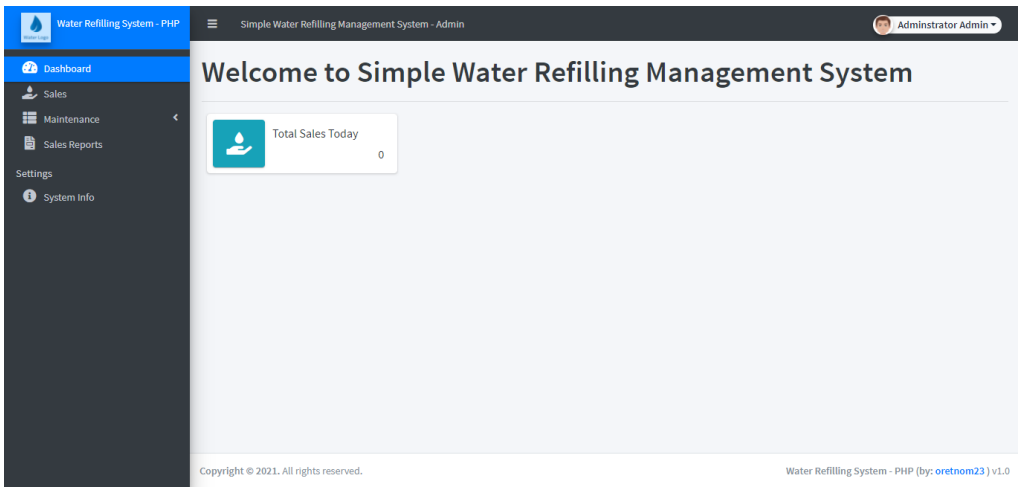
nu11secur1ty Update README.MD ... on Oct 30, 2021 History

..	
docs	last year
CVE-2021-38840.py	last year
PWNPHPSESSID.py	last year
README.MD	last year
chromedriver.exe	last year
templeate_report.txt	last year
water_refilling_0.zip	last year

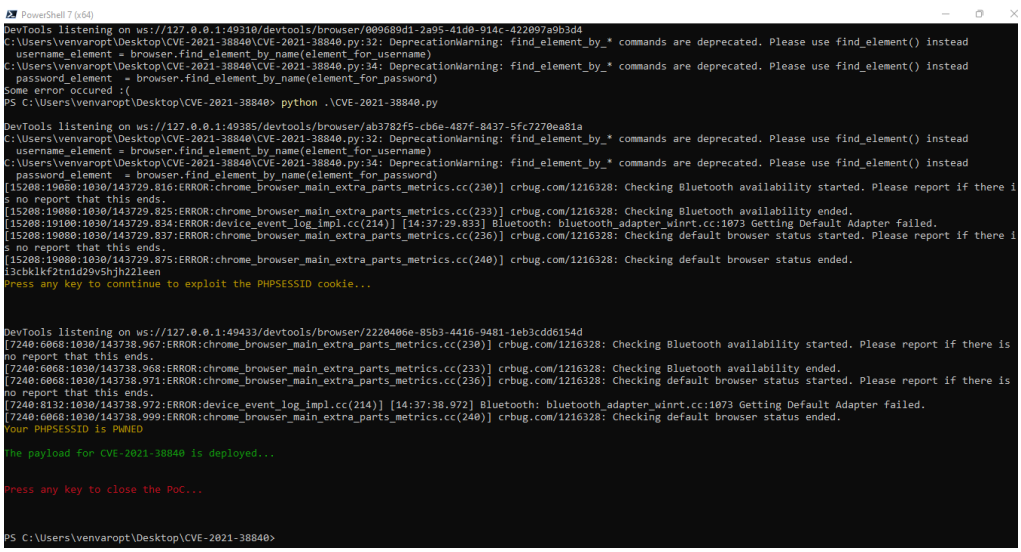
README.MD

CVE-2021-38840



Vendor

Software



Description:

The Water Refilling System - PHP (by: oretnom23) v1.0 is vulnerable to remote SQL-Injection-Bypass-Authentication + XSS-Stored Hijacking PHPSESSID

- m0re info: https://portswigger.net/support/using-sql-injection-to-bypass-authentication. The parameter (username) from the login form is not protected correctly and there is no security and escaping from malicious payloads. When the user will sending a malicious query or malicious payload to the MySQL server he can bypass the login credentials and take control of the administer account.

2. XSS - Stored PHPSESSID Vulnerable

- The vulnerable XSS app: is "maintenance", parameters: "name" After the successful SQL injection, the malicious user can be storing an XSS payload whit who can take the active PHPSESSID session.

3. remote PHPSESSID - Injection

- After the successful XSS attack the malicious user can take control of the administrative account of the system from everywhere by using the PHPSESSID, and then he can make a lot of bad things!

CONCLUSION: This vendor must STOP creating all these broken projects and vulnerable software programs, probably he is not a developer!

BR

- [+] @nu11secur1ty System Administrator - Infrastructure and Penetration Testing Engineer

Reproduce:

href

Proof:

href

BR nu11secur1ty