20 Lines or Less: Security Headers and DNS

Jason Rahm, 2016-14-03

What could you do with your code in 20 Lines or Less?

That's the question we like to ask from, for, and of (feel free to insert your favorite preposition here) the DevCentral community, and every time we do, we go looking to find cool new examples that show just how flexible and powerful iRules can be without getting in over your head. Thus was born the 20LoL (20 Lines or Less) series many moons ago. Over the years we've highlighted hundreds of iRules examples, all of which do downright cool things in less than 21 lines of code.

Security Headers

At RSA a couple weeks ago I presented on how to secure your clients with regards to their experience on your web applications. Scott Helme created the SecurityHeaders.io site where you can test your apps to see what is and isn’t supported currently. I can’t stress enough how important it is to read carefully and test thoroughly before implementing some of these headers, you can dos yourself fairly easily. That said, putting in the work to protect your users is a worthy effort, and it’s a pretty easy implementation with iRules, or with an LTM policy. You can test CSP and HPKP using the -Report-Only trailer to those headers at another site of Scott's called Report-URI.io.

```
when RULE_INIT {
  set static::fqdn_pin1 "X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg="
  set static::fqdn_pin2 "MHJYVThihUrJcxW6wcqyOISTXIsInsdj3xK8QrZbHec="
  set static::max_age 15552000
}
when HTTP_REQUEST {
  HTTP::respond 301 Location "https://[HTTP::host][HTTP::uri]"
}
when HTTP_RESPONSE {
  #HSTS
  HTTP::header insert Strict-Transport-Security "max-age=$static::max_age; includeSubDomains"
  #HPKP
  HTTP::header insert Public-Key-Pins "pin-sha256=\"$static::fqdn_pin1\" max-age=$static::max_age; in
  #X-XSS-Protection
  HTTP::header insert X-XSS-Protection "1; mode=block"
  #X-Frame-Options
  HTTP::header insert X-Frame-Options "DENY"
  #X-Content-Type-Options
  HTTP::header insert X-Content-Type-Options "nosniff"
  #CSP
  HTTP::header insert Content-Security-Policy "default-src https://devcentral.f5.com:443"
  #CSP for IE
  HTTP::header insert X-Content-Security-Policy "default-src https://devcentral.f5.com:443"
}
```

Redirect the NXDOMAIN Response

We haven't featured too many DNS-based iRules, but we are starting to see an uptick in their presence in the community. The result of the conversation between dearsanky and Kai Wilke is a short but sweet sample redirecting non-existent domain queries

```
when DNS_RESPONSE {
  if { [DNS::header rcode] eq "NXDOMAIN" } {
    DNS::header rcode NOERROR
    DNS::answer insert "[DNS::question name]. 60 [DNS::question class] [DNS::question type] 1.1.1.1"
  }
}
```

DNS Recursion & Blacklisting

Another more complex DNS sample, also a result of an exchange between dearsanky and Kai Wilke. This iRule blocks queries not configured in the admin_datagroup data-group as well as looks for blacklisted ip's and blocks those as well. Before the DNS namespace was added to iRules (note: license required if you don't have GTM/BIG-IP DNS) this was an exercise in binary scans and formats, but is made far simpler with clear commands.

```
when RULE_INIT {
 set static::blacklist_reply_IPV4 "10.10.10.10"
 set static::blacklist_ttl "100"
}
when DNS_REQUEST {
  set Blacklist_Match 0
  set Blacklist_Type ""
  set domain_name [DNS::question name]
  if {[DNS::header "rd"] == 1 } {
    if { not [class match [IP::client_addr] eq "admin_datagroup" ] } {
      DNS::drop
    } elseif { [string tolower [class match $domain_name eq Blacklist_Class]] } {
        set Blacklist_Match 1
        DNS::return
    }
  }
}
when DNS_RESPONSE {
  if { $Blacklist_Match } {
    switch [DNS::question type] {
      "A" {
        DNS::answer clear
        DNS::answer insert "[DNS::question name]. $static::blacklist_ttl [DNS::question class] [DNS::
        DNS::header ra "1"
      }
      default { DNS::last_act reject } }
    }
  }
}
```

And there it is, another edition of 20 Lines or Less, the power of iRules on full display. Happy coding out there, and I look forward to seeing what excellent contributions might make the next edition!

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