Code Injection Questions
IN618 Security

Introduction

Over the past few weeks we have examined a variety of somewhat related *code injection* vulnerabilities in web applications. Research and answer the follwoing questions to demonstrate your understanding of these topics. Note that some of the question are likely to require some online research beyond what was directly discussed in class.

Note that you are free to discuss these questions with other classmates, but the responses you submit must be your own writing. This is not a formal writing assignment so it is not necessary for you to fully cite all your sources, but you should cite any source that was especially good or that you used heavily.

Questions

1. In a cross site scripting attack it is the user's browser that is exploited. The vulnerable web application serves as an attack vector to reach the user's browser. Explain why this is true.
2. I commented in class (without particulary explaining why) that if a web application is vulnerable to cross site scripting, then it is also vulnerable to cross site request forgery. Explain why this is true.
3. Suppose you build a web site on which a user can "like" items posted on the site. How might an attacker use cross site request forgery to surreptitiously generate fake likes? How would use of an anti-forgery token work to prevent this?
4. How does the use of prepared SQL statements prevent SQL injections? E.g., why doesn't injecting code like `x'; DROP TABLE users;` – do any harm when it's used with prepared statements?

Submission requirements

Write your responses to these questions using a word processor or similar tool of your choice and submit a **hard copy** of your document by the second class session next week.