Apache Configuration Items

ModSecurity Errors

Recently I noticed errors on my Ubuntu 18.04 machine in /var/log/apache2/errors.log that look as below. These may also occur on any other Linux server running Apache and ModSecurity.

```
[Tue Jan 14 09:58:51.980208 2020] [:error] [pid 8812] [client ::1:48280] [client ::1] ModSecurity: Rule
7f6584a61a50 [id "-"][file "/usr/share/modsecurity-crs/rules/RESPONSE-951-DATA-LEAKAGES-SQL.conf"][line "98"] -
Execution error - PCRE limits exceeded (-8): (null). [hostname "localhost"] [uri "/open-audit/index.php
/discoveries/26"] [unique_id "Xh0EO9HUUpzELlm@OJLwKwAAAAA"], referer: http://localhost/open-audit/index.php
/discoveries/26
```

These would show multiple times for any requested page.

According to the Atomicorp ModSecurity page here - https://support.atomicorp.com/hc/en-us/articles/360000188468-Rule-execution-error-PCRE-limits-exceeded-8-null- you should increase a couple of limits.

I have edited /etc/modsecurity/modsecurity.conf and set these as recommended below.

```
SecPcreMatchLimit 250000
SecPcreMatchLimitRecursion 250000
```

I restarted Apache (sudo systemctl restart apache2) and I have no more warnings in my Apache error log.

Headers

Why don't we simply ship these as .htaccess file? At least in my default apache config (on Debian), NoOverrides are set (and Open-AudIT is in the default 'site'), so .htaccess file will not have any effect. The simplest way is to edit the apache site config if you really need these enabled.

MimeType woff2

Apache doesn't (at least on my Debian machine) know the mime type of woff2. This is generally not an issue, however some security tools will report this as not being set and raise a flag. The simplest way to resolve this is to add it to your configuration. In my case, I added it to /etc/apache2/sites-available /000-default.conf. Inside the VirtualHost section, I added the below:

```
<IfModule mod_mime.c>
        AddType application/woff2 .woff2
</IfModule>
```

Once I restarted apache I can see the header being passed as the security tools expect.

X-Content-Type-Options nosniff

As with the above, some security tools want to see this header passed. Again, on my apache it was not being passed by default. I edited the same file as above and added the below (again, in the VirtualHost section).

```
<IfModule mod_headers.c>
        Header set X-Content-Type-Options nosniff
</IfModule>
```

Restart Apache and you're good to go.

Windows Apache User

See the details on this page - Running Open-AudIT Apache Service under Windows.