Validated Transaction

(Mini-Pattern)

Abstract

The *Validated Transaction* pattern puts all of the security-relevant validation for a specific transaction into one page request. A developer can create any number of supporting pages without having to worry about attackers using them to circumvent security. And users can navigate freely among the pages, filling in different sections in whatever order they choose. The transaction itself will ensure the integrity of all information submitted.

Problem

Web applications often have to collect a great deal of data from a user in order to complete a single transaction. E-commerce purchases, for example, require that a user to select items for purchase, provide contact information and a shipping address, choose shipping options, and submit credit card information. Rather than simply present the user with a huge form with a bewildering array of options, most sites prefer to guide the user through the process, validating each piece of data as it is provided.

This approach can be vulnerable to attacks. An attacker can use known URLs to jump between the different pages, in attempt to bypass some of the data validation checks. For example, if the application developer is not extremely careful, it may be possible for the attacker to add items to the order after having paid.

Solution

The *Validated Transaction* pattern solves this problem by establishing a single point at which the transaction is committed. At that point, any data validation checks are duplicated in order to ensure that data tampering will be discovered. Furthermore, data consistency checks are also implemented at that point.

This pattern can be used to retrofit an application that was not designed with security in mind. Alternately, it allows developers of the application to make changes to the application, safe in the knowledge that the *Validated Transaction* pattern offers a safety net against security problems.

Related Patterns

- *Client Input Filters* – a related pattern that can use this validated transaction mechanism to enforce that client input is validated.

- *Directed Session* – a complementary pattern that exposes a single URL to the user and enforces form validation by storing the actual URL in session data.

References

None.