A NEW-AGE TECHNIQUE OF PHISHING USING XSS

Negrilă Alexandru[1]

Introduction

Since internet appeared, information about us are not safe anymore. There are constantly persons who are trying to penetrate a system or to steal data about other people. Few of them want to demonstrate to themselves that they can but there are others that try to obtain money from hacking or stealing data.

In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Usually there is sent a spam to many email addresses with a fake email saying to update some information and leading to a phishing web page.

Phishing techniques

"***Social engineering***"consists in a URL that looks pretty same as the original URL. For example: HTTP://BANKSlTE.COM looks pretty same to HTTP://BANKSITE.COM actually it isn't, there is an "L" in the first site not an "I".

"**Browser vulnerability**" consists in a browser vulnerability that can spoof the TitleBar to show another URL than the original. This technique is browser targeted, not all browsers having the same vulnerability.

"**No TitleBar**" consists in a page that is not having a TitleBar, that not allowing the user to see the page location.

"**Pop-up**" consists in another window with no TitleBar that pops in front of the real page, allowing the real page URL to be displayed. It is usually used with **No TitleBar** technique to make the popped page to hide the address bar.

"**Man in the middle**" the attacker has access to a computer between the user and the real site. The attacker can sniff the traffic to a certain site or to make a fake page that saves all data the user send to a certain page and the user to believe that he sends data to the original page.

[1] Negrilă Alexandru, Student, Faculty of Computer Science for Business Management, Romanian-American University, Bucharest, email: madagent2005@yahoo.com

These are not all the techniques used today phishers use but they are the most known one and which affect many users.

What is XSS?

XSS means Cross Site Scripting and it was named also CSS but because of confusion with Cascading Style Sheet XSS was more frequently used and is now the standard name for Cross Site Scripting.

XSS allows a person that modifies an URL to inject script into a trusted site by modifying the page content. It is a lack of security on the website, the site showing unfiltered user input. It usually is found in forms like login and search where after an unsuccessful search the term that was searched is shown to the user.

Old-age technique of phishing using XSS

Yes, XSS has been used in the past too for phishing users. It was used for bypassing spam filters(as I wrote in the introduction too, the phishers use mass mailing to find their victims) and for masking the URL from the browser Status Bar and make a victim to click on the URL. After the URL was cliked the victim is sent to the official website but with an injected code inside that is sending the victim to the phishing site.

This technique had a huge impact when it first appeared and there has one today too(as major used sites that handle money such as PayPal and eBay are vulnerable to XSS). but if no other technique is used the possible victim can anytime see if that the phishing page is not a legit website just by looking to the address bar.

Of course, it can be used with a browser vulnerability, but as I wrote before not all people use same browser and not all browsers have the same vulnerability or have any known vulnerability at all.

Pop-up technique could be also used to fool a victim that it is a legit site site but it can be noticed by an average internet user even by mistake. The pop-up can be moved and the user can notice it is a fake page in front of the original page.

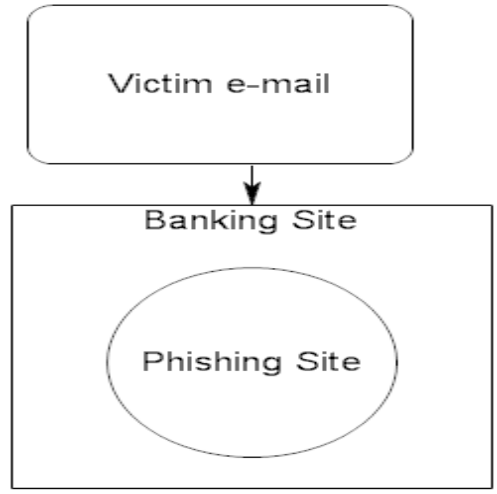
New-age technique of phishing using XSS

Presentation

The concept is the same as in the old-age technique. A vulnerable XSS site is injected with a malicious code that can force the page to make something that is wanted by the attacker.

A web page can include another web page, so using an XSS vulnerability an attacker can make a vulnerable web page to include a phishing or any malicious web page. That is the main concept over the new-age phishing technique.

The main key point of this is that the status bar from email will show that it's the legit site and the legit site will be shown in title bar too. So an average user can not know that is victim to phishing until it is too late and the phisher already used the stolen data and maybe not even then. The only way this can be noticed is by analyzing the source code and decoding the address bar URL, but even then, the it can't be found if the phisher can know how to hide his injection into the vulnerable site.



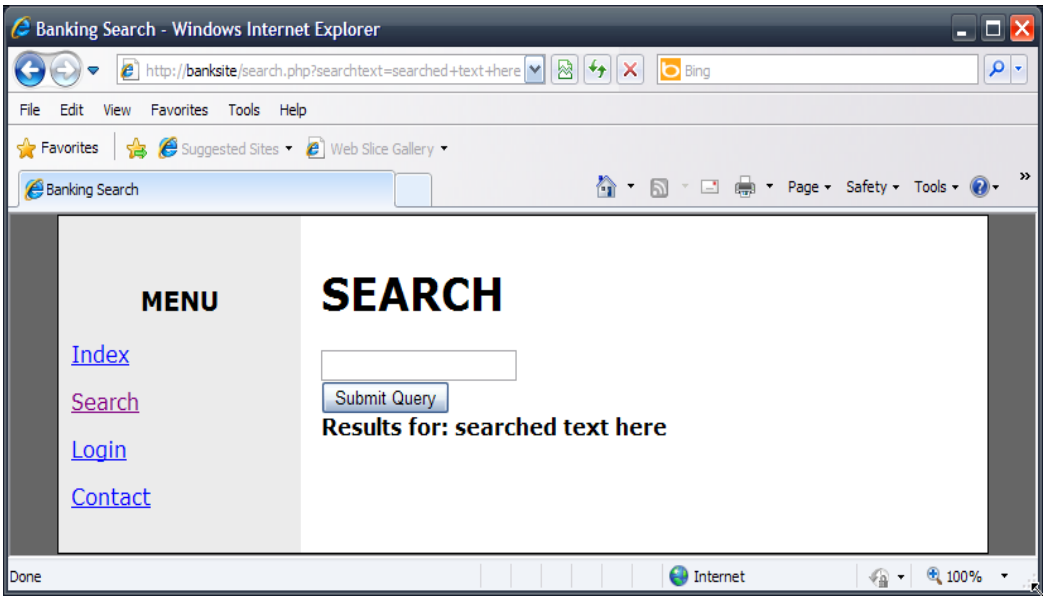
But how could a web page be included in other page? The simplest way for this is using frame or iframe. In the next part I will be using iframe to show this technique.

So everything should be simple. Well… it is not as simple as it looks. When this idea first came into my mind I tried frame, iframe and other techniques to include a page to a possible vulnerable site and everything went well, but that was just because it was a test page simply coded by me with a simple form and nothing more in it. In real life those kind of websites are rare and they represent no interest, so I coded a more complex testing page with a XSS vulnerability, but I noticed that every time I was trying to include a page with iframe it included it more than once(the user inserted text was shown more than once on the site) and there was something else than I was intending to happen.

The solution of this was to make something else invisible but the iframe and to set the frame to 100% width and height. This was done by using javascript, and it is a frequent technique used in AJAX site building.

Example

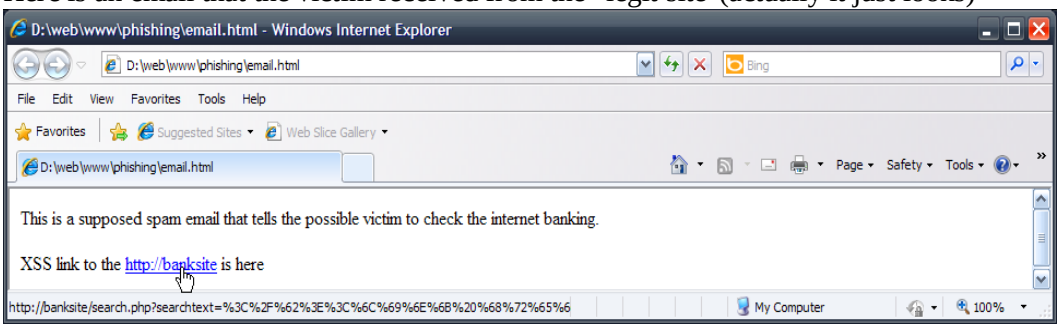
The vulnerable site looks like this:



And it has the following php code which the attacker wouldn't know if this wouldn't be an example but he found a XSS vulnerability and supposes that it should look something like this:

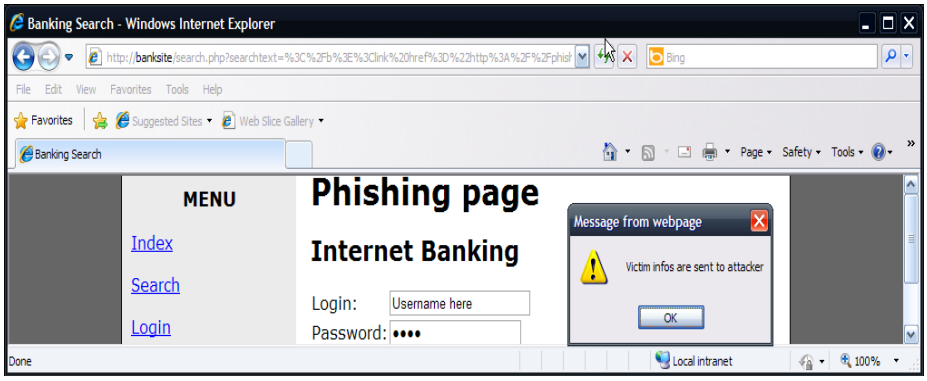
```
<?php

if (isset($_GET["searchtext"])) {
  echo "<b> Results for: ". $_GET["searchtext"] ."</b>";
 }
//MySQL code here
?>
```

Here is an email that the victim received from the "legit site"(actually it just looks)



Notice that the Status Bar is pointing to the real site. An average user do not analyze much a status bar link, some not even look at it. The full url looks like http://banksite/search.php?searchtext=%3C%2F%62%3E%3C%6C%69%6E%6B%20 but much longer and the part after http://banksite/search.php?searchtext= is just the injection HTML escaped. The HTML is encoded to prevent data loosing that may be caused by email provider, email client or browser.

The final page should look something like this:



Notice that there is a bank site link into the Title Bar

Fixes

As this is a server side vulnerability, it depends on how good the site is built. It's good that always secure inputs from the user even if the script is working with them or if they are shown back to the user. The user output can easy be secured with htmlentities(PHP) and HtmlEntityEncode(ASP) functions.