

Sri Lanka Institute of Information Technology



IT21299902 (ZAKY M.S.M.A)

Bug bounty Report 04.

Domain: MalwareBytes.com

Web security – IE2062

B.Sc. (Hons) in Information Technology Specialization in
cyber security.

Declaration:

- I hereby certify that no part of this assignment has been copied from any other work or any other source. No part of this assignment has been written/produced for me by another person.
- I hold a copy of this assignment that I can produce if the original is lost or damaged.

1. Using components with known vulnerabilities.

- **Outdated version of bootstrap (Possible XSS attack).**

I hope this message finds you well. I am writing to report a vulnerability I discovered under the domain of <https://www.malwarebytes.com/js/bootstrap.js> during my participation in the bug bounty program. Please find below the details of the vulnerability for your review and further action.

	Out-of-date Version (Bootstrap)	GET	https://www.malwarebytes.com/js/bootstrap.js	MEDIUM
---	---	-----	---	--------

Vulnerability title: outdated version of bootstrap (XSS possible)

Severity: Medium

Affected versions: 1.0.0 to 3.3.7

OWASP classification 2013: A9

CVSS 3.0 score: -

CVSS 3.1 score: -

CVSS string: -

Effectuated components: Payment forms.

User authentication.

Order processing and checkout.

Database

Date of Discovery: 2023/05/10

Date of Report: 2023/05/12

2. Vulnerability Description.

If a BREACH attack is successful, the attacker can potentially access sensitive information transmitted over an encrypted connection. I have identified a possibility of BREACH attack within the affected system. If this attack succeeds in the system it will lead to data leakage, session hijacking, confidentiality breach, and data manipulation.

3. Impact assessment.

Under this OWASP category I have identified this vulnerability too. Also identified that this version of bootstrap program is vulnerable to cross site scripting attacks. Also, there is a considerable amount of records to prove that this version is vulnerable to these XSS attacks.

Found this vulnerability under the domain of <https://www.malwarebytes.com/js/bootstrap.js>. version 1.0.0. to 3.3.7 are vulnerable to this attack type.

1. Older versions of Bootstrap can include security flaws that have been found and patched in more recent versions. Attackers may take advantage of these flaws to jeopardize the security of your application. To reduce the danger of such vulnerabilities, it is crucial to maintain updated frameworks and libraries.

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Affected Versions

1.0.0 to 3.3.7

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Affected Versions

1.0.0 to 3.3.7

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

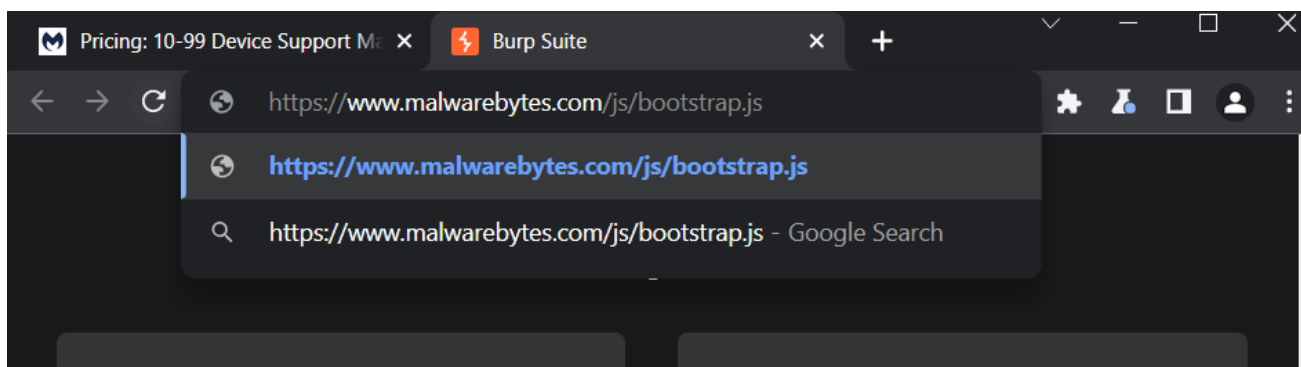
2. Updates for Bootstrap frequently include new features, improvements, and additions. You lose out on these upgrades if you continue to use an outdated version, which restricts the functionality and potential of your web application. The most recent responsive design features, component updates, bug fixes, and other advancements made in more recent versions might not be available to you.
3. Performance improvements in Bootstrap's latest iterations frequently include improved code organization, smaller file sizes, and faster rendering. You can lose out on these improvements if you're using an outdated version, which will make the user experience slower and less effective.

Because of this vulnerability marked as **MEDIUM**. It's a must to address it with a good solution.

4. Steps to Reproduce.

1. Examine the source code of the page.
 - Launch a web browser and access the web application.
 - Open the browser's developer tools by selecting "Inspect" or "Inspect Element" from the context menu when you right-click on the web page.
 - Search the page source code for references to Bootstrap files.
2. Verify Bootstrap's version:
 - Look for the Bootstrap-related CSS and JavaScript files in the page's source code.
 - Search for files with "bootstrap" or "bootstrap.min" and a ".css" or ".js" ending.
 - Determine whether the filenames or contents contain the version number.
3. Referencing the documentation for Bootstrap
 - Go to the documentation page on the official Bootstrap website (getbootstrap.com).
 - Search for the documentation for the version that you noted in the prior step.
 - Compare the code used in your web application with the features, elements, and syntax stated in the documentation.
4. Also, the versions of the libraries used in a web application, including Bootstrap, can be determined via automated methods. Outdated library versions can be found with the help of tools like Retire.js, Dependency Check, or built-in security scanners in web development frameworks.

5. Proof of concept.



```

/*!
 * Bootstrap v3.3.5 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */

if (typeof jQuery === 'undefined') {
  throw new Error('Bootstrap\'s JavaScript requires jQuery')
}

+

function($) {
  'use strict';
  var version = $.fn.jquery.split(' ')[0].split('.')
  if ((version[0] < 2 && version[1] < 9) || (version[0] == 1 && version[1] == 9 && version[2] < 1))
  {
    throw new Error('Bootstrap\'s JavaScript requires jQuery version 1.9.1 or higher')
  }
}(jQuery);

/* =====
 * Bootstrap: transition.js v3.3.5
 * http://getbootstrap.com/javascript/#transitions
 * =====
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 * ===== */

+


```

```

/*!
 * Bootstrap v3.3.5 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */


```

← → ↻ <https://getbootstrap.com> 🔍 ☆ ⚙️ 👤 ⋮



New in v5.3


Color mode support, expanded color palette, and more!



Build fast, responsive sites with Bootstrap

Powerful, extensible, and feature-packed frontend toolkit. Build and customize with Sass, utilize prebuilt grid system and components, and bring projects to life with powerful JavaScript plugins.

```
$ npm i bootstrap@5.3.0-alpha3
```

 Read the docs

Currently **v5.3.0-alpha3** · [Download](#) · [v4.6.x docs](#) · [All releases](#)

<https://blog.getbootstrap.com>

Identified Version

- 3.3.5

Latest Version

- 3.4.1 (in this branch)

Vulnerability Database

- Result is based on 05/09/2023 20:30:00 vulnerability database content.

Request

```
GET /js/bootstrap.js HTTP/1.1
Host: www.malwarebytes.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: global_variables.user.type=eyJpc0J1c2luZXNzU21hbGwiOnRydWUsImlzQnVzaW5lc3NMYXJnZSI6ZmFsc2UsImlzQnVzaW5lc3MiOnRydWUsImlzQ29uc3VtZXIiOmZhbnRlQ%3D%3D; global_variables.user.type=eyJpc0J1c2luZXNzU21hbGwiOnRydWUsImlzQnVzaW5lc3NMYXJnZSI6ZmFsc2UsImlzQnVzaW5lc3MiOnRydWUsImlzQ29uc3VtZXIiOmZhbnRlQ%3D%3D; over100=false; over100=false; visited=true
Referer: https://www.malwarebytes.com/se
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 416.5949 Total Bytes Received : 75915 Body Length : 75275 Is Compressed : No

```
/*!
 * Bootstrap v3.3.5(http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */

if (typeof jQuery === 'undefined') {
  throw new Error('Bootstrap\'s JavaScript requires jQuery
  ...
```


6. Proposed mitigation/fix.

1. Find the most recent stable Bootstrap version, then update your web application to use it. New features, performance enhancements, security updates, and bug fixes are often included in the most recent versions. To ensure a seamless move to the new version, follow the migration guides and documentation for Bootstrap.
2. If updating to the most recent version is not immediately possible, look for any security updates or Bootstrap-specific changes. Patches for known vulnerabilities may have been released by Bootstrap or the development community. To fix the security flaws in your current version, apply these updates.
3. Update all your dependencies and libraries, including Bootstrap. This makes it possible to guarantee that your web application makes use of the most recent security updates and features. Check for updates frequently, and plan maintenance windows to update libraries as needed.
4. Keep up with any Bootstrap-related security warnings or vulnerability announcements. To get updates on new vulnerabilities and patches, join security newsletters or follow trustworthy sources. Apply any security updates to your web application as soon as possible.