**Отчет по пентесту-номер задания 11.9 модуля 11**

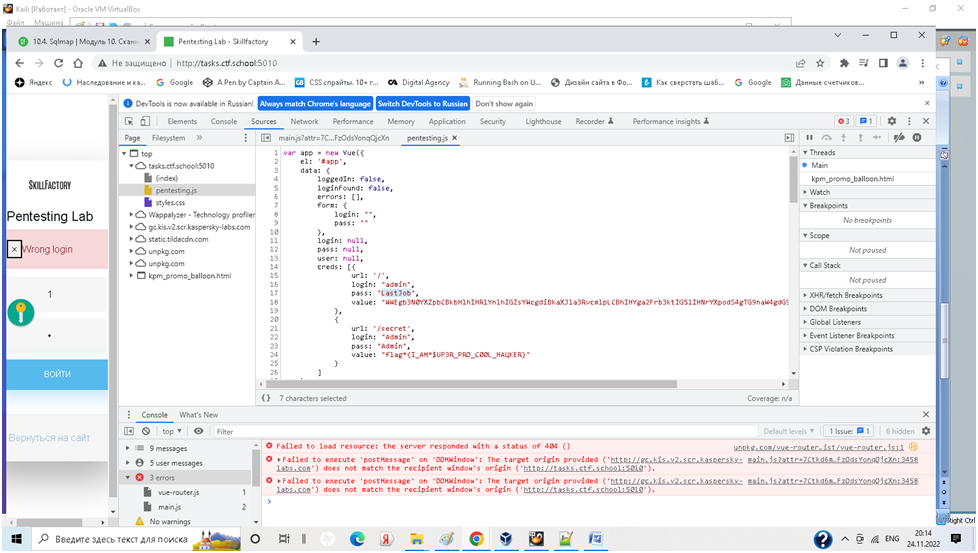
**Персонализация:** Ермакова Наталья Олеговна (natalysoliton@mail.ru)

**Лабораторная работа №11.9 “Практическая работа и отчёт по пентесту” :**

* Общая информация:
  + Период тестирования: 24.11.2022
  + Объект тестирования: http://tasks.ctf.school:5010
* Описание действий:

Для определения логина и пароля <http://tasks.ctf.school:5010/> хотела пойти по пути - использовать Burp Suite, но были некоторые тех сложности и зависания.

Пошла простым путем- посмотрела код страницы <http://tasks.ctf.school:5010/> и нашла логин и пароль в файле prntrsting.js:



секция:

creds: [{

url: '/',

**login: "admin",**

**pass: "LastJob",**

value: "WWEgb3N0YXZpbCBkbHlhIHRlYnlhIGZsYWcgdiBkaXJla3RvcmlpLCBhIHYga2Frb3ktIG5lIHNrYXpodS4gTG9naW4gdG90IHpoZSwgcGFzc3dvcmQ6IEFkbWlu"

},

{

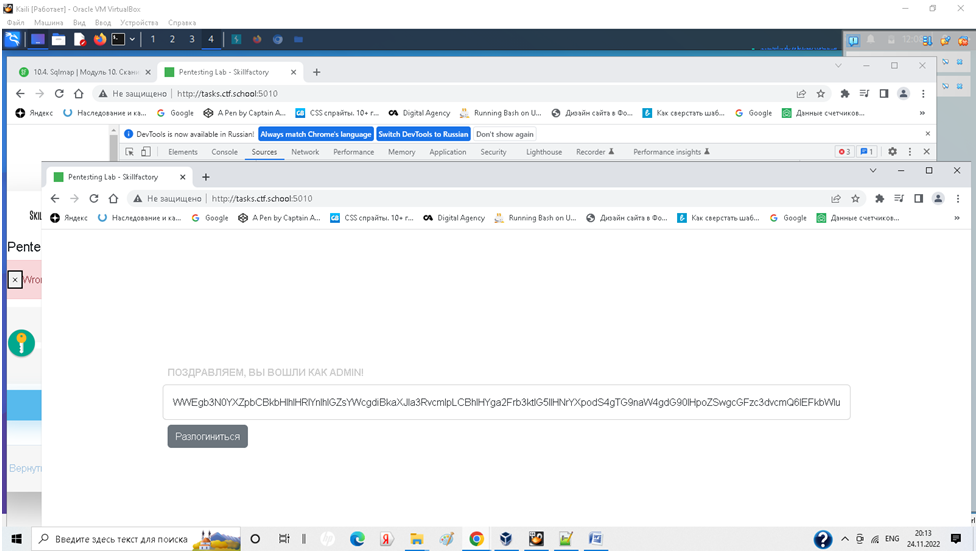
url: '/secret',

**login: "Admin",**

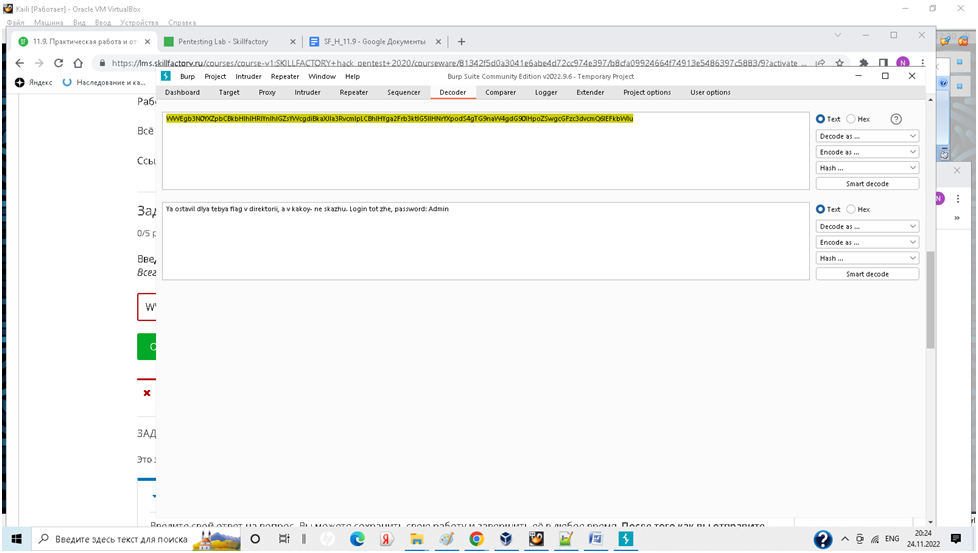
**pass: "Admin",**

**value: "flag\*{I\_AM\*$UP3R\_PRO\_C00L\_HAЦKER}"**

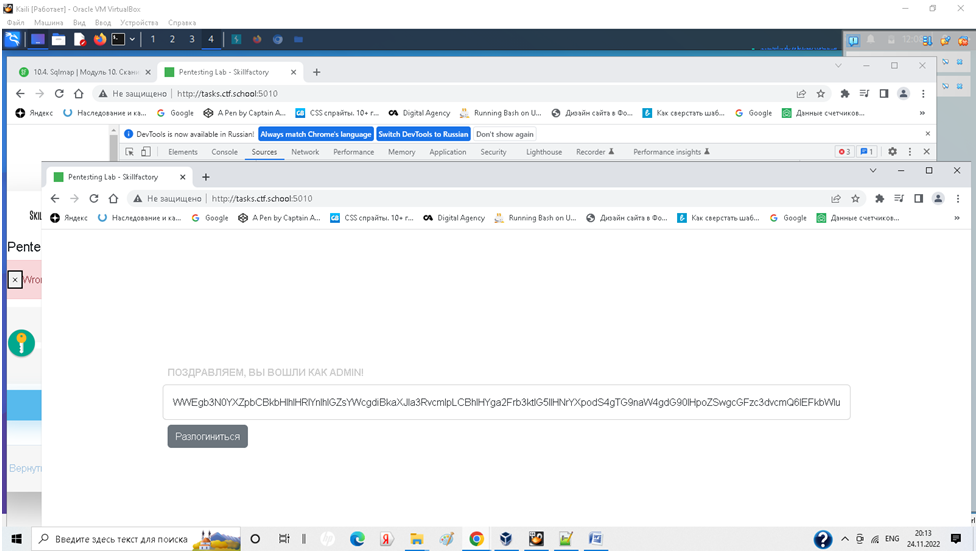
Ввела логин admin и пароль LastJob и все получилось, виден хэш, что написано выше в коде:



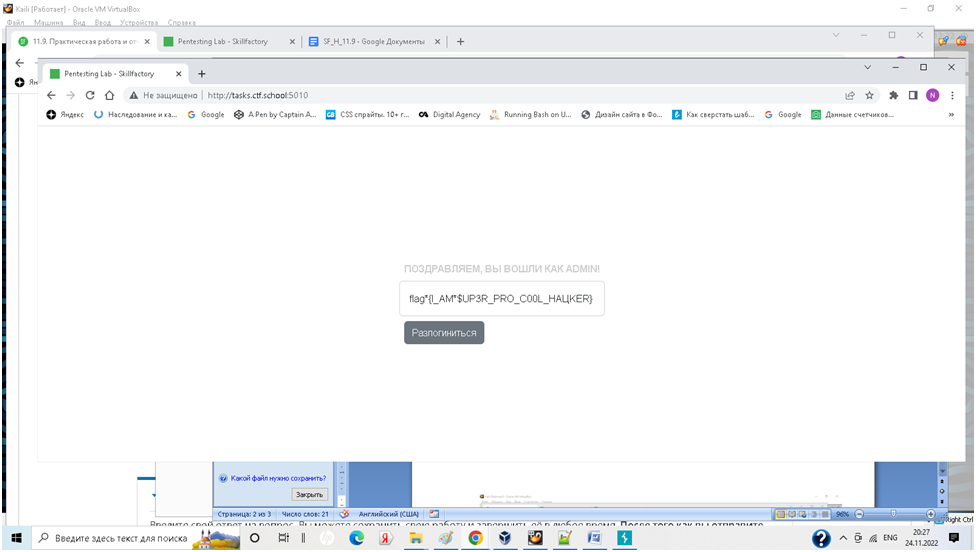
Декодировала хэш, получилось- Ya ostavil dlya tebya flag v direktorii, a v kakoy- ne skazhu. Login tot zhe, password: Admin (хотя и в коде выше видно какая директория /secret и логин с паролем одинаковые Admin):



Разлогинюсь



в урл добавлю директорию secret и введу логин и пароль Admin, получу флаг:



Кстати, видела переменную KasperskyLab :) Люблю KL :).

**Вопросы для самопроверки:**

* для декодирования использовала Burp Suite, а остальное-ручное исследование кода
* совет по защите кода, например, креды можно хранить в БД с защищенной архитектурой и использовать защищенный сертификат https.
* Мне кажется уязвимость высокой опасности 9.0.10.0 по шкале:

