CSCI 345 – Homework

XSS, SQL Injection, & TCP/IP stack

1. TCP/IP stack (5 pts)
   Complete the following GENI experiment: https://witestlab.poly.edu/blog/tcp-ip-protocol-stack/.
   There is an exercise at the end of this webpage. Submit this exercise in place of your experiment report.

2. XSS and SQL Injection (10 pts)
   a. For this assignment you will use the OWASP Juice Shop Project, an intentionally vulnerable e-commerce website.
   b. Use Docker for your installation – the goal is to learn about containers!
      https://github.com/bkimminich/juice-shop#setup
   c. You will need to perform the tasks listed below. There will be hints for each task:
      i. **Perform a reflected XSS attack with <script>alert("XSS1")</script>**
         Background: Reflected Cross-site Scripting (XSS) occur when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself; it is non-persistent and only impacts users who open a maliciously crafted link or third-party web page. The attack string is included as part of the crafted URI or HTTP parameters, improperly processed by the application, and returned to the victim.
         Hints
            1. Look for an input field where its content appears in the response HTML when its form is submitted.
            2. Try probing for XSS vulnerabilities by submitting text wrapped in an HTML tag which is easy to spot on screen, e.g. <h1> or <strike>.
      ii. **Access the administration section of the store.**
         Hints
            1. Knowing it exists, you can simply guess what URL the admin section might have.
            2. Alternatively, you can try to find a reference or clue within the parts of the application that are not usually visible in the browser.
      iii. **Perform a persistent XSS attack with <script>alert("XSS2")</script> bypassing a client-side security mechanism.**
         Background: This challenge is founded on a very common security flaw of web applications, where the developers ignored the following golden rule of input validation: **Be aware that any JavaScript input validation performed on the client can be bypassed by an attacker that disables JavaScript or uses a Web Proxy. Ensure that any input validation performed on the client is also performed on the server.**
         Hints
            1. There are only some input fields in the Juice Shop forms that validate their input.
2. Even less of these fields are persisted in a way where their content is shown on another screen.
3. Bypassing client-side security can typically be done by either disabling it on the client (i.e. in the browser by manipulating the DOM tree) or by ignoring it completely and interacting with the backend instead.

iv. *Order the Christmas special offer of 2014.*
To solve this challenge you need to order a product that is not supposed to be available any more.

Hints
1. Find out how the application hides deleted products from its customers.
2. Try to craft an attack string that makes deleted products visible again.
3. You need to get the deleted product into your shopping cart and trigger the Checkout.

v. *BONUS POINTS: Retrieve a list of all user credentials via SQL Injection (3 pts)*
This challenge explains how a considerable number of companies were affected by data breaches without anyone breaking into the server room or sneaking out with a USB stick full of sensitive information. Given your application is vulnerable to a certain type of SQL Injection attacks, hackers can have the same effect while comfortably sitting in a café with free WiFi.

Hints
1. Try to find a page where you can influence a list of data being displayed.
2. Craft a UNION SELECT attack string to join data from another table into the original result.
3. You might have to tackle some query syntax issues step-by-step, basically hopping from one error to the next.

What to submit: a report with a short description of your thinking process and a screenshot of the successful result for each challenge. *If you do not complete a challenge, describe your work and thought process for partial credit.*


Your goal with the security review assignment is to evaluate the potential security and privacy issues with new technologies, evaluate the severity of those issues, and discuss how those technologies might address those security and privacy issues. These assignments should reflect deeply on the technology that you're discussing, and should therefore be significantly longer than your current events assignments.

Each security review should contain:

- Summary of the technology that you're evaluating. You may choose to evaluate a specific product (like the Miracle Foo) or a class of products with some common goal (like the set of all implantable medical devices). This summary should be at a high level, around one or two paragraphs in length. State the aspects of the technology that are relevant to your observations below. If you need to make assumptions about a product, then it is extremely important that you state what those assumptions are. To elaborate on the latter, if you end up making assumptions about a product like the Miracle Foo, then you are not studying the Miracle Foo
but "something like the Miracle Foo," and you need to make that extremely clear in your review.

- State at least two assets and, for each asset, a corresponding security goal. Explain why the security goals are important. You should produce around one or two sentences per asset/goal.
- State at least two possible threats, where a threat is defined as an action by an adversary aimed at compromising an asset. Give an example adversary for each threat. You should have around one or two sentences per threat/adversary.
- State at least two potential weaknesses. Again, justify your answer using one or two sentences per weakness. For the purposes of these security reviews, you don't need to fully verify whether these potential weaknesses are also actual weaknesses. (You may find some overlap with your answer here and your answer to the bullet above.)
- State potential defenses. Describe potential defenses that the system could use or might already be using to address the potential weaknesses you identified in the previous bullet.
- Evaluate the risks associated with the assets, threats, and potential weaknesses that you describe. Informally, how serious do you think these combinations of assets, threats, and potential weaknesses are?
- Conclusions. Provide some thoughtful reflections on your answers above. Also discuss relevant "bigger picture" issues (ethics, likelihood the technology will evolve, and so on).