Information Security Animations – Web Application Security (Script)

What is Web Application?

Web application is a series of programs executed on a web server. The server is connected to a backend database. It responds to client’s requests from dynamic webpages via Hypertext Transfer Protocol (HTTP) to provide cross-platform services on the Internet and intranet. For instance, in an electronic transaction, the user inputs information including the credit card number on the webpage, and completes the transaction.

Security Threats to Web Applications

Since web applications are usually connected to the Internet or intranet, users can utilise the resources provided by the system and enhance work efficiency. However, web applications also bring about certain security threats.

Generally, security threats to web applications originate from:

1. Untrustworthy client
   A web application usually cannot monitor the operation of its clients. Therefore the application should not be designed to fully trust and directly process the data inputted by clients.

2. Security loopholes in the application design
   Attackers will launch attacks targeting security loopholes in the design of the web application.
   
   The most typical attacks include code injection attack, cross site scripting attack (XSS), etc.

3. Insecure network communication
   If the web application communicates unencrypted information with its clients via the Internet or other insecure networks, such information can be intercepted and altered during transmission.

Security Measures

In designing web applications, organisations should adopt appropriate security measures to mitigate
security risks. In general, security measures can be categorised as follows:

(1) **Web application security architecture**

The typical web application architecture contains three tiers, the external web server, the application server, and the database server. With such a tier-based architecture, even if an attacker can intrude the external web server, he still has to find ways to attack the internal network. The external web server should be placed within a demilitarised zone (DMZ) which is a special network segment containing servers with access to Internet services. Servers storing sensitive information should be located in the internal network with additional protection.

(2) **Web server software security guideline**

Website system administrators should configure web servers securely and assign access rights in accordance with the web server software security guideline. For example, avoid using privileged accounts (e.g. "root", "SYSTEM", "Administrator") to run web server processes so that the web server software cannot modify unauthorised system files. In addition, take appropriate precautionary measures such as using secure sockets layer (SSL), etc. to encrypt the transmitting data.

(3) **Web application development process**

The security controls of web applications should be analysed and defined during the early stages of software development. For instance, perform source code review to identify security bugs that were overlooked during the development stage. Risk assessment will also help reduce common security loopholes.

(4) **Web application secure coding**

Software development teams should follow a set of web application secure coding practices, for instance, validate all input parameters and filter special characters such as ~!#$%^&*()<> to
prevent attacks of code injection and cross site scripting (XSS) effectively.

**Quiz**

Please select the correct answer.

1. Which of the following security threat will happen to web applications?

   A) Untrustworthy client
   B) Security loopholes in the web application design
   C) Insecure network communication
   D) All of the above [Correct]

2. Can attacks of code injection and cross site scripting be prevented by validating all input parameters and filtering special characters?

   A) Yes [Correct]
   B) No

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk