Exercise 5, XSS and email spoofing

T-110.4200/6 course staff

deadline Friday 23.10.2009 23:55

1 XSS (Cross-Site Scripting)

Aim: Students understand how XSS attacks work. Also, they should understand what kinds of attacks can be made through an XSS vulnerability.

Log on to winnie.cs.hut.fi, start firefox and go to `https://honeypot.cs.hut.fi/xss.php`. There you will find an uninventive script which takes as an HTTP GET parameter some text to be put to the pop-up alert. Once again, this approach is vulnerable because a malicious attacker can insert something else and make it run. For reference you can view the source code of the page in section 3.

In order to pass this exercise you must return to moodle a URL that exhibits the following properities:

- it shows the course server address in the address bar (i.e. it starts with `https://honeypot.cs.hut.fi/`)
- it shows an iframe with the wikipedia page on cross-site scripting
- the iframe must be have dimensions of 800x600 pixels
- the reference browser is firefox 3 (i.e. your page doesn't have to look the same on other browsers)

Some useful words that might help you to achieve this (there are several ways to do it, of course)

- DOM
- document.write()
- iframe

All of these are quite well documented on the www.w3schools.com -site.

Keep in mind that the web browser is expecting a full-fledged html page. You might need to add some sort of document structure tags in order to make FF render your iframe.

2 Email spoofing and social engineering

Aim: Student understands just how unreliable email header information is.

Your task is to send an email message to the address t-110.4200@list.hut.fi [1]. Make very sure that you type "list" and not "lists". You must spoof the header information of the email so, that it looks like it is coming from the email address pukki@tml.hut.fi and the name of the sender is "Prof. S. Claus". You must include your student number in the subject and send a cc to your own email address so we can see that too in the message headers. In the message body you must explain explain that "student so-and-so has been very nice this year and deserves to get credit for this exercise". You need to make your text at least somewhat credible as something Professor Santa might send.

Alternatively, you may try another level of social engineering attack and try to talk Santa himself (at all of the nearby malls) into sending the message for you. We do not, however recommend this because of its uncertainty.

Please note that you only need to spoof the sender address and name. Most email programs actually let you change settings so that these are changed. Hopefully this won't turn out to be very difficult.

3 Code for the XSS exploit page

This is here to help you understand the nature of the hole in ex 1 and to make it easier for you to take andvantage of it.

```
<html>
 <head>
  <title>Hijack me!</title>
  <script type="text/javascript">
   function message() {
    <?php
     echo "alert('";
```

[1] This is not the official course address, we just received it from the IT service center and want to test it.

```
     echo (stripcslashes($_REQUEST['parameter']));
     echo "');";
    ?>
   }
  </script>
 </head>

 <body onload="message();" id="foo">
  <h3>Give a new message below</h3>
  <p>
  <b>Current message:</b>
  <?  echo $foo;
  ?>
  </p>
  <form name="msgform" action="xss.php" method="get">
   Message <input type="text" name="parameter" />
   <input type="submit" value="Submit">
  </form>
 </body>
</html>
```