CS 332: Ethical Hacking

Study Guide for the Final Exam

1 The Labs

SQL Injection Attack Lab. In the context of SQL Injection, what's the difference between SELECT and UPDATE statements?

SQL Injection Attack Lab. We only need one VM to perform every task in this lab, but in reality, the web server and the web client are located in two different machines. And if we do want to complete this lab lesson with two VMs, what changes do we need to make?

SQL Injection Attack Lab. In this lab, we used Apache as the web server. What are the other famous web server software?

SQL Injection Attack Lab. We hosted several websites on the same virtual machine, like one website for the SQL injection attack lab, one website for the CSRF attack lab, and one website for the XSS attack lab. Which feature in the Apache software allows us the achieve this goal - hosting multiple web sites on one machine.

SQL Injection Attack Lab. In the context of computer security, what does CIA stand for? Which of these CIA properties could be compromised by a successful SQL injection attack?

SQL Injection Attack Lab. Describe whether or not the password minder and Ellen's minder protector, as well as that minder protector minder, would protect your password from SQL injection attacks. And why? (see Ellenshow: Out of Your Password Minder:
https://www.youtube.com/watch?v=Srh_TV_J144;)

SQL Injection Attack Lab. In this lab, the server's source code has this line: $hashed\_pwd = sha1$(input_pwd); this line will encrypt the password. Explain: Is this encryption sufficient to protect you against SQL injection attack.

SQL Injection Attack Lab. Explain why in lab task 2.3, the attack fails.

SQL Injection Attack Lab. Explain how prepared statements can prevent SQL injection attacks.

Cross Site Request Forgery Attack Lab. SQL injection, CSRF, and XSS, which one is attacking the web server, which one is attacking the web client?

Cross Site Request Forgery Attack Lab. Explain how tokens can prevent CSRF attacks.

Cross Site Request Forgery Attack Lab. Explain why in this lab we used the firefox add-on "HTTP Header Live".

Cross Site Request Forgery Attack Lab. CSRF attacks using GET requests, or using POST requests, which one is more dangerous (i.e., cause more severe damage)?

Cross Site Request Forgery Attack Lab. In lab task 3, if Boby would like to launch the attack

to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile? Please explain.

Cross Site Request Forgery Attack Lab. The CSRF attack we did in this lab is based on a social media network websites, in which the vulnerability allows attackers to add someone as a friend without the victim's knowledge, or update the victim's profile page without the victim's knowledge. Describe with an example how CSRF vulnerabilities would affect other types of websites.

Cross Site Scripting Attack Lab. Describe what problem the Samy worm caused back in 2005.

Cross Site Scripting Attack Lab. Why would attackers be interested in stealing someone's cookies?

Cross Site Scripting Attack Lab. Explain the difference between reflected XSS attack and persistent XSS attack. The attack in lab task 4, is it a reflected XSS attack, or is it a persistent XSS attack? The attack in lab task 5, is it a reflected XSS attack, or is it a persistent XSS attack?

Cross Site Scripting Attack Lab. HTML defines many elements, what element is needed for an XSS attack?

Cross Site Scripting Attack Lab. In lab task 4, what is the sendurl supposed to be? Should it be the same sendurl as in task 5?

Cross Site Scripting Attack Lab. In lab task 5, why did we need such a line:
"if(elgg.session.user.guid!=samyGuid)".

Cross Site Scripting Attack Lab. XSS attack works only if your browser supports Javascript. So why don't people disable javascript in their browsers?

Cross Site Scripting Attack Lab. Describe what is self-propagating XSS worm.

Cross Site Scripting Attack Lab. On any website (e.g., Google, Facebook, Twitter), if the web page allows you to type in something, what would you type in so as to find out if the web site is vulnerable to XSS attack or not.

Cross Site Scripting Attack Lab. Why cross site scripting is NOT called CSS, but is called XSS?

2 The Slides

1. What's the difference between static web pages and dynamic web pages?
2. What's the difference between http requests and http responses?
3. What's the difference between http get and http post requests?

4. Which of the cookie attributes is used for defending against XSS attacks?

5. What is the "secure" cookie attribute used for?

6. Describe why input validation is important from security's perspective.

7. Describe the difference between HTTP and HTTPS. Which port is by default used by HTTPS? which port is by default used by HTTP?

8. Besides SQL injection, CSRF, XSS, name one more famous vulnerability included in the OWASP top 10 list, and briefly explain it.