



SQL

injection

SQL injections

(læs mere her: [Medium: You have to know this, SQL-injections are crazy! \(Explanation + examples\)](#))

- Webside med login formular:

Login

E-mail:

Password:

Login

```
SELECT *  
FROM users  
WHERE username = 'admin' AND password = 'password123'
```

SQL injections

- En hacker taster nu:

Login

E-mail:

admin

Password:

qwerty' OR '1'='1'

Login

```
SELECT *  
FROM users  
WHERE username = 'admin' AND (password = 'qwerty' OR '1'='1');
```

Script injection hos Bahne

- [Artikel i Version 2, den 29. november 2019](#)



The image shows a screenshot of a news article header from the website 'Version 2'. The header features the site's logo 'VERSION 2' in large white letters on a dark background. To the right of the logo are social media icons for RSS, Facebook, Twitter, and LinkedIn. Below these icons is a navigation menu with the following items: 'IT-NYHEDER', 'BLOGS', 'DEBAT', 'IT-JOB', 'SEKTIONER', and 'MERE'. The main headline of the article is 'Bahne advarer kunder efter script injection: Spær dit betalingskort - det kan være blevet misbrugt'. At the bottom left of the article header is the 'bahne' logo with the tagline 'ELKOMMEN HEM'. At the bottom right is a search bar with the placeholder text 'Søg efter varer her...' and a magnifying glass icon.

VERSION 2 IT-NYHEDER BLOGS DEBAT IT-JOB SEKTIONER MERE

Bahne advarer kunder efter script injection: Spær dit betalingskort - det kan være blevet misbrugt

bahne
ELKOMMEN HEM

Søg efter varer her...

Lad os hacke en bank 😊

Kan du ændre en af kundernes password?

Sign Off | Contact Us | Feedback | Search Go

Altoro Mutual

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

Online Banking Login

Username:

Password:

Login

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

Link til banken:

<http://altoro.testfire.net/login.jsp>

Under "username" taster du:

admin

Under "password" taster du:

qwerty' OR '1'='1

DON'T DO THIS AT HOME!



**Det var
selvfølgelig en
PRANK!**

DON'T DO THIS AT HOME!



Brevkassespørgsmål til cyberhus.dk:

Hej cyberhus. Jeg vil lige høre om det er tilladt at sql injecte en side bare for at se om det er muligt og så ikke gøre noget ved det? Evt. ringe til admin på siden?

Svar:

SQL Injection er stærkt ulovligt og det eksempel du har opstillet med at teste og ringe til admin, ville i bund og grund svare til at slå en person, for at teste om det gør ondt. SQL Injection er ikke ulovligt hvis det mislykkedes, men hvis det lykkedes dig at bryde ind på andres systemer (.. i denne sag SQL databasen), vil det være overtrædelser af flere lovgivninger og kan reelt give en fængselsstraf, hvis admin laver sag mod dig.

Tænk på hvordan det vil være i den fysiske verden...

- Er det lovligt at prøve at bryde ind i min nabos hus – bare for at se om det kan lade sig gøre? Så vil jeg bagefter kontakte ham og fortælle hvor svaghederne er...

Ej vel!