Lab 10: ZAP, XSS

Preliminaries

Refer to Lecture 11 slides.

Tasks

Turn on Kali VM, Metasploitable2 VM, and Win7 VM.

Log into Kali VM, and start Firefox. Log into Win7 as 'admin'. Then, complete the following tasks. Write your answers for all questions to your lab report.

1. Using ZAP to intercept and observe HTTP messages

Start ZAP, and configure Firefox to use ZAP as web proxy. Then, follow the ZAP Example 1 in Lecture 11 slides to go through all of its steps from (a) to (m).

1.1 In step (c), you capture a request message.
- (i) What's the URL requested in this message?
- (ii) Does this message have a body part?
- (iii) Grab a screenshot to prove your answer.

1.2 In step (e), you capture a Response message.
- (i) What are the names and values of the two cookies to be set by this message?
- (ii) This response message also redirects your browser to another page. What is this page?
- (iii) Grab a screenshot to prove your answer.

1.3 In step (f), you capture a second request message.
- (i) What's the URL requested in this message?
- (ii) What are the names and values of the two cookies carried by this message?
- (iii) Are these two cookies having the same names and values as the two captured in Task 1.2?
- (iv) Grab a screenshot to prove your answer.

1.4 In step (g), you capture a second response message.
- (i) Does this message have a body part?
- (ii) If so, use one sentence to describe what is contained in this body part.
- (iii) Why does not this message carry cookies?
- (iv) Grab a screenshot to prove no cookies.

1.5 In step (i), you capture a third request message.
- (i) What's the request method used in this message: GET or POST?
- (ii) Use one sentence to describe what is contained in the body part of this message.
- (iii) Grab a screenshot to prove your answer.

1.6 In step (j), you capture a third response message.
  (i) Does this message indicate that your login is successful?
  (ii) Why?
  (iii) Grab a screenshot to prove your answer.

1.7 In step (k), you capture a fourth request message.
  (i) What's the URL requested in this message?
  (ii) What are the cookie values contained in this message?
  (iii) Grab a screenshot to prove your answer.

1.8 In step (l), you capture a fourth response message.
  (i) Use one sentence to describe what's contained in the body part of this message.
  (ii) Grab a screenshot to prove your answer.

1.9 Click the 'History' tab to review the four pairs of request/response messages captured above. Why is the 'login.php' requested twice?

2. Using ZAP to modify HTTP messages

Follow the ZAP Example 2 in Lecture 11 slides to go through all of its steps from (a) to (j).

2.1 In step (a):
  (i) How many pairs of request/response messages are captured during the process of changing the security level (i.e., interacting with security.php)?
  (ii) Grab a screenshot to prove your answer.

2.2 In step (e):
  (i) Why are there no cookies in the captured GET message?
  (ii) Grab a screenshot to prove no cookies.

2.3 In step (g), you insert the saved cookie header in step (b) into the captured GET message. Grab a screenshot to show your insertion.

2.4 In step (j), you should notice that you obtain a logged-in HTTP session with Security Level being 'low'.
  (i) Grab a screenshot to prove this.
  (ii) Explain why you can achieve this.

3. Stored XSS

For each task below, you should include the following into your lab report:

- Your crafted input for the 'Message' field
- A screenshot about the IE browser at Win7 VM to prove your success.

Note: Your crafted inputs should be different from the ones given in the lecture slides. Any difference will be OK (e.g., you can change the alert message, the image file name, etc), no matter how small it is. Try to make it as big as you can. To achieve this, you need to understand all lecture slides thoroughly first.

3.1 Set Firefox to use 'No Proxy'. Follow the Stored XSS Example 1 in Lecture 11 slides to generate an alert box.
   (i) Crafted input:
   (ii) Screenshort:

3.2 Follow the Stored XSS Example 2 in Lecture 11 slides to retrieve cookies.
   (i) Crafted input:
   (ii) Screenshot:

3.3 Follow the Stored XSS Example 3 in Lecture 11 slides to send stolen cookies to a web server you set up to display them. Specifically, you should use a crafted guestbook message which includes JS code to report the cookies of a web session to the SimpleHTTPServer you set up. You should then use the IE browser at Win7 to view the guestbook, and have the cookies for this new web session reported to the SimpleHTTPServer.
   (i) Crafted input:
   (ii) Command line to set up the SimpleHTTPServer:
   (iii) Screenshot for the cookies from IE reported at SimpleHTTPServer:

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.