Offensive Approach to Hunt Bugs

Parameter Tampering

Background Concept about Parameter Tampering

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

Background Concept about Parameter Tampering

Example 1

The parameter modification of form fields can be considered a typical example of Web Parameter Tampering attack.

- For example, consider a user who can select form field values (combo box, check box, etc.) on an application page. When these values are submitted by the user, they could be acquired and arbitrarily manipulated by an attacker.

Background Concept about Parameter Tampering

Example 2

<input type=”hidden” id=”1008” name=”cost” value=”70.00”>

- In this example, an attacker can modify the “value” information of a specific item, thus lowering its cost.

Background Concept about Parameter Tampering

Example 3

http://www.attackbank.com/default.asp?profile=741&debit=1000

- In this case, an attacker could tamper with the URL, using other values for profile and debit:

  http://www.attackbank.com/default.asp?profile=852&debit=2000