JavaScript, Sixth Edition

Chapter 9 Solutions

Short Quiz 1

1. How do you reference a passed query string in your code?

The search property of the Location object contains a URL’s query or search parameters.

1. How is data in a query string separated from a URL? How are individual name-value pairs distinguished within a query string?

A query string is separated from a URL with the ? character.

Individual name-value pairs are separated within a query string by the & character.

1. How is a hidden form field different from other form fields?

A hidden form field is not displayed by web browsers and, therefore, allows developers to hide information from users. Hidden form fields temporarily store data that needs to be sent to a server along with the rest of a form, but that a user does not need to see.

Short Quiz 2

1. What are the two main types of cookies? What is the difference between them?

Cookies can be temporary or persistent. Temporary cookies remain available only for the current browser session. Persistent cookies remain available beyond the current browser session and are stored in a text file on a client computer.

1. How do you delete a cookie in your code?

To delete a cookie, you must set its expiration to a date in the past.

1. What are some advantages of using Web Storage rather than cookies? Why might a developer choose to continue using cookies?

Creating, reading, and removing cookies requires complex code that’s not always straightforward. In addition, all cookies are sent to the server with each HTTP request. Storing and reading data with Web Storage is much more straightforward than using cookies.

Because Web Storage is not supported by a number of older browser versions, cookies are still the standard for storing information on the client about a user’s interactions with a web server.

Short Quiz 3

1. What is a code injection attack?

JavaScript code on a web page that is not written securely is vulnerable to a code injection attack, in which a program or user enters JavaScript code that changes the function of the web page. For instance, a malicious program could open a web page containing a form and enter JavaScript code in one of the form fields designed to retrieve sensitive information from the server. Such a program could then relay this information to a person other than the owner.

1. What is the same origin policy?

Under the same origin policy, windows and tabs can view and modify the elements and properties of documents displayed in other windows and tabs only if they share the same protocol (such as HTTP) and exist on the same web server.

1. What is a third-party script? How do you include one in a web document?

A third-party script is a script from another domain that you want to run on your web pages.

To enable a third-party script in a web document, you simply include a script element with a src value pointing to the third-party content. The same origin policy limits scripts to those referenced by HTML documents from the original web server; this enables web pages to use third-party scripts.

# Review Questions

1. HTTP was originally designed to be \_\_\_\_\_\_\_\_\_\_, which means that web browsers stored no persistent data about a visit to a web site.
   1. hidden
   2. encrypted
   3. stateless
   4. stateful
2. What character is used to separate individual name-value pairs within a query string?
   1. &
   2. $
   3. ?
   4. %
3. To concatenate names and values into a query string, you can use methods of the \_\_\_\_\_\_\_\_\_\_ class.
   1. Array
   2. String
   3. Number
   4. Date
4. The \_\_\_\_\_\_\_\_\_\_ method of a form automatically creates a query string from its field values.
   1. reset
   2. change
   3. click
   4. submit
5. Which type value for the input element creates a field that is not displayed by web browsers?
   1. hidden
   2. invisible
   3. none
   4. text
6. Which is the only required attribute of the cookie property?
   1. path
   2. domain
   3. expires
   4. name
7. You can use special characters in your cookies if you use \_\_\_\_\_\_\_\_\_\_.
   1. secure coding
   2. encoding
   3. a CDN
   4. the secure attribute
8. Cookies created without a(n) \_\_\_\_\_\_\_\_\_\_ attribute are available for the current browser session only.
   1. path
   2. domain
   3. expires
   4. name
9. Which function do you use as part of the process of parsing a cookie?
   1. encodeURI()
   2. decodeURI()
   3. encodeURIComponent()
   4. decodeURIComponent()
10. To delete cookies in your code, you change the value of which cookie attribute?
    1. path
    2. domain
    3. expires
    4. name
11. Which property of the Web Storage API do you use to store data that remains until you run code to delete it, similar to persistent cookies?
    1. localStorage
    2. sessionStorage
    3. persistentStorage
    4. webStorage
12. Which method do you use to delete a specific item from Web Storage?
    1. clear()
    2. getItem()
    3. removeItem()
    4. setItem()
13. Your first line of defense in securing your JavaScript programs is to \_\_\_\_\_\_\_\_\_.
    1. require a login for every user
    2. validate all user input
    3. encode all data
    4. restrict access to a single subdomain
14. An attack in which a program or user enters JavaScript code that changes the function of a web page is known as a(n) \_\_\_\_\_\_\_\_\_\_ attack.
    1. code injection
    2. secure coding
    3. cross-site
    4. SSL
15. It’s important to \_\_\_\_\_\_\_\_\_\_ characters in form field values that could be part of malicious code, which involves converting the characters to their character code equivalents.
    1. encrypt
    2. decrypt
    3. encode
    4. escape
16. Why should a password never be stored in a cookie?

Cookies are stored on a user’s computer as plain text files. If a user’s computer is infected with malware, any data, including the contents of cookies, is vulnerable to being stolen and used fraudulently by a third party.

1. What is the difference between temporary and persistent cookies?

Temporary cookies remain available only for the current browser session. Persistent cookies remain available beyond the current browser session and are stored in a text file on a client computer.

1. Explain how to modify an existing cookie.

To modify an existing cookie, you simply assign a new name-value pair to the document.cookie property. If the name-value pair already exists it will be overwritten.

1. Describe one advantage and one disadvantage of using Web Storage rather than cookies.

Creating, reading, and removing cookies requires complex code that’s not always straightforward. In addition, all cookies are sent to the server with each HTTP request. However, Web Storage is not supported by a number of older browser versions.

1. Explain what a code injection attack is, and one step you can take to prevent such attacks.

JavaScript code on a web page that is not written securely is vulnerable to a code injection attack, in which a program or user enters JavaScript code that changes the function of the web page. For instance, a malicious program could open a web page containing a form and enter JavaScript code in one of the form fields designed to retrieve sensitive information from the server. Such a program could then relay this information to a person other than the owner.

Validating forms before submission is an important part of preventing injection attacks. In addition, it’s important to escape characters in form field values that could be part of malicious code, which involves converting the characters to their character code equivalents, as you do when URL encoding cookie data. For form input, escaping is generally performed by the web server before processing user input.

# Case Projects

## Individual Case Project

Enhance the personal website you’ve created in the preceding chapters of this book to prevent security issues. To do this, review each form field in your site and identify any additional validation that you could reasonably add. In particular, look for situations where you could use a regular expression to limit the allowable characters in order to exclude characters used in creating JavaScript code. Use word-processing software to create a table like Table 9-4, which includes an example. Add a row for each form field in your website.

|  |  |  |  |
| --- | --- | --- | --- |
| **filename** | **field label** | **validation performed before submission** | **validation left to web server** |
| index.htm | Zip | Numbers and hyphen only  no more than 10 digits | Verifying that Zip value is appropriate for provided State value |

**Table 9-4: Table for planning additional validation**

When you’ve reviewed each field in your website, add the validation described in your table. Test each field until you’re satisfied with your new validation code.

**Grading Rubric:**

Each student should submit a completed table like the one in Table 9-4 that includes potential security and validity issues relevant to any forms in their individual website. Each student should also submit a revised version of their individual website in which each of these issues has been addressed.

## Group Case Project

Have each group member present the table and website from their Individual Case Project to the group. When presenting your website, solicit feedback from other group members regarding additional validation that you could add to your site, and discuss as a group the pros and any cons of the suggested enhancement. After all group members have presented their sites and received feedback, implement any suggestions for your site that your group generally felt would be good additions.

**Grading Rubric:**

Students should be able to list the additional validation issues highlighted by group members, as well as some pros and cons for each. Their individual websites should reflect revisions that implement any of these suggestions that their group felt were advisable.