Authentication Bypass in GRANDCOM CMS

- Vendor Homepage: https://www.grandcom.sk/
- Affected Version: 4.2 and older
- CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37413

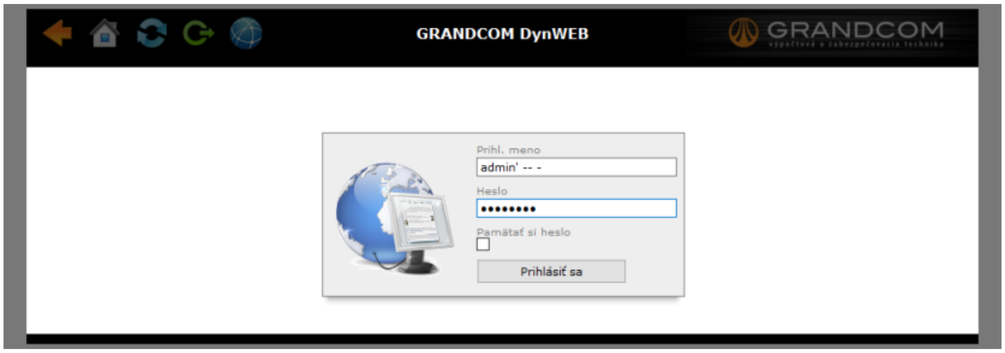
SQL injection vulnerability in GRANDCOM CMS allows remote unauthenticated attackers to bypass authentication via a crafted username during a login attempt. Any unauthorized user with access to the application is able to exploit this vulnerability.

> SQL Injection attack consists of inserting an SQL query through the input data from the client into the application. Upon successful misuse, it is possible to retrieve detailed data from the database, edit database data such as inserting, updating or deleting data, work with administrative operations in the database, or in some situations run commands directly on the operating system.

Steps to reproduce

1. Visit the following resource `/admin/index.php` .
2. Enter the below mentioned credentials in the vulnerable field:

- username: `admin' -- -`
- password: *anything*



Prihl. meno
admin' -- -
Heslo
••••••••
Pamätať si heslo
□

5. Press the **Login** button, this will result in a successful Authentication Bypass.

Remediation

- Use of Prepared Statements (with Parameterized Queries)
- Use of Stored Procedures
- Allow-list Input Validation
- Escaping All User Supplied Input

Discovered by Martin Kubecka, July 19, 2021.