**Research on Vulnerability: CVE-2023-26136**

**Description:**

Versions of the package tough-cookie before 4.1.3 are vulnerable to Prototype Pollution due to improper handling of Cookies when using CookieJar in rejectPublicSuffixes=false mode. This issue arises from the manner in which the objects are initialized.

<https://nvd.nist.gov/vuln/detail/CVE-2023-26136>

**Introduction:**

**What is Prototype Pollution?**

JavaScript has the concept of objects, which is somewhat like dictionaries. An object can hold a set of variables of different types (e.g. string, Boolean, int etc.), the variable name is a key, and its value is the value, if we continue with the analogy of dictionaries and objects. More precisely, the object is analog to the dictionary **data structure** itself, and each variable is analog to a **key-value pair**. Objects also has the keyword **\_\_proto\_\_** which enables to add additional variables to an object via modifying its prototype. **Prototype Pollution** is an attack in which the attacker pollute his object, by adding to it additional variables, via the \_\_proto\_\_ keyword. The below interaction with the browser’s console demonstrates the attack.



As we can see, we have two users: admin1 and user1. admin1 object has a Boolean variable: “isAdmin”, which is set to true. User1 doesn’t has this variable altogether. At line 7, we add the isAdmin variable to the user1’s prototype, and even though it is evident from line 10 that the variable hasn’t been added to the user1’s object itself, the console responds positively, this time, when we check for the value of user1.isAdmin.



**What are cookies?**

Cookies (often known as internet cookies) are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a network. Specific cookies are used to identify specific users and improve their web browsing experience.

Courtesy of Kaspersky: <https://www.kaspersky.com/resource-center/definitions/cookies>

**What is CookieJar?**

CookieJar is an object for storing cookies.