1) В заголовках ответа сервера отсутствует флаг HttpOnly и Secure. При добавлении в конфигурацию Nginx следующего параметра:

add\_header Set-Cookie "Path=/; HttpOnly; Secure";

происходит периодическое разлогирование пользователей (подробнее описать может Морозов С.С.).

Для чего это.

Если флаг HttpOnly (необязательно) включен в заголовок ответа HTTP, доступ к файлу cookie через клиентский скрипт невозможен. В результате, даже если существует ошибка межсайтового скриптинга (XSS), и пользователь случайно получает доступ к ссылке, которая использует эту уязвимость, браузер не будет раскрывать файл cookie третьей стороне. Установив флаг HttpOnly для файла cookie, который он создает, что указывает на то, что файл cookie не должен быть доступен на клиенте.

https://owasp.org/www-community/HttpOnly

2) На странице авторизации <https://crm.ohholding.com.ua/dashboard/> в поле для ввода логина (<input type="text" name="auth\_login" value="">), есть XSS уязвимость позволяющая выполнить произвольный javascript код.

XSS уязвимость - https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2%D1%8B%D0%B9\_%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%B8%D0%BD%D0%B3

Как воспроизвести:

в поле логина вводим, например строку "><script>alert(111)</alert> и принажатие на Enter получаем выполнение данного скрипта в браузере.