Securing your web application with deep HTTP understanding

Or Katz, 2011-12-10

Securing your web application is not an easy job. In this blog post I will explain some of the challenges in protecting a web application and how F5 Application Security Manager (ASM) can help mitigate security risks.

HTTP is a flexible protocol that allows clients (browsers in this case) to communicate with servers (web applications) passing information back and forth. The information can be delivered in many ways, and it is up to the application developer to decide how it will be done. For example, information can be delivered by using:

1. Quary based HTTP parameters
2. Content based HTTP parameters (POST)
3. Content based HTTP parameters (MulitPart data)
4. XML content
5. JSON content
6. HTTP Header

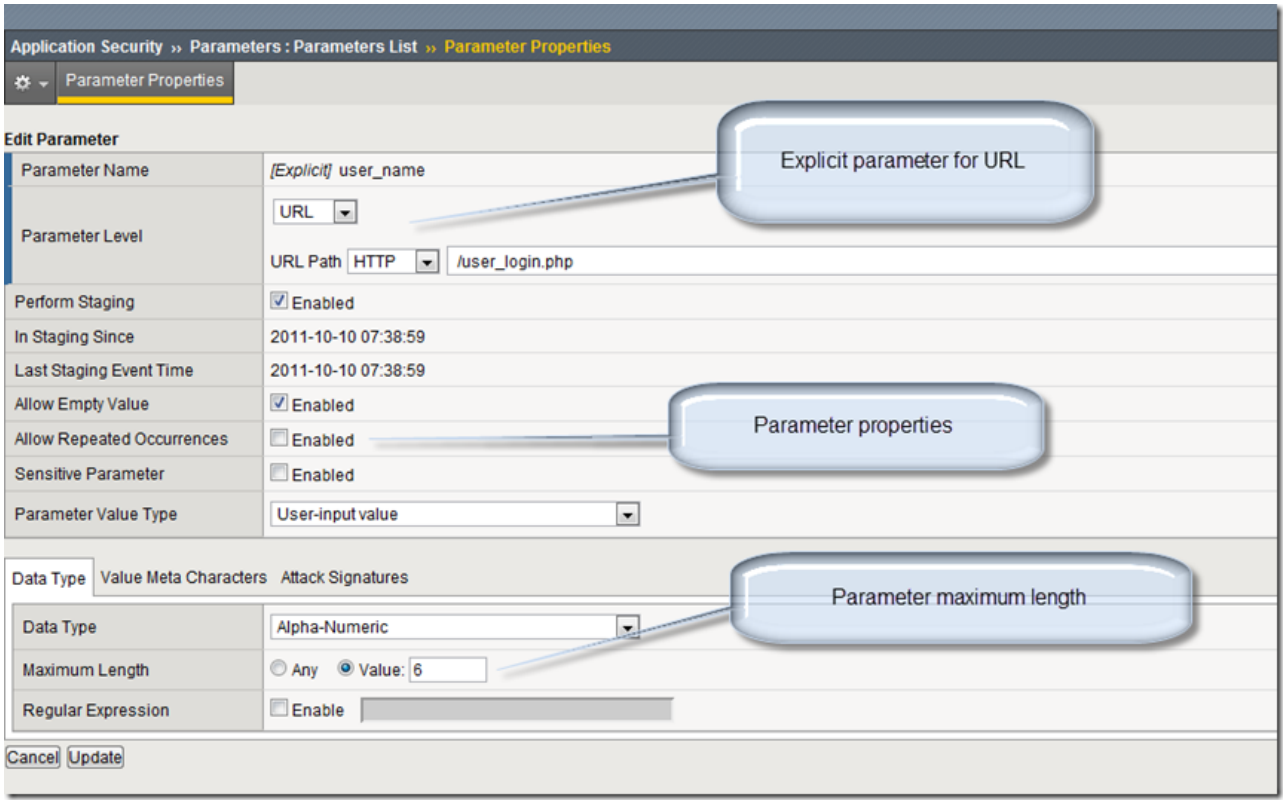
From the application security point of view, looking at the HTTP request as one big chunk of data is not acceptable. Having a fine-tuned security policy should be the right approach due to the following reasons:

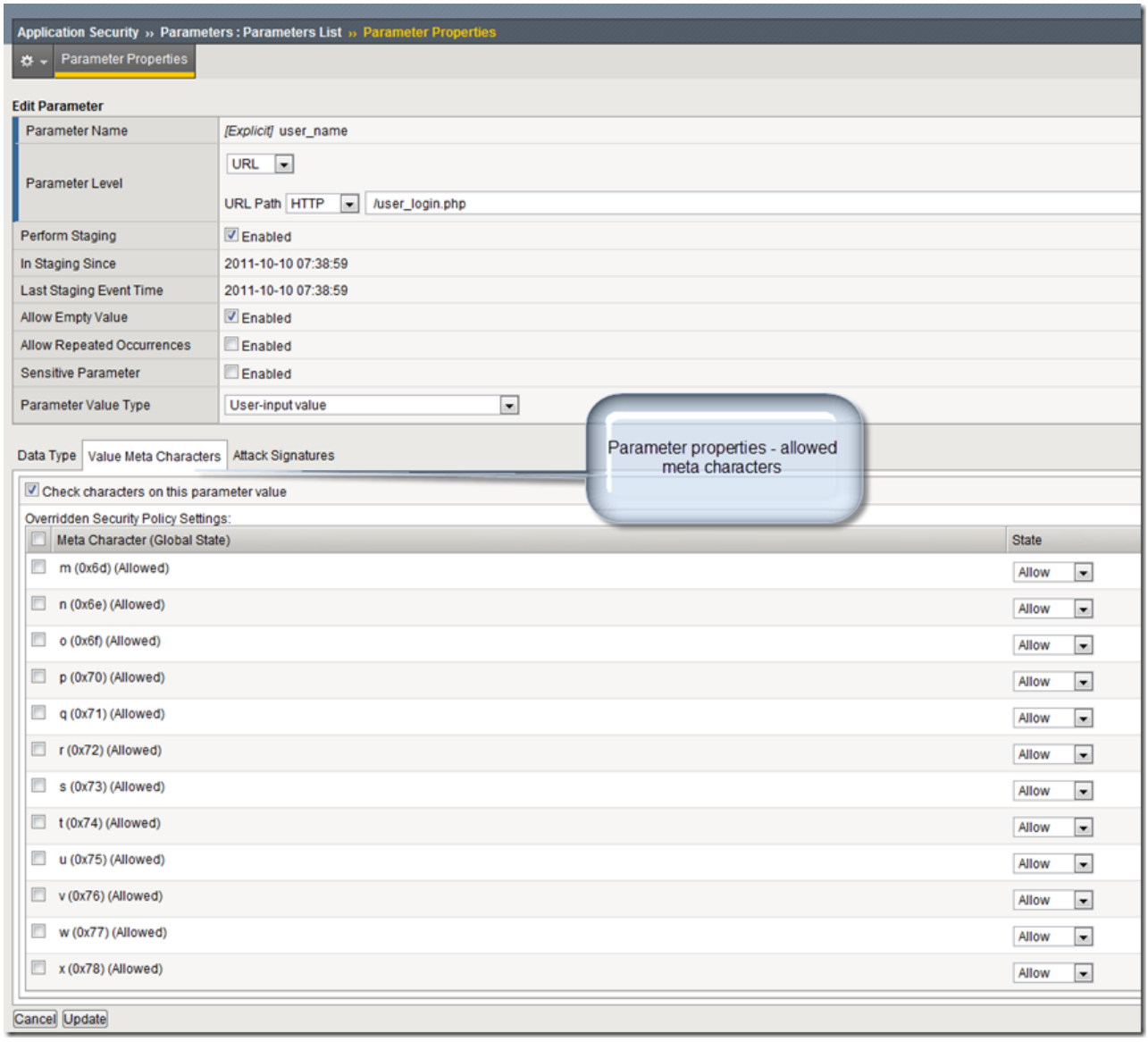
1. Securing each HTTP data object separately and maintaining a unique profile for each object improves security by reducing the attack surface.
2. It reduces false alarms without losing any security capabilities. For example, instead of entirely disabling an attack signature when it is matched, you can disable the signature on a specific HTTP object, therefore preserving attack signature security functionality for the rest of the application.

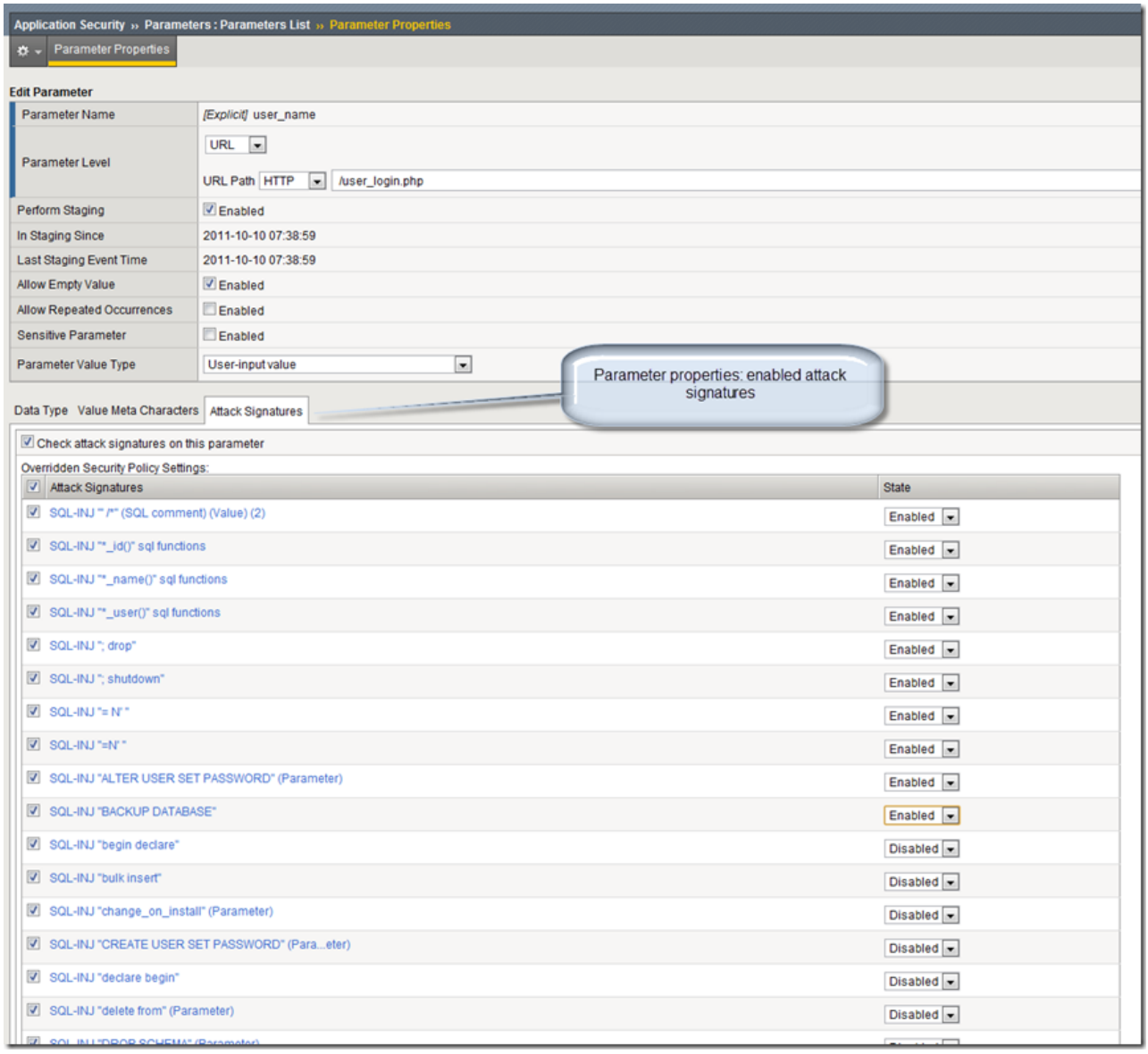
Example

In the attached picture you can see an example of the ASM parameter properties screen. On this screen you can control all the HTTP parameter properties, for example:

1. Allowed meta characters.
2. Activate attack signatures.
3. Parameter properties such as: parameter length, is the parameter allowed to appear more than once, and whether the parameter is allowed to contain an empty value.


Application Security ›› Parameters : Parameters List ›› Parameter Properties
Parameter Properties
Edit Parameter
Parameter Name
[Explicit] user_name
Parameter Level
URL
URL Path HTTP /user_login.php
Explicit parameter for URL
Perform Staging
Enabled
In Staging Since
2011-10-10 07:38:59
Last Staging Event Time
2011-10-10 07:38:59
Allow Empty Value
Enabled
Allow Repeated Occurrences
Enabled
Sensitive Parameter
Enabled
Parameter properties
Parameter Value Type
User-input value
Data Type
Value Meta Characters
Attack Signatures
Data Type
Alpha-Numeric
Maximum Length
Any
Value: 6
Parameter maximum length
Regular Expression
Enable
Cancel
Update


Application Security ›› Parameters : Parameters List ›› Parameter Properties
Parameter Properties
Edit Parameter
Parameter Name
[Explicit] user_name
Parameter Level
URL
URL Path HTTP /user_login.php
Perform Staging
Enabled
In Staging Since
2011-10-10 07:38:59
Last Staging Event Time
2011-10-10 07:38:59
Allow Empty Value
Enabled
Allow Repeated Occurrences
Enabled
Sensitive Parameter
Enabled
Parameter Value Type
User-input value
Data Type
Value Meta Characters
Attack Signatures
Parameter properties - allowed meta characters
Check characters on this parameter value
Overridden Security Policy Settings:
Meta Character (Global State)
State
m (0x6d) (Allowed)
n (0x6e) (Allowed)
o (0x6f) (Allowed)
p (0x70) (Allowed)
q (0x71) (Allowed)
r (0x72) (Allowed)
s (0x73) (Allowed)
t (0x74) (Allowed)
u (0x75) (Allowed)
v (0x76) (Allowed)
w (0x77) (Allowed)
x (0x78) (Allowed)
Allow
Cancel
Update



Summary

Today's web applications are usually the combination of different technologies developed by internal and third party software teams across the globe. Understanding and controlling these applications has become an almost impossible mission to those responsible for securing these applications.

The Attack surface of the web application is derived from the complexity of the HTTP protocol, without the understanding of the application data objects and their characteristics, and without the ability to secure each data object from the threats waiting to be exploited.

F5 Application Security Manager (ASM) parses the HTTP request to its most delicate parts allowing you to learn and manage security profiles to each of the HTTP objects and as a result harden web application security and improve your protection capabilities.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com