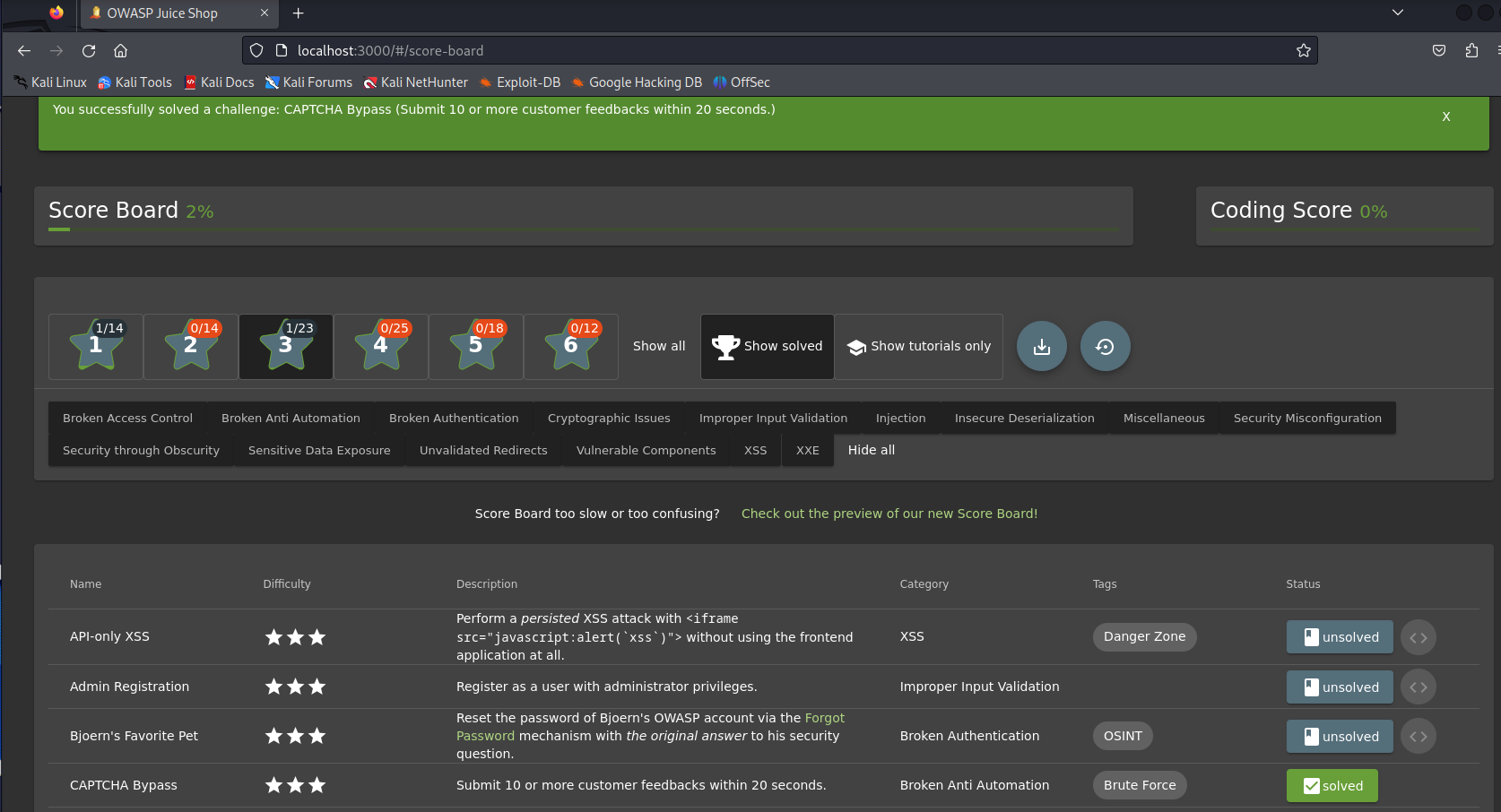
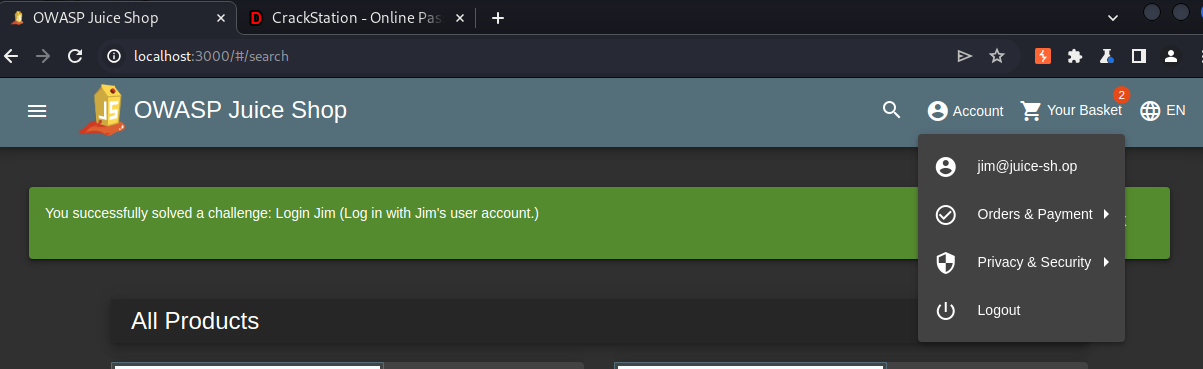
Анализ защищенности ПО. Практика.

Исходная среда: KaliLinux 2023.3. Все инструменты, утилиты и Juice Shop развернуты на этой же виртуальной машине.

1. **CAPTCHA Bypass.**  
   Краткий алгоритм:
   1. Включаем перехват.
   2. Оставляем отзыв, проходим капчу. Несколько раз.
   3. Через Proxy->HTTP history изучаем структуру получения и отправки запросов.
   4. Отправляем Request с успешными captchaID и captcha в Repeater.
   5. Через Repeater отправляем нужное количество раз.  
      Также подобный сформированный запрос можно использовать в любых программных средствах, скриптах и т.д.  
        
      
2. **Database Schema**  
   Краткий алгоритм:
   1. Включаем перехват.
   2. Через строку поиска делаем легитимный запрос.
   3. Через историю находим запрос поиска, отправляем в Repeater.
   4. Пробуем менять параметры поиска напрямую в запросе:   
      /rest/products/search?q=
   5. Добавляем к запросу одинарную ковычку.  
      Пример: ‘apple или apple’
   6. Получаем ошибку и узнаем какая база данных используется.  
      message": "SQLITE\_ERROR: near \"apple\": syntax error"
   7. В процессе экспериментов с запросом сначала получаем ошибку незавершённого запроса и добавляем две закрывающие скобки.  
      Попутно получаем:  
      
   8. Зная продукт (БД) и синтаксис пробуем к запросу поиска добавить свой:  
      UNION%20SELECT%201,2,3,4,5,6,7,8,9%20FROM%20sqlite\_master—
   9. Успех. Развиваем:  
      UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite\_master
   10. Успех. В ответе видим всю схему.  
       
3. **Login Jim**  
   Краткий алгоритм:
   1. В предыдущем этапе мы получили схему и нашли таблицу Users. Аналогично объединяя запрос получим содержимое таблицы.  
      XUY'))%20UNION%20SELECT%20id,email,password,'4','5','6','7','8','9'%20FROM%20Users--
   2. Параллельно получаем:  
      
   3. Находим пользователя Jim. В поле Description написаны символы похожие на хэш. Пробуем с ним поработать.
   4. Используем сервис crackstation.net, получаем пароль.
   5. Используем полученные данные для логина:  
      



1. **Semgrep**

Файлы помещаем в ~/scan/ и запукаем сканирование:  
  
