

[\(https://blog.rapid7.com/\)](https://blog.rapid7.com/)

[View All Tags \(/tag/\)](#)

[Blog Home \(https://blog.rapid7.com/\)](https://blog.rapid7.com/) //

R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI (CVE-2016-5682)

Rapid7 Blog

R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI (CVE- 2016-5682)



Scott Davis [\(/author/scott-davis/\)](/author/scott-davis/)

Sep 02, 2016 | 1 min read

POST STATS: 0

Parameters within a Swagger document are insecurely loaded into a browser based documentation. Persistent XSS occurs when this documentation is then hosted together on a public site. This issue was resolved in [Swagger-UI 2.2.1](https://github.com/swagger-api/swagger-ui/releases/tag/v2.2.1) (<https://github.com/swagger-api/swagger-ui/releases/tag/v2.2.1>).

Summary

One of the components used to build the interactive documentation portion of the swagger ecosystem is the [Swagger-UI](https://github.com/swagger-api/swagger-ui) (<https://github.com/swagger-api/swagger-ui>). This interface generates dynamic documentation based on a referenced Swagger document that can interact with the referenced API. If the swagger document itself contains XSS payloads, the swagger-ui component can be tricked into injecting unescaped content into the DOM.

Product Description

From the README at <https://github.com/swagger-api/swagger-ui> (<https://github.com/swagger-api/swagger-ui>).

"Swagger UI is part of the Swagger project. The Swagger project allows you to produce, visualize and consume your own RESTful services. No proxy or 3rd party services required. Do it your own way.

Swagger UI is a dependency-free collection of HTML, Javascript, and CSS assets that dynamically generate beautiful documentation and sandbox from a Swagger-compliant API. Because Swagger UI has no dependencies, you can host it in any server environment, or on your local machine."

Swagger Petstore

This is a sample server Petstore server. You can find out more about Swagger at <http://swagger.io> or on [#swagger](irc.freenode.net). For this sample, you can use the api key `special-key` to test the authorization filters.

Find out more about Swagger

<http://swagger.io>
[Contact the developer](#)
[Apache 2.0](#)

pet : Everything about your Pets

Show/Hide | List Operations | Expand Operations

store : Access to Petstore orders


Show/Hide | List Operations | Expand Operations

GET	/store/inventory	Returns pet inventories by status
POST	/store/order	Place an order for a pet
DELETE	/store/order/{orderId}	Delete purchase order by ID
GET	/store/order/{orderId}	Find purchase order by ID

user : Operations about user

Show/Hide | List Operations | Expand Operations

[BASE URL: /v2 , API VERSION: 1.0.0]

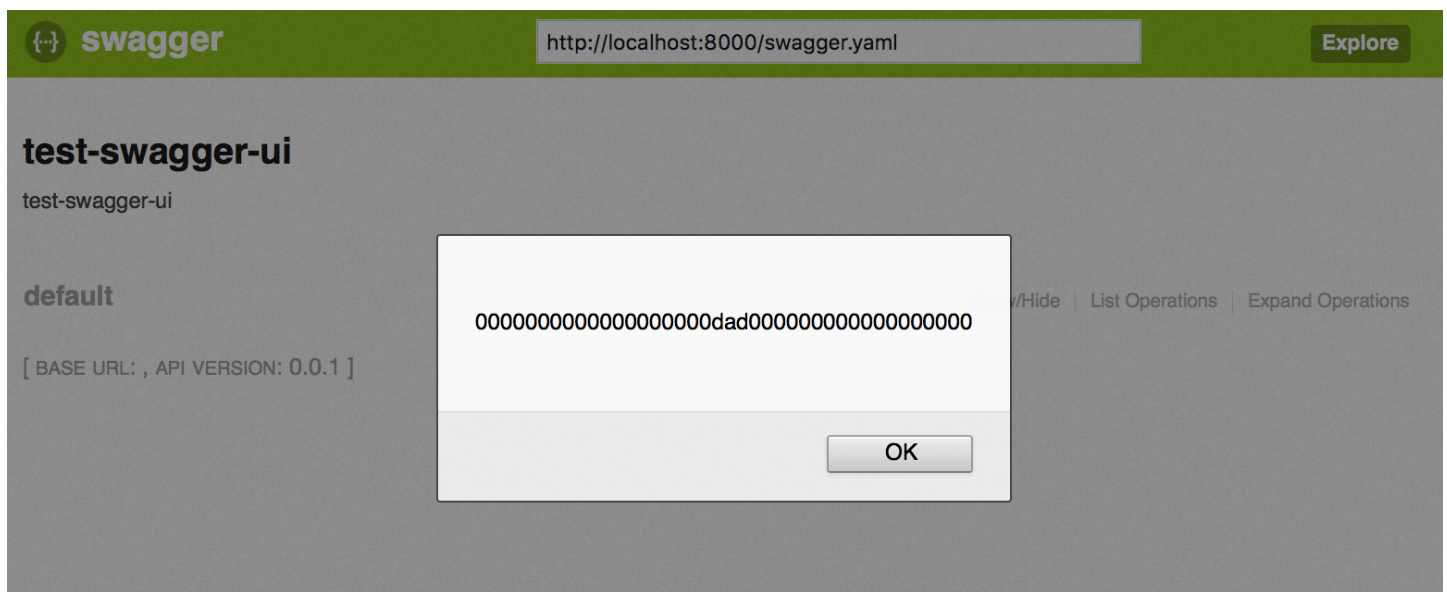
VALID

The swagger UI will parse a chosen swagger file, and generate dynamic colorful documentation that enables users to interact with a RESTful API.

Credit

Scott Lee Davis, scott_davis@rapid7.com (mailto:scott_davis@rapid7.com), Application Security Researcher, Rapid7

Exploitation



If a swagger file contained in the definitions section, a default value with an XSS payload can be loaded unescaped into the DOM.

Definitions

Type: string

Description: prints xss

Default: `<script>console.log('00000000000000000000dad000000000000000000')`

Mitigations

Sanitation of HTML content should be done by an engine built for the job ([https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet#RULE_236 - Sanitize HTML Markup with a Library Designed for the Job](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet#RULE_236_-_Sanitize_HTML_Markup_with_a_Library_Designed_for_the_Job)). The swagger-ui team chose to solve this issue with the npm (<https://www.npmjs.com/>) module sanitize-html (<https://www.npmjs.com/package/sanitize-html>).

Disclosure Timeline

This vulnerability advisory was prepared in accordance with Rapid7's disclosure policy. (<http://rapid7.com/disclosure.jsp>).

- Thu, Jun 09, 2016: Discovery by Scott Lee Davis of Rapid7, Inc.
- Fri, Jun 17, 2016: Attempted to contact the vendor

- Mon, Jul 11, 2016: Disclosed details to the vendor at security@swagger.io (<mailto:security@swagger.io>).
- Wed, Jul 27, 2016: Disclosed details to CERT as VR-316
- Tue, Aug 09, 2016: CVE-2016-5682 assigned by CERT
- Tue, Aug 23, 2016: Fixed in Swagger-UI 2.2.1
- Fri, Sep 02, 2016: Public disclosure

WANT MORE? DON'T MISS THESE POSTS

[\(/2017/09/27/macos-keychain-security-what-you-need-to-know/\)]((/2017/09/27/macos-keychain-security-what-you-need-to-know/))

[\(/2017/09/27/macos-keychain-security-what-you-need-to-know/\)]((/2017/09/27/macos-keychain-security-what-you-need-to-know/))
[\(/2017/09/27/macos-keychain-security-what-you-need-to-know/\)]((/2017/09/27/macos-keychain-security-what-you-need-to-know/))

If you follow the infosec twitterverse or have been keeping an eye on macOS news sites, you've likely seen a tweet [<https://twitter.com/patrickwardle/status/912...>]

[\(/2017/09/27/macos-keychain-security-what-you-need-to-know/\)]((/2017/09/27/macos-keychain-security-what-you-need-to-know/))

[EXPLOITS \(/TAG/EXPLOITS\)](#)

Summary The Workspaces component of Biscom Secure File Transfer (SFT) version 5.1.1015 is vulnerable to stored cross-site scripting in two fields. An attacker w...

VULNERABILITY DISCLOSURE (/TAG/VULNERABILITY-DISCLOSURE).

POST STATS

0


POST TAGS


EXPLOITS (/TAG/EXPLOITS/) XSS (/TAG/XSS/)


VULNERABILITY DISCLOSURE (/TAG/VULNERABILITY-DISCLOSURE/)

VULNERABILITY MANAGEMENT (/TAG/VULNERABILITY-MANAGEMENT/).

SHARING IS CARING

 [_ \(https://www.linkedin.com/shareArticle?mini=true&url=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/&title=R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI \(CVE-2016-5682\)&summary=Parameters within a Swagger document are insecurely loaded into a browser based documentation. Persistent XSS occurs when this documentation is then hosted together on\)](https://www.linkedin.com/shareArticle?mini=true&url=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/&title=R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI (CVE-2016-5682)&summary=Parameters within a Swagger document are insecurely loaded into a browser based documentation. Persistent XSS occurs when this documentation is then hosted together on)

 [_ \(https://twitter.com/intent/tweet?text=R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI \(CVE-2016-5682\)&url=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/\)](https://twitter.com/intent/tweet?text=R7-2016-19: Persistent XSS via Unescaped Parameters in Swagger-UI (CVE-2016-5682)&url=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/)

 [_ \(https://www.facebook.com/sharer/sharer.php?u=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/\)](https://www.facebook.com/sharer/sharer.php?u=https://blog.rapid7.com/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui/)

AUTHOR

Scott Davis

[\(/author/scott-davis/\)](/author/scott-davis/)



[\(/author/scott-davis/\)](/author/scott-davis/)

[View Scott Davis's Posts \(/author/scott-davis/\)](#)

0 Comments **rapid7**

 **doge** ▾

 **Recommend**

 **Tweet**

 **Share**

Sort by Best ▾



Start the discussion...

Be the first to comment.

 **Subscribe**  **Add Disqus to your site**[Add DisqusAdd](#)  **Disqus' Privacy Policy**[Privacy PolicyPrivacy](#)

[Blog Feed \(https://blog.rapid7.com/feed/\)](https://blog.rapid7.com/feed/)



[Legal Terms \(https://www.rapid7.com/legal\)](https://www.rapid7.com/legal). | [Privacy Policy \(https://www.rapid7.com/privacy-policy\)](https://www.rapid7.com/privacy-policy). |

[Export Notice \(https://www.rapid7.com/export-notice\)](https://www.rapid7.com/export-notice). | [Trust \(https://www.rapid7.com/trust\)](https://www.rapid7.com/trust). |

[Contact Us \(https://www.rapid7.com/contact\)](https://www.rapid7.com/contact). | [Careers \(https://www.rapid7.com/careers\)](https://www.rapid7.com/careers).