**PHP Timeclock Vulnerability Disclosure**

*Multiple 0-Day Vulnerabilities Discovered in PHP Timeclock 1.0.3*

**Tyler Butler**

*Freelance Security Researcher*

Friday, May 7th, 2021

Table of Contents

[Executive Summary 3](#_Toc71157975)

[What is a Good Faith Vulnerability Disclosure? 3](#_Toc71157976)

[Identified Vulnerabilities 4](#_Toc71157977)

[Multiple Reflective Cross-Site Scripting Vulnerabilities via Get Request 4](#_Toc71157978)

[Multiple Cross-Site Scripting Vulnerabilities via Post Parameters in Reporting Tools 5](#_Toc71157979)

# Executive Summary

On May 3rd, 2021, I became aware that the Southcentral Unified School District was operating an instance of the PHP Timeclock Time Management Software on its domain timeclock.southcentralunified.org.

At first glance, it became obvious that this posed a serious vulnerability risk to your organization, as the domain was using several extremely deprecated and unsupported versions of legacy software, including php 5.3. I took it upon myself to create my own test environment for PHP Timeclock, and discovered several high-risk vulnerabilities including cross-site scripting (XSS) and SQL Injection (SQLi). This report details my findings and is considered a “Good Faith Vulnerability Disclosure”. In the sections below I will detail each finding, outlining their risk. In most vulnerability disclosures security researchers will include remediation suggestions. In this case, the only suggestion necessary is to cease the use of this domain. There are already several well-known vulnerabilities in the legacy version of PHP in use.

## What is a Good Faith Vulnerability Disclosure?

## About the Researcher

Tyler Butler is a freelance security researcher with a background in information technology, penetration testing, and software development. Outside of his professional role, he conducts freelance research on a variety of web and iOT applications. From time to time, this research results in the discovery of a 0-day vulnerability, which is so called because it is previously unknown ( or has 0 prior days of being known).

# Identified Vulnerabilities

## Multiple Reflective Cross-Site Scripting Vulnerabilities via Get Request

The PHP Timeclock application is vulnerable to reflective cross-site scripting via URL manipulation. By appending a backslash and a single quote to the get request URL, an attacker is able to insert a XSS payload to receive arbitrary JavaScript execution. In total, 4 resources are vulnerable and are listed below. Image 1 shows an example of exploiting the vulnerability on the researcher’s test environment.

1. /login.php
2. /timeclock.php
3. /reports/audit.php
4. /reports/timerpt.php

Graphical user interface, application

Description automatically generated**Image 1: Exploiting a Reflective Cross Site Scripting Vulnerability**

## Multiple Cross-Site Scripting Vulnerabilities via Post Parameters in Reporting Tools

The PHP Timeclock application is vulnerable to multiple cross site scripting vulnerabilities in the reporting functionalities of total\_hours.php, timerpt.php, and audit.php. Each of these resources is vulnerable to payload injection in the from\_date, and to\_date parameters. The effected components are listed below.

1. total\_hours.php
2. timerpt.php
3. A screenshot of a computer

   Description automatically generated with medium confidenceaudit.php

**Image 2: Exploiting a Cross Site Scripting Vulnerably in Reporting Post Parameters**

# Contact

If there are any questions about the report or its findings, please feel free to reach out to me at any of the below methods.

Email: [tcbuter320@gmail.com](mailto:tcbuter320@gmail.com)

Twitter: tbutler0x90