JavaScript: An AppSec perspective on the multi-faceted devil that calls the Internet its home.

The average user’s experience of the Internet relies on three elements: Content (HTML), Style (CSS), and Behavior (JavaScript). A great majority of modern frameworks that use a variety of languages and approaches usually boil back down to these three concepts in these three formats.

Concentrating on Behavior, we will take a closer look at JavaScript, which has grown to outgrow the user’s browser, now enabling a massive ecosystem that allows the construction of API's, of games, and more.

The aim for this presentation is first to give an overview of how JS works, in and out of the browser and what capabilities are there for eager or seasoned developers to take advantage of and play around with.

Then, it will try to consider how an Application Security centric approach can mitigate various exploits and benefits the developer, as well as a malicious approach which would try to make use of said exploits.

Finally, a special consideration will be given to the usage of obfuscation, whether it be via WTFJS style obfuscation (also known as non-alpha-numeric obfuscation) or control-flow obfuscation for example. Since these can be used on either side of the ethical boundary, whether it be to shield application logic or to make malware written in JavaScript harder to detect, it is an important component of JS’s everyday usage.