57118130

王嘉麟

Task1:

**Add friend http get request**

http://www.csrflabelgg.com/action/friends/add?friend=42&\_\_elgg\_ts=1599963784&\_\_elgg\_token=QDzE89dZCxw1Of8HArMZvg&\_\_elgg\_ts=1599963784&\_\_elgg\_token=QDzE89dZCxw1Of8HArMZvg

Host: www.csrflabelgg.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.csrflabelgg.com/profile/alice

X-Requested-With: XMLHttpRequest

Cookie: Elgg=dcd3etivpfvleltu4ub37un062

Connection: keep-alive

GET: HTTP/1.1 200 OK

Date: Sun, 13 Sep 2020 02:23:38 GMT

Server: Apache/2.4.18 (Ubuntu)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Content-Length: 368

Keep-Alive: timeout=5, max=99

Connection: Keep-Alive

Content-Type: application/json;charset=utf-8

**Change profile HTTP post request**

http://www.csrflabelgg.com/action/profile/edit

Host: www.csrflabelgg.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.csrflabelgg.com/profile/boby/edit

Content-Type: application/x-www-form-urlencoded

Content-Length: 531

Cookie: Elgg=foda2utuuip53uchc4lursn6t6

Connection: keep-alive

Upgrade-Insecure-Requests: 1

\_\_elgg\_token=Eu\_TD8Dy-IEyxHYnaPCitA&\_\_elgg\_ts=1599964888&name=Boby&description=<p>I want to be alice&#39;s friend!</p>

&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=43

POST: HTTP/1.1 302 Found

Date: Sun, 13 Sep 2020 02:41:41 GMT

Server: Apache/2.4.18 (Ubuntu)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: http://www.csrflabelgg.com/profile/boby

Content-Length: 0

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html;charset=utf-8

http://www.csrflabelgg.com/profile/boby

Host: www.csrflabelgg.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.csrflabelgg.com/profile/boby/edit

Cookie: Elgg=foda2utuuip53uchc4lursn6t6

Connection: keep-alive

Upgrade-Insecure-Requests: 1

POST: HTTP/1.1 200 OK

Date: Sun, 13 Sep 2020 02:41:41 GMT

Server: Apache/2.4.18 (Ubuntu)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 3698

Keep-Alive: timeout=5, max=99

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

**请求报头**

请求报头通知服务器关于客户端求求的信息，典型的请求头有：

Host：请求的主机名，允许多个域名同处一个IP地址，即虚拟主机

这里host为 [www.csrflabelgg.com](http://www.csrflabelgg.com) 根据apache server的配置文件

对应本机的根目录 /var/www/CSFR/Elgg

User-Agent：发送请求的浏览器类型、操作系统等信息

这里看到，本机操作系统为ubuntu 浏览器为Firefox 60.0

Accept：客户端可识别的内容类型列表，用于指定客户端接收那些类型的信息

\*代表所有文件类型

Accept-Encoding：客户端可识别的数据编码

这里支持gzip和 deflate两种内容编码格式，似乎主流就这两种吧

Accept-Language：表示浏览器所支持的语言类型

支持美式英语 使用英语 q为权重系数,意义不明

Referer: 来源

请求来自当前目录

Connection：允许客户端和服务器指定与请求/响应连接有关的选项

Keep-Alive则表示保持连接。

**响应报头**

用于服务器传递自身信息的响应，常见的响应报头：

Server：包含可服务器用来处理请求的系统信息，与User-Agent请求报头是相对应的

这里是Apache 服务器

**实体报头**

实体报头用来定于被传送资源的信息，既可以用于请求也可用于响应。请求和响应消息都可以传送一个实体，常见的实体报头为：

Content-Type：用于定义网络文件的类型和网页的编码

application/json 和text/html代表一种文档格式 charset指字符集，这里用utf-8

Content-Encoding：gzip

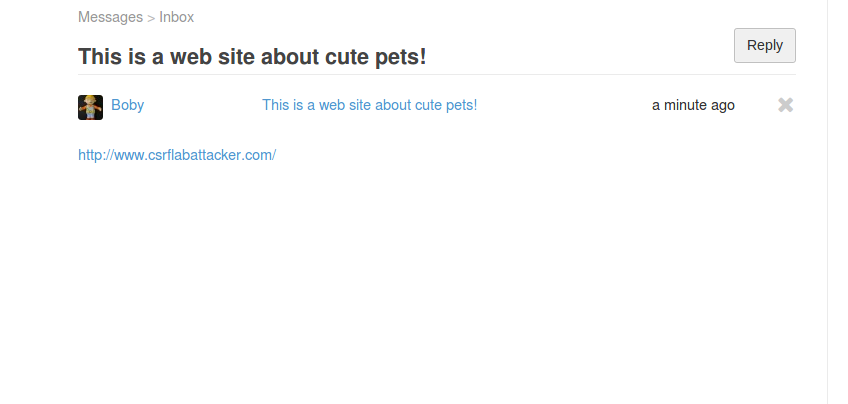
Expires：实体报头给出响应过期的日期和时间

Etag是 Entity tag的缩写，可以理解为“被请求变量的实体值”,通过客户端和服务器对比，可减少数据传输

Task2:

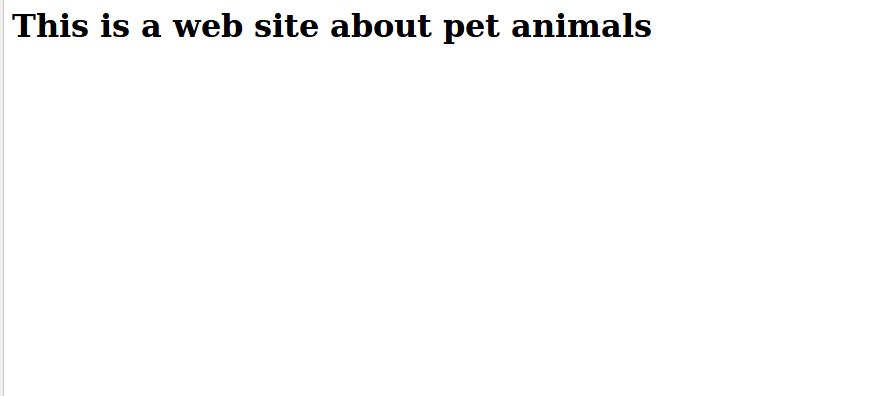
Bob给Alice发一个邮件，邮件里包括一个恶意网站链接，Alice好奇点入，进入网站后

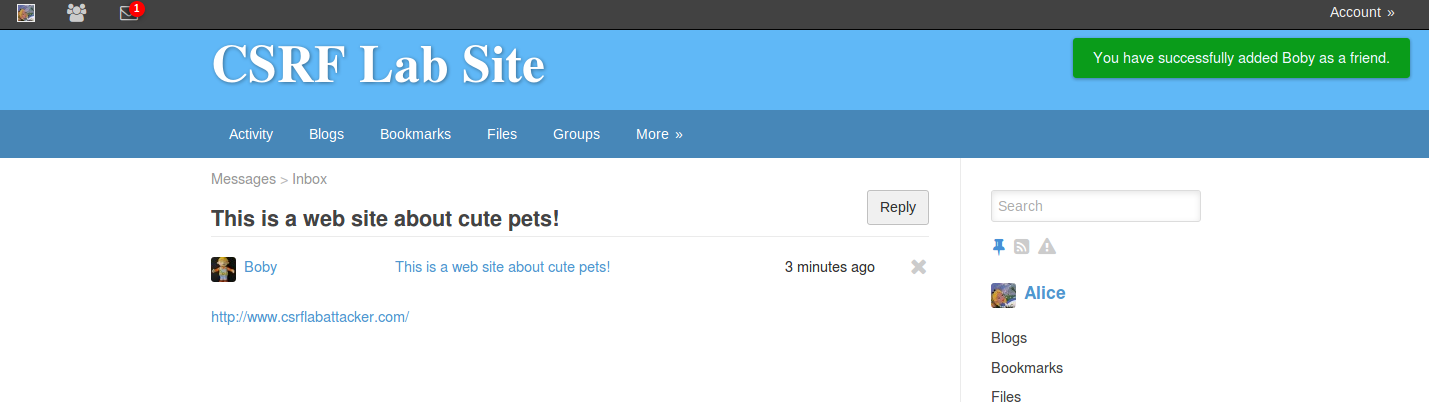
里面有一个很小的img，img会触法一个http get request,这个request 利用Alice浏览器上的cookie自动将Bob加为好友



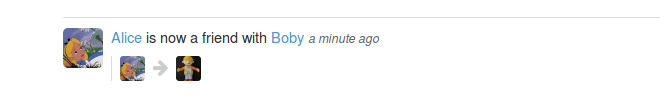
The source of the website







返回后如图Alice ???，asshole Boby

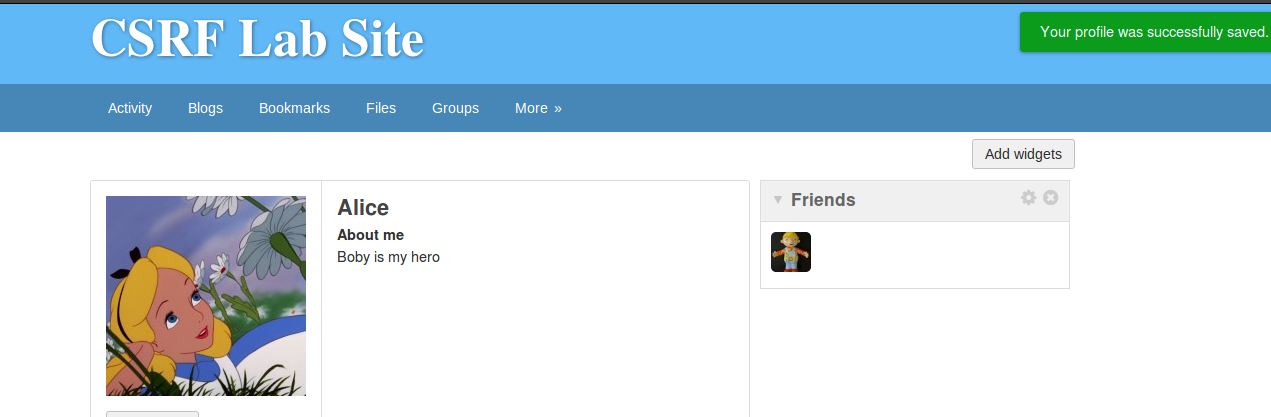


Task3:

根据Task1中Boby修改自己profile的post请求，修改适当参数Alice ：guid=42，通过JavaScript脚本修改Alice主页

将Task2中index.html改为以下代码





Q1：boby直到他可以通过添加或删除alice好友的操作，自己抓取http get request 来获得Alice的guid

Q2:可以，boby不知道其他用户的guid，但是可以通过大量随机测试，可能可以成功，用户名（name）方面，未必需要用自己名字,也可以达到攻击的效果.

Task4:



1. 出现没法跳转回去的现象，之前都是直接跳转到成功界面



2.在malicious site上反复发送post请求不成功，返回后提示



分析：\_elgg\_token是一个md5哈希值，由当前时间戳，user session id 和 随机字符串唯一指定，保证用户认证的唯一和隐秘。当Boby发起攻击时，没有进行token和时间戳的认证，当然也不可能知道token和ts，所以攻击被拒绝，只有alice本人登录账户运行http insector才能得到