



The PDF problem

How to overcome recent PDF security risks using an F5 iRule.

IF YOU OWN the F5 BIG-IP application delivery networking product, version 9, you already have the ability to create your own rules-based language called iRules. And now we've created a new iRule that allows you to protect user systems accessing Adobe PDF files. Best of all, it's free.

In recent weeks, conversation regarding a pervasive security risk making use of Adobe software on users' systems has cropped up among security groups and hacker forums alike. The Adobe vulnerability quickly garnered a large amount of attention, even from mainstream media.

This vulnerability is a cross-

site scripting attack that causes victims to run an attacker's script while in the context of the attacked site. Any PDF can be used, since the problem is with the way the PDF is presented in the browser. (For a detailed description of the problem, go to the webapp security list, www.webappsec.org.)

Adobe has acknowledged the problem and has posted information at www.adobe.com/support/security/advisories/apsa07-01.html.

The new iRule forces a redirection on PDF requests and uses the redirection to remove fragments (anchors) that were on the original link. It also verifies that the requestor hasn't changed IP addresses, and that they're making the request to the redirect destination URL within 10 seconds of their initial request by passing some additional, encrypted info in the URL and verifying it after the redi-

rection. If things don't line up, or things look suspicious, the iRule simply forces the user to download the PDF, which is the current solution proposed by many today.

What does all of this mean? It means organizations hosting PDF files on their websites that want to greatly reduce the risk of this widespread problem, but don't want to force users to download every PDF, every time, now have a way to do so.

To view the code, visit F5's online developer community, DevCentral, at <http://devcentral.f5.com>.

iRule, Do You? contest winners

F5 recently announced the winners of its second annual DevCentral iRule contest, “iRule, Do You?” A panel of industry experts recognized six application developers and network professionals for their BIG-IP iRules development expertise:

iRULES WINNERS - Customer Division

FIRST PLACE iRULE: “reverseproxy_webmail_prod” by Jamey Price (USA)

This iRule provides reverse-proxy functionality for a set of Lotus Notes 7 servers to provide webmail to end users. The results of developing this iRule were reduced configuration complexity and avoidance of previously unacceptable performance provided by alternative solutions. According to Jason Bloomberg, contest judge and senior analyst with ZapThink LLC, “The cookie manipulations make this iRule especially interesting.”

SECOND PLACE iRULE: “OCSP authentication error redirect” by Kevin Stewart (USA)

When clients fail Online Certificate Status Protocol (OCSP) authentication, secure Web pages are usually replaced with a basic “Page cannot be displayed” error consisting of very little information for troubleshooting. This iRule helps users and reduces IT help desk workloads by generating dynamic HTML/CSS/JavaScript that includes the specific error for further diagnosis. Judge

Jason Rahm, 2005 “iRule, Do You?” Contest grand prize winner, commented, “As a former help desk worker, THANK YOU! Ingenious use of error data to provide exactly the problem in the HTTP::response event helps keep support calls short and sweet.”

THIRD PLACE iRULE: “Antispam” by Jari Leppala (Finland)

Spam is a universal challenge. To reduce connections to back-end servers that steal valuable processing cycles, this iRule detects and rejects sources opening large amounts of client connections in a short time frame, which can be indicative of spam. It does so by counting SMTP connections from a specific IP address within a given time frame. If an abusive IP client is detected, a message is sent to the email originator and it is added to an abusers list to block future attempts. “Handling spam at this stage can significantly cut down on network traffic,” said judge Zeus Kerravala, a senior vice president at Yankee Group Research Inc.

iRULES WINNERS - Partner Division

FIRST PLACE iRULE: “iRule_Persist_On_HTTP_Data” by Sake Blok, ion-ip B.V. (The Netherlands)

For SOAP-based authentication against LDAP servers and cached for performance optimization, traditional load balancing was not a viable option due to the burden large cache files placed on each server. By using this iRule to parse HTTP requests for Session-ID data, and either persist the session to the originating server or create a new Session-ID, ion-ip’s customer was able to avoid a costly investment in larger servers to support this application. “The extent to which traffic can be persisted is really shown off here,” said judge Rahm.

SECOND PLACE iRULE: “w3c_iRule” by Nuno Paulino, Telindus Portugal (Portugal)

To support W3C logging formats with host-header validation, this ingenious iRule translates floating-point values to strings and makes appropriate conversions as string

functions. In this case, it was translation of milliseconds to seconds. Judge Joe Pruitt, senior strategic architect at F5, commented, “You have to give credit when someone finds a unique solution to a known issue in one of your products. This iRule will be very useful to the community.”

THIRD PLACE iRULE: “irule_limit_num_connections_googlebot” by Eduardo Saito, Assistec Integracao (Brazil)

While most websites desire regular crawling by leading search engines, many prefer to limit the number of server cycles consumed by the process. By utilizing connection limits for a known source IP address, this iRule protects server performance while still enabling crawling. It also helps manage this process from the network before the requests reach the servers. According to judge Pruitt, “This iRule enables a number of useful ways to limit connection rates for abusive clients.”

About F5’s iRules and iControl API

F5’s iRules represent a revolutionary approach to intercepting, parsing, modifying, and routing application traffic based on extremely customizable logical policies. iRules, exclusive to F5 Networks’ BIG-IP v9, utilize a standard scripting language—Tool Command Language (TCL)—to construct these policies that you can apply to any IP application. You can use many of the standard TCL commands—plus a robust set of extensions that BIG-IP provides to help administrators and application developers further optimize and secure application traffic—to meet specific requirements, expand upon an application’s functionality, or even offload some of the work to the network layer. For more information, visit F5’s online developer community, DevCentral, at <http://devcentral.f5.com>.

DCTV and iTunes

When we rolled out DevCentral Television (DCTV), we had no idea how popular it would be. Over a year and tens of thousands of views later, we’re expanding both the topics we cover and the ways we reach viewers. Because so many people have the ever-popular iPod, we’ve decided to syndicate our DCTV videos—which now include security experts and topics as well as the usual suspects—through iTunes. Now, you can download DCTV to your video iPod and get the latest dose of technical TV wherever your travels take you. You’ll laugh, you’ll cry ... and maybe even learn a new iRule command or two.