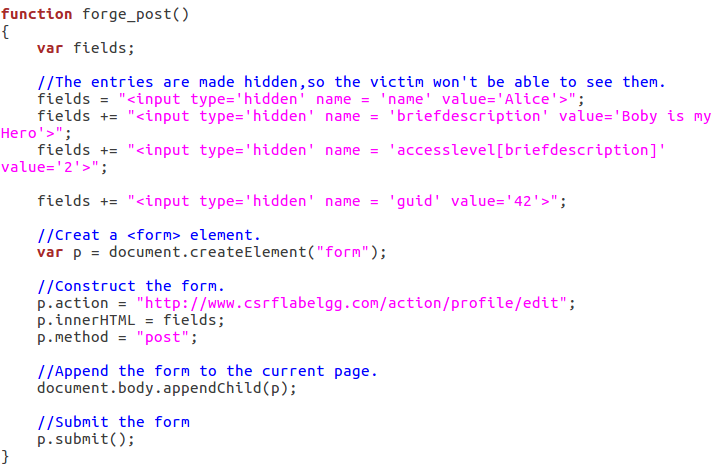
回到Alice的个人页面并刷新，发现添加好友成功，即攻击成功。

Task3：

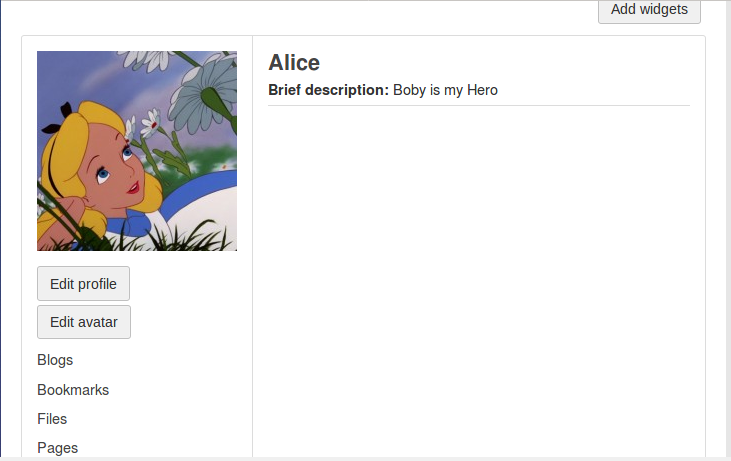
先通过Alice账号输入并保存briefdescription的内容，用插件捕获post报文，观测post报文的参数内容



在var/www/CSRF/Attack文件目录下用管理员权限修改attack.html内容，部分截图如下

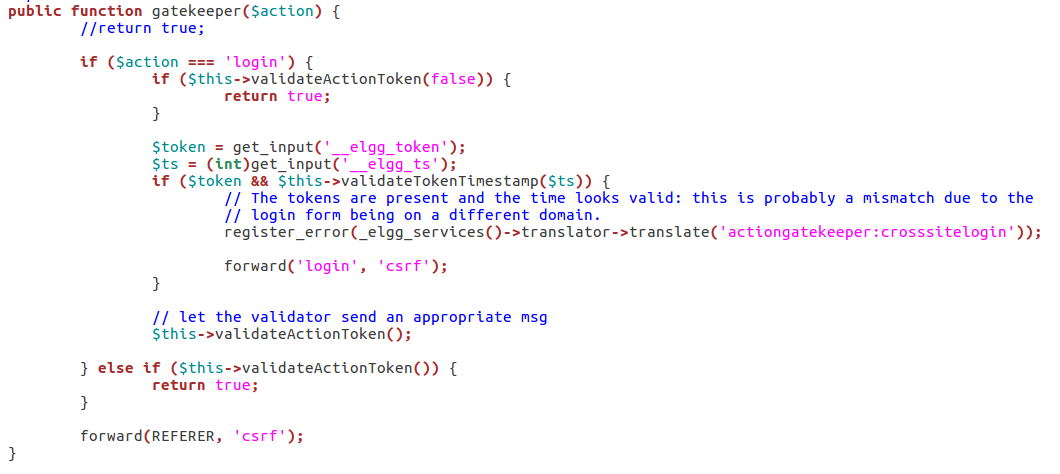


删除签名后用用Alice账号再次点击之前Boby账号博客中的链接，刷新之后发现签名已被修改

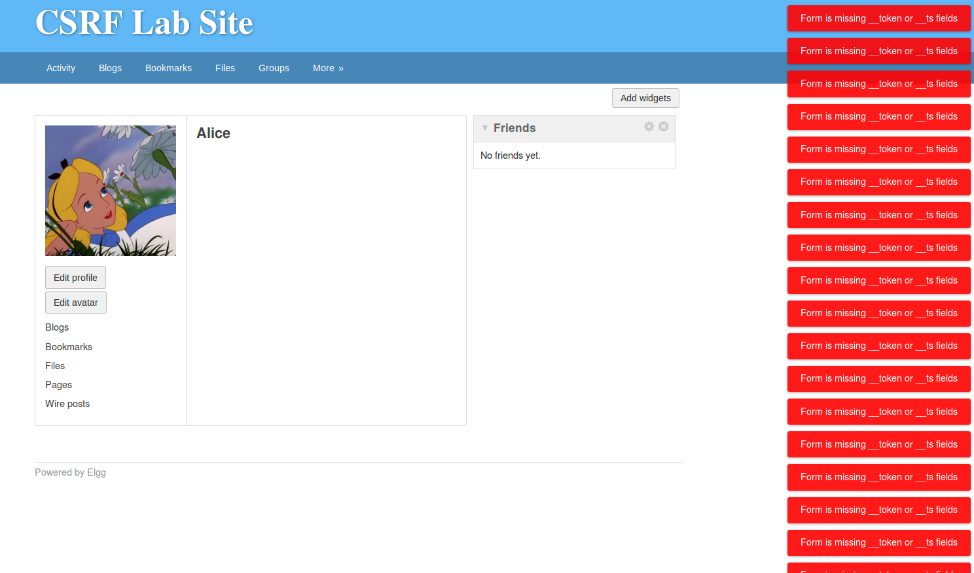


Task4;

将/var/www/CSRF/ Elgg/vendor/elgg/elgg/engine/classes/Elgg目录下ActionsService.php文件中gatekeeper函数的return true注释掉，即重启了elgg的时间戳保护



再次重复task3中的操作，发现点击恶意链接后页面不会跳转，进入Alice的界面之后会弹出如下信息，且签名不会被添加



即保护措施开启成功，攻击失败