**Vulnerability Report**

Vulnerability: long password Dos attack

# \*\*Description:

By sending a very long password (1.000.000 characters) it’s possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion.This vulnerability was detected by sending passwords with various lengths and comparing the measured response times. Consult details for more information.

# \*\*Instance:

https://24eshop.in/my-account/

**\*\*Steps to reproduce:**

1. Go to https://24eshop.in/my-account/
2. Then fill your details like email address
3. In password field give a password of 2000 or more characters.
4. I have tried -

WjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhgWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggQWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhggWjwjjwjwbwhhgcfiggibbghujhgftihbgggghhhbggfruhvvfjgggggjbbcfkjhvvvvffghbbbbhhhhhhggggghhhhhgg

1. Then click on register.
2. You can see that it will accept this 2000 characters password.

**\*\*Impact:**

It’s possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive

**\*\*Remediation:**

The password hashing implementation must be fixed to limit the maximum length of accepted passwords.

Impact

**\*\*Severity**:

HIGH

**\*\*Classification**:

CWE-400 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

**\*\*Tags:**

Denial Of Service

**\*\*References:**

Drupal Core – Moderately Critical – Multiple Vulnerabilities – SA-CORE-2014-006

Timing Attack and the importance of controlling the length of the input | The Case of Drupal CVE-2014-9016