SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Web Security- IE2062

SQL INJECTION

A03:2021

Danuka Nuwan

IT22349842

Title – SQL Injection Vulnerability in User Authentication

Vulnerability: The application is vulnerable to SQL injection attacks against the user authentication process due to inadequate input validation and sanitization. More precisely, the login form accepts untrusted user input and neglects to escape it before processing it. As a result, a malicious actor could enter arbitrary SQL syntax into the login fields, resulting in data leaks, account hijacking, and potentially complete compromise of the application. This vulnerability also in top 3 vulnerability type on OWASP top 10. This is exploitable in the following areas of the system:

- User authentication

- Login

The severity of this vulnerability is considered high.

An attacker who exploits this vulnerability could potentially access the system without authorization jeopardizing the security, privacy and accessibility of data and resources.

Depending on the permissions linked to the compromised account the attacker might engage in activities, like stealing data escalating privileges or launching more attacks on other users or systems.

Website- www.naviant.com

Instructions to Replicate:

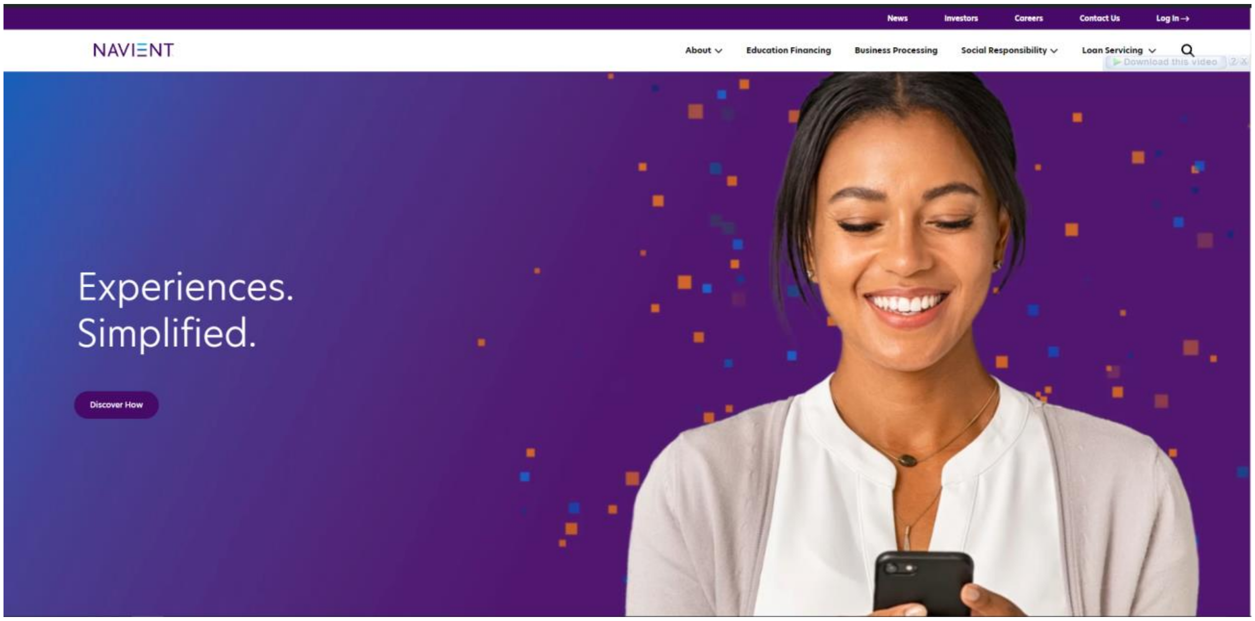
1. Go to the login page of the website.

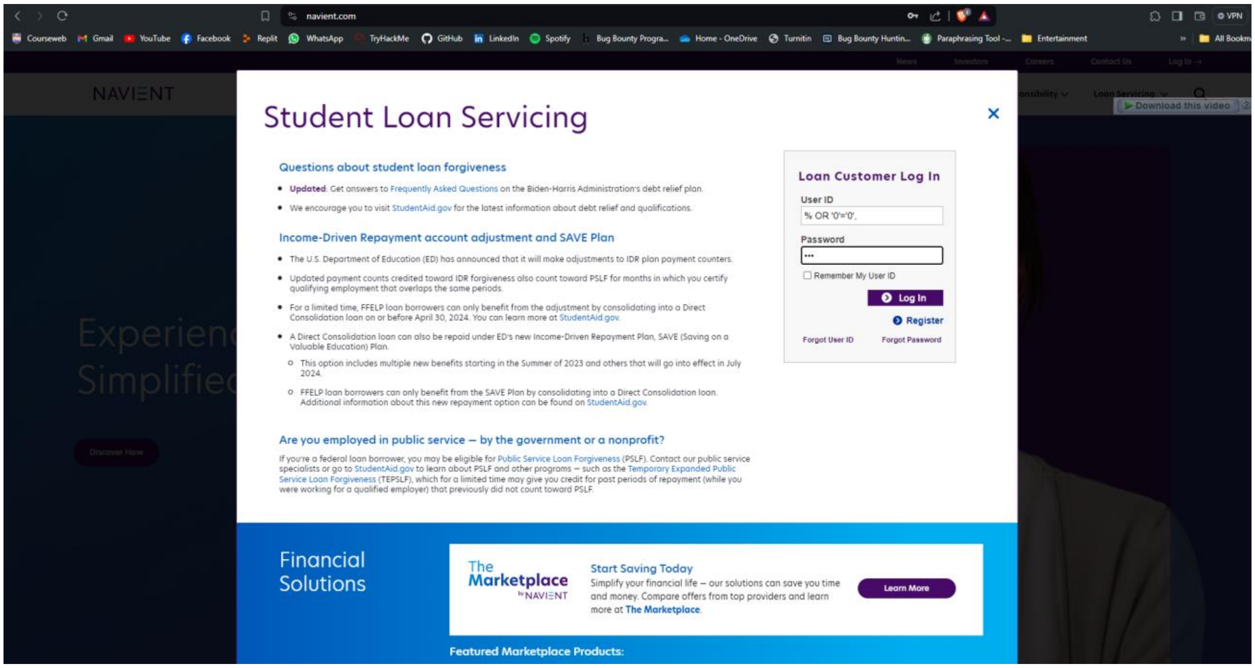
2. Enter a quote character (') in either the password field.

3. Submit the form.

4. Look for any error message or strange behavior that suggests a SQL injection attack.

Proof of Concept:





Student Loan Servicing

Questions about student loan forgiveness

- **Updated**: Get answers to Frequently Asked Questions on the Biden-Harris Administration's debt relief plan.
- We encourage you to visit StudentAid.gov for the latest information about debt relief and qualifications.

Income-Driven Repayment account adjustment and SAVE Plan

- The U.S. Department of Education (ED) has announced that it will make adjustments to IDR plan payment counters.
- Updated payment counts credited toward IDR forgiveness also count toward PSLF for months in which you certify qualifying employment that overlaps the same periods.
- For a limited time, FFELP loan borrowers can only benefit from the adjustment by consolidating into a Direct Consolidation loan on or before April 30, 2024. You can learn more at StudentAid.gov.
- A Direct Consolidation loan can also be repaid under ED's new Income-Driven Repayment Plan, SAVE (Saving on a Valuable Education) Plan.
    - This option includes multiple new benefits starting in the Summer of 2023 and others that will go into effect in July 2024.
    - FFELP loan borrowers can only benefit from the SAVE Plan by consolidating into a Direct Consolidation loan. Additional information about this new repayment option can be found on StudentAid.gov.

Are you employed in public service — by the government or a nonprofit?

If you're a federal loan borrower, you may be eligible for Public Service Loan Forgiveness (PSLF). Contact our public service specialists or go to StudentAid.gov to learn about PSLF and other programs — such as the Temporary Expanded Public Service Loan Forgiveness (TEPSLF), which for a limited time may give you credit for past periods of repayment (while you were working for a qualified employer) that previously did not count toward PSLF.

Loan Customer Log In

User ID: % OR '0'='0',

Password: •••

□ Remember My User ID

Log In

Register

Forgot User ID   Forgot Password

Financial Solutions

The Marketplace by NAVIENT

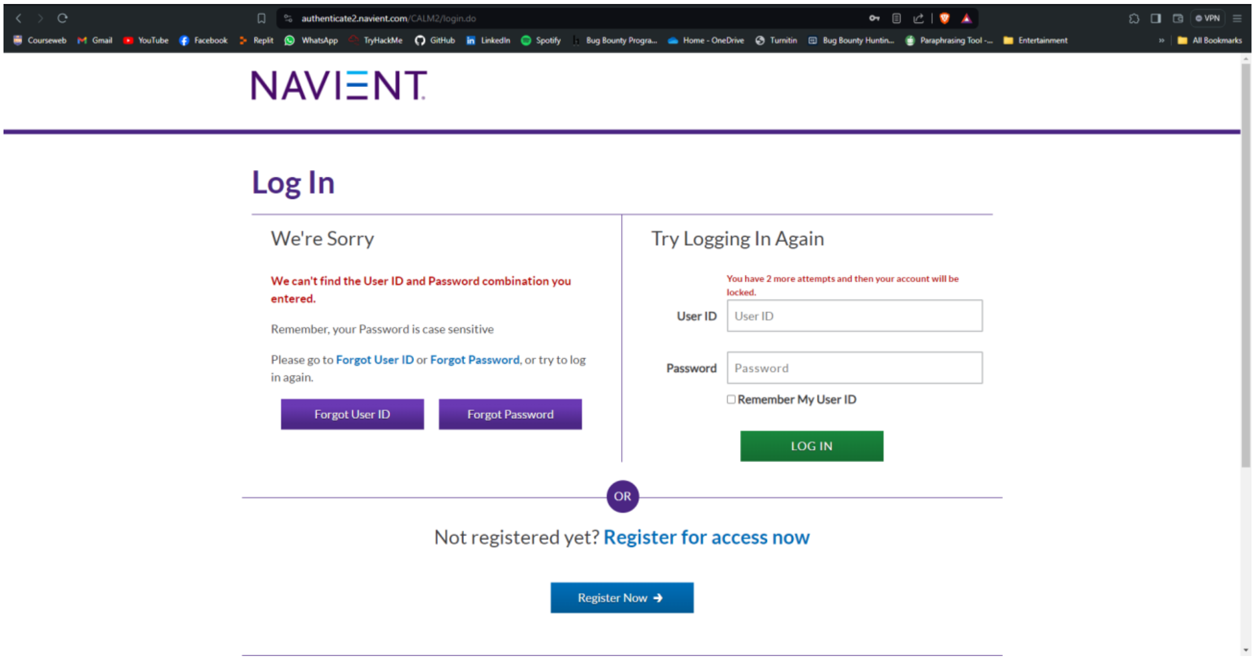
Start Saving Today

Simplify your financial life — our solutions can save you time and money. Compare offers from top providers and learn more at The Marketplace.

Learn More

Featured Marketplace Products:

I use some small SQL injection commands for this site. Some are '% OR '0'='0', " or ""=". These are very small command.



authenticate2.navient.com/CALM2/login.do

Log In

We're Sorry

We can't find the User ID and Password combination you entered.

Remember, your Password is case sensitive

Please go to Forgot User ID or Forgot Password, or try to log in again.

Try Logging In Again

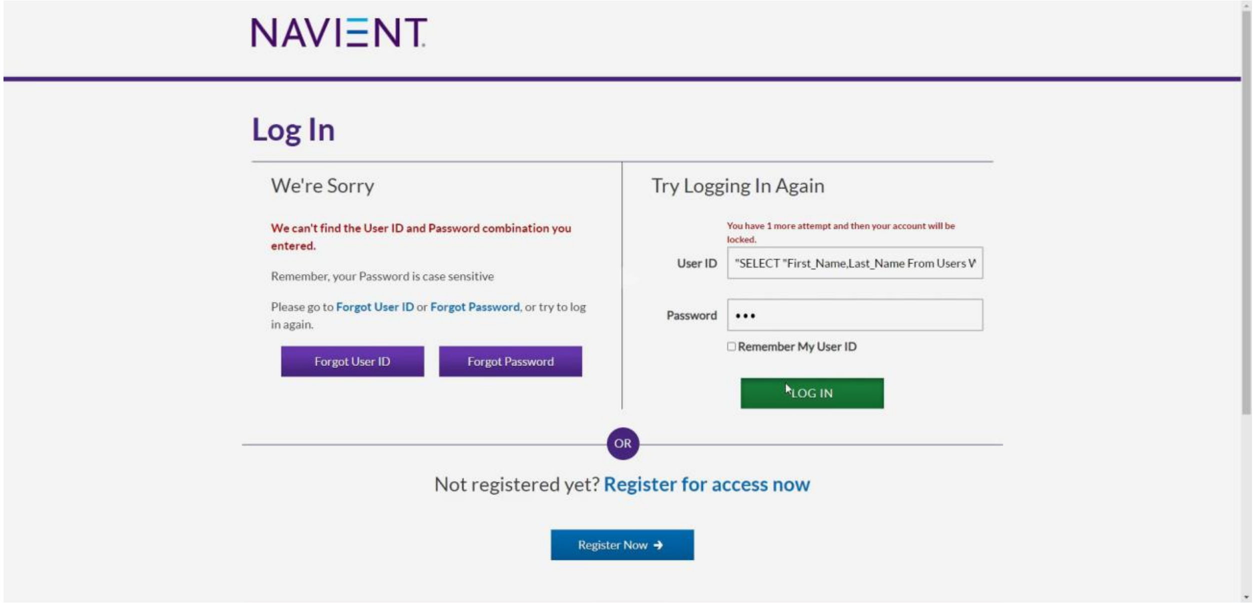
You have 2 more attempts and then your account will be locked.

User ID: User ID

Password: Password

□ Remember My User ID

Not registered yet? Register for access now



Log In

We're Sorry

We can't find the User ID and Password combination you entered.

Remember, your Password is case sensitive

Please go to Forgot User ID or Forgot Password, or try to log in again.

Try Logging In Again

You have 1 more attempt and then your account will be locked.

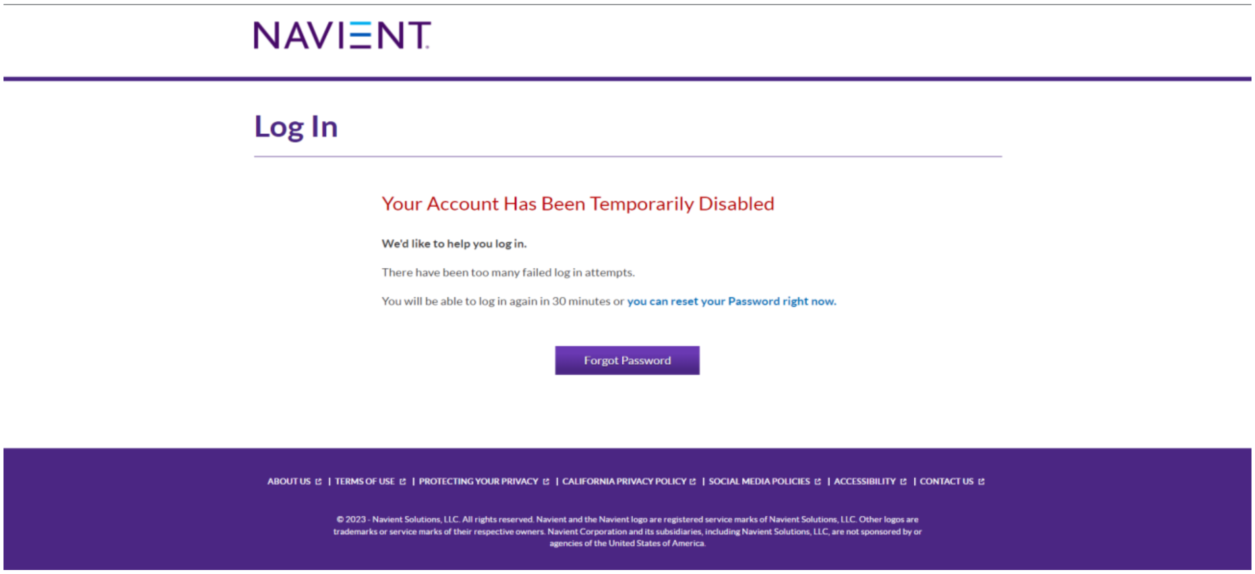
User ID: "SELECT "First_Name,Last_Name From Users V

Password: •••

□ Remember My User ID

Not registered yet? Register for access now

Again, I entered SQL Injection command to the Username and Password boxes in the login page. I used SELECT “First_Name,Last_Name FROM users WHERE ID=’1';”


NAVIENT
Forgot Password
ABOUT US | TERMS OF USE | PROTECTING YOUR PRIVACY | CALIFORNIA PRIVACY POLICY | SOCIAL MEDIA POLICIES | ACCESSIBILITY | CONTACT US

Log In

Your Account Has Been Temporarily Disabled

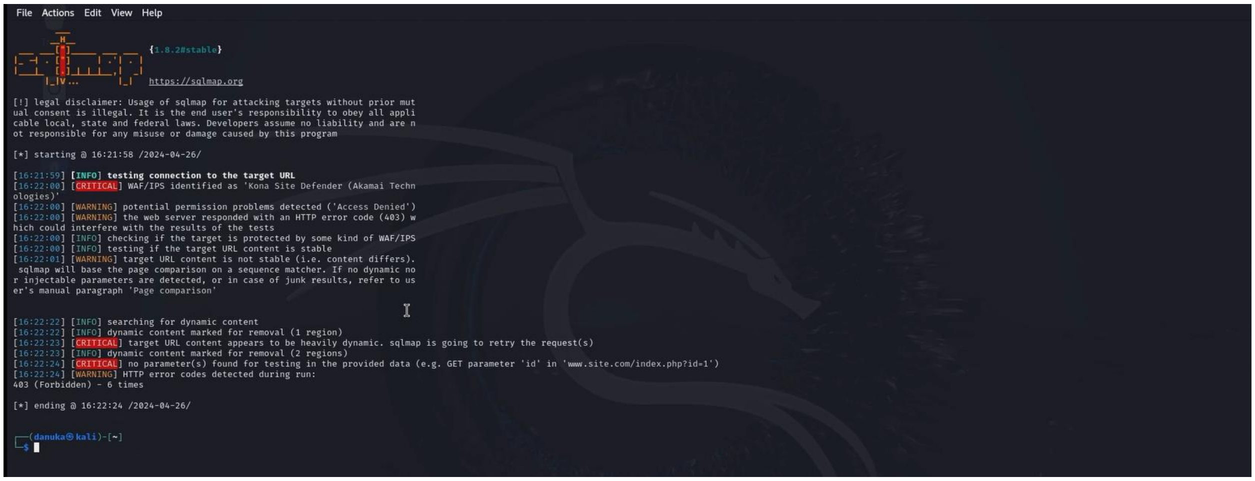
We'd like to help you log in.

There have been too many failed log in attempts.

You will be able to log in again in 30 minutes or you can reset your Password right now.

© 2023 - Navient Solutions, LLC. All rights reserved. Navient and the Navient logo are registered service marks of Navient Solutions, LLC. Other logos are trademarks or service marks of their respective owners. Navient Corporation and its subsidiaries, including Navient Solutions, LLC, are not sponsored by or agencies of the United States of America.

After I entered some commands my ip address was blocked. I think this site is more secure on that side.



```
{1.8.2#stable}

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 16:21:58 /2024-04-26/

[16:21:59] [INFO] testing connection to the target URL
[16:22:00] [CRITICAL] WAF/IPS identified as 'Kona Site Defender (Akamai Techn
ologies)'
[16:22:00] [WARNING] potential permission problems detected ('Access Denied')
[16:22:00] [WARNING] the web server responded with an HTTP error code (403) w
hich could interfere with the results of the tests
[16:22:00] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:22:00] [INFO] testing if the target URL content is stable
[16:22:01] [WARNING] target URL content is not stable (i.e. content differs).
 sqlmap will base the page comparison on a sequence matcher. If no dynamic no
r injectable parameters are detected, or in case of junk results, refer to us
er's manual paragraph 'Page comparison'


[16:22:22] [INFO] searching for dynamic content
[16:22:22] [INFO] dynamic content marked for removal (1 region)
[16:22:23] [CRITICAL] target URL content appears to be heavily dynamic. sqlmap is going to retry the request(s)
[16:22:23] [INFO] dynamic content marked for removal (2 regions)
[16:22:24] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[16:22:24] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 6 times

[*] ending @ 16:22:24 /2024-04-26/


┌──(danuka㉿kali)-[~]
└─$ 
```

Next I tried automation tool and I did not find any vulnerability.

Impact:

If this vulnerability is successfully exploited the attacker can enter the application with permissions, bypassing authentication measures. This could result in access to data, data manipulation and service disruption.

Suggested Resolution:

Implement validation and sanitization processes, for user input to ensure that data provided by users is properly sanitized before being used in SQL queries.

Use parameterized queries or prepared statements to prevent SQL injection vulnerabilities.

Make sure that the database user accounts used by the application only have the permissions needed for their tasks.

Keep the applications software components up, to date by updating and patching them regularly to fix any known security issues.

Perform security tests like vulnerability scanning and penetration testing to find and fix any vulnerabilities in the application.

Teach developers about secure coding practices and train them on how to recognize and address security risks, like SQL injection.