



VDB-308197 · CVE-2025-4482 · GCVE-100-308197

PROJECT WORLDS STUDENT PROJECT ALLOCATION SYSTEM 1.0 FORGOT_PASSWORD_SQL.PHP PAT_BLOODGROUP1 SQL INJECTION

A vulnerability classified as critical was found in Project Worlds Student Project Allocation System 1.0. Affected by this vulnerability is an unknown functionality of the file `/change_pass/forgot_password_sql.php`. The manipulation of the argument `Pat_BloodGroup1` with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is known as CVE-2025-4482. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. By approaching the search of `inurl:change_pass/forgot_password_sql.php` it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entry VDB-306495 is pretty similar.

Product

Type

- Project Management Software

Vendor

- Project Worlds

Name

- Student Project Allocation System

Version

- 1.0

License

- free

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒

VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3

VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3

VulDB Temp Score: 6.6

VulDB Vector: 🔒

VulDB Reliability: 🔍

CVSSv2

CVSSv2	CVSSv3	CVSSv4	CVSSv2	CVSSv3	CVSSv4
7.3	7.3	7.3	7.3	7.3	7.3
6.6	6.6	6.6	6.6	6.6	6.6
7.3	7.3	7.3	7.3	7.3	7.3

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Sql injection

CWE: CWE-89 / CWE-74 / CWE-707

CAPEC: 🔒

ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 
Access: Public
Status: Proof-of-Concept
Download: 
Google Hack: 
Price Prediction: 
Current Price Estimation: 



Threat Intelligence

Interest: 
Active Actors: 
Active APT Groups: 

Countermeasures

Recommended: no mitigation known
Status: 

0-Day Time: 

Timeline

05/09/2025		Advisory disclosed
05/09/2025	+0 days	VulDB entry created
05/09/2025	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4482 ()
GCVE (CVE): GCVE-0-2025-4482
GCVE (VulDB): GCVE-100-308197
scip Labs: <https://www.scip.ch/en/?labs.20161013>
See also: 

Entry

Created: 05/09/2025 01:51 PM

Changes: 05/09/2025 01:51 PM (57)

Complete: 🔍

Submitter: attackxu

Cache ID: 5:7E4:101

Submit

Accepted

- Submit #566719: projectworlds Student Project Allocation System v1.0 SQL Injection (by attackxu)

Discussion

No comments yet. Languages: en.

Please log in to comment.