XSnare Signature Language Specification

Jose Carlos Pazos

February 25, 2021

This is a description of the XSnare signature language, using the context of WordPress as examples. Further examples of working signatures can be found in the extension's **sigs.js** file:

- url: If the exploit occurs in a specific URL or subdomain, this is defined as a string, e.g. `/wp-admin/options-general.php?page=relevanssi\%2Frelevanssi.php`, otherwise null.
- software: The software framework the page is running if any, e.g. WordPress. A hand-crafted page might not have any identifiable software.
- softwareDetails: If running any software, this provides further information about when to load a signature. For WordPress, these are plugin names as depicted in the HTML of a page running such plugin.
- version: The version number of the software/plugin/page. This is used for versioning of the software run by the page.
- type: A string describing the signature type. A value of "string" describes a basic signature. A value of 'listener' describes a signature which requires an additional listener in the background page for network requests.
- sanitizer: A string with one of the following values: "DOMPurify", "escape", and "regex". This item is optional, the default is DOMPurify.
- config: The config parameters to go along with the chosen sanitizer, if necessary. For "DOMPurify", the accepted values are as defined by the DOMPurify API (i.e, DOMPurify.sanitize(dirty, config). For "escape", an additional escaping pattern can be provided. For "regex", this should be the pattern to match with the injection point content.
- typeDet: A string with the following pattern: 'occurrence-uniqueness', 'ocurrence' has values single/multiple, which describes the existence of one or multiple independent injection points; the 'uniqueness' has values unique/several, specifying whether an injection point occurs once or several times throughout the document.
- endPoints: An array of startpoint and endpoint tuples, specified as strings for regex matching.

- endPointsPositions: An array of integer tuples. These are optional but useful when the one of the endPoints HTML are used throughout the whole page and appear a fixed number of times. For example: if an injection ending point happens on an element ¡h3 class='my-header'¿, this element might have 10 appearances throughout the page. However, only the 4th is an injection ending point. The signature would specify the second element of the tuple to be 7, as it would be the 7th such item in a regex match array (using 1-based indexing), counting from the bottom up. For ending points, we have to count from the bottom up because the attacker can inject arbitrarily many of these elements before it, and vice versa for starting points.

Additionally, if the value of type is 'listener', the signature will have an additional field called listenerData. Similarly to a regular signature, this consists of the following pieces of information:

- listenerType: The type of network listener as defined by the WebRequest API (e.g. 'script', 'XHR', etc.)
- listenerMethod: The request's HTTP method, for example "GET" or "POST".
- url: the URL of the request target.

If a listener is present, the signature's fields can be used to specify the listener's request injection points.