VelocityReport Plugin - Feature #1574

Support for HttpOnly with optionally Secure and SameSite flag for Cookies

08/24/2020 12:12 PM - Robert Ivens

Status:	Resolved	**Start date:**	08/24/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	velocity	**Estimated time:**	0.00 hour
Target version:			
Browser (if web client):			

Description

To make cookies more resistant against XSS there is a HttpOnly flag to disallow JavaScript from accessing the cookies.

Further reading:
https://securityboulevard.com/2020/08/the-httponly-flag-protecting-cookies-against-xss

P.s. I do see a 'secure' property for cookies in the Velocity plugin but there is no tooltip and the Wiki also doesn't mention it.

History

#1 - 08/28/2020 06:00 PM - Patrick Talbot

The "secure" property adds the secure flag indeed.

There's no property for HttpOnly and SameSite, because I am relying on java's libraries from previous versions that exposes methods for secure but not the others.

I'll check with newer versions and see if this is available, if so, I'll add the properties, although I will have to add some Reflection code to avoid MethodNotFoundException if Velocity is running in older java versions.

Starting with Java 8 javax.servlet.http.Cookie (which is in /lib/servlet-api.jar) it looks like HttpOnly is supported (But not SameSite):
https://javaee.github.io/javaee-spec/javadocs/javax/servlet/http/Cookie.html

#2 - 08/28/2020 08:13 PM - Patrick Talbot

- Status changed from New to Resolved

An httpOnly property has been added to v3.5.83 - check it out!