iRule Security 101 - #1 - HTTP Version

Joe Pruitt, 2007-27-07

When looking at securing up your web application, there are a set of fairly standard attack patterns that application firewalls make use of to protect against those bad guys out there who are trying exploit your website. A good reference for web application attacks is the Open Web Application Security Project (OWASP). In this series of blog posts, I'm going to highlight different attacks and how they can be defended against by using iRules.

In the first installment of this series I will show how to only allow valid HTTP requests to your application server. The most common HTTP versions out there are 1.0 and 1.1 although version 0.9 is still used in places. A common attempt to fool an application is by passing an invalid HTTP Version causing the server to not interpret the request correctly. The "HTTP version" iRules command contains the request version and you can ensure that only valid requests are processed and allowed to your app servers with this iRule:

```
when RULE_INIT {  set INFO 0  set DEBUG 0  #-------------------------------------------------------------------  # HTTP Version  #-------------------
```

In the RULE_INIT method I've created a few global variables enabling one to turn on or off the verification. Without all the extra conditionals, the iRule can be stripped down to the following couple of lines:

```
when RULE_INIT {  set sec_http_versions [list "0.9" "1.0" "1.1" ]}when HTTP_REQUEST {  if { ! [matchclass [HTTP::version] equals $::sec_http_versions ] }
```

Stay tuned for the next installment of iRules Security 101 where I'll show how to validate HTTP methods.

-Joe

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