Introduction to Cryptography and Software Security
Problem Set 4: Web Security

Due date: 30/5/2019

Please provide your solution by choosing the correct answer for each question and completing the on-line quiz.

1. SQL injection often allows an attacker to do which of the following?
   - Access information he should not be able to access.
   - Overrun a buffer to smash the stack.
   - Cause memory to be used after it has been freed.
   - All of the above.
2. If you had to summarize the key (most specific) programming failure with SQL injection, it would be:
   - Bypassing authentication.
   - Overflowing a buffer.
   - Trusting without verifying.
   - Circumventing the same origin policy.
3. What is escaping an example of?
   - Validation.
   - Whitelisting.
   - Blacklisting.
   - Sanitization.
4. Suppose a web application implements authentication by constructing an SQL query from HTML from data **using PHP's prepared statements**. What would happen if an attacker entered `FRANK' OR 1=1;) --` in the web form's user field?
   - The application will try to authenticate a user whose name is `FRANK' OR 1=1;) --`.
   - The text will be confused as the password and authentication will probably fail.
   - The text will corrupt the query structure and the database will view it as a syntax error.
   - The text will modify the structure of the SQL query and possibly bypass authentication.
5. Suppose a browser submits a GET request to `http://www.mybank.com/accountinfo` on February 20th 2015. Which of the following cookies, if already stored at the browser, would be sent with the request?
   - `sessid=ABCDEFG; expires=Sat, 21-Feb-2015; path=/; domain=.mybank.com`
   - `prefs=small:blue:refresh; expires=Sat, 1-Aug-2015; path=/specialoffers/; domain=.mybank.com`
   - `lang=us-english; expires=Sat, 1-Aug-2015; path=/accountinfo/; domain=.fidelity.com`

We thank Prof. Michael Hicks (UMD) and Coursera for generously sharing some of their teaching resources with us.

- `edition=us; expires=Wed, 18-Feb-2015; path=/; domain=.mybank.com`

6. `<script> </script>` tags in HTML pages most often identify programs written in what language?
   - PHP.
   - Javascript.
   - C.
   - Java.
7. The browser implements security for Javascript programs for what reason?
   - It does not – these programs are only used to render dynamic content but are otherwise not security-relevant.
   - Such programs could deny service by running forever.
   - It does not – Javascript programs run at the server so the browser can ignore them.
   - Such programs may access browser-controlled resources, which include potentially sensitive data in HTML documents and cookies.
8. XSS subverts what policy?
   - Same origin.
   - Availability.
   - Secure defaults.
   - Whitelisting.
9. What is the difference between stored (or persistent) XSS and reflected XSS?
   - Stored XSS is amenable to blacklisting but reflected XSS is not.
   - Stored XSS embeds Javascript in a URL, while reflected XSS embeds it in a mirrored site.
   - Stored XSS works on database queries while reflected XSS works on cookies, which are received from and reflected back to the server.
   - Stored XSS works by injecting code in a site's served content, while reflected XSS injects code in a URL.