Отчет по лабораторной работе№4 WebGoat

Дмитрий Баринов

4 июня 2015 г.

1 Проект OWASP WebGoat

1.1 Цель работы

Исследовать безопасность Web-приложения на основе уязвимого приложения WebGoat.

1.2 Ход работы

Исследование 10 самых распространенных web-уязвимостей по рейтингу OWASP

1. **Injection** Атака на интепритатор машины-цели, позволяя выполнять произвольный код от ее имени. Чаще всего встрачаются в SQL, LDAP, Xpath, или NoSQL запросах, парсерах xml, аргументах программ и т.д.

2. **Broken Authentication and Session Management** Атака на уязвимости систем авторизации и управления сессиями с целью кражи и/или выполнения каких либо действий от чужого имени.

3. **Cross-Site Scripting** Атака на браузер путем подмены загружаемых скриптов. В результате злоумышлиниками может быть получена почти любая информация.

4. **Insecure Direct Object References** Суть атаки - изменение некого объекта, используемого в авторизированной сессии. Пример:

   ```
   String query = "SELECT * FROM accts WHERE account = ?";
   PreparedStatement pstmt = connection.prepareStatement(query , ... );

   pstmt.setString( 1, request.getParameter("acct")); <<<<<

   ResultSet results = pstmt.executeQuery( );
   ```

   Изменение параметра позволит отправлять измененные запросы от имени авторизированного пользователя.

5. **Security Misconfiguration** Ошибки в конфигурации. Атакующий может получить доступ к файлам, акаунтам, системе и т.д.

6. **Sensitive Data Exposure** Кража ценной/личной информации. Атака сложна если используется шифрование. В таком случае данные крадутся косвенными методами: на стороне клиента, когда данные уже рашифрованы, man-in-the-middle атака и другими способами.

7. **Missing Function Level Access Control** Доступ неавторизированного пользователя к привелегированным функциям. Пример:

   ```
   http://example.com/app/getappInfo
   http://example.com/app/admin_getappInfo <<<<
   ```

   Доступ к функции admin_getappInfo должен иметь только администратор. Соответственно, если пользователь, не являющийся администритором получает доступ к данной функции - это уязвимость.

8. **Cross-Site Request Forgery** Атака путем выполнения запросов к некоторому защищенному ресурсу от его имени авторизованного пользователя. Недостаток - атакующий **НЕ** может перехватить ответ от ресурса. В этом случае вводят так называемые CSRF-токены: каждый последующий пакет от клиента содержит токен, полученный в пердыдущем ответе сервера.

9. **Using Components with Known Vulnerabilities** Атака на уязвимый компонет системы, выявленный в результате сканирования.

10. **Unvalidated Redirects and Forwards** Скрытые ссылки в картинках, фреймах и т.д., ведущих на доверенный сайт. Позволяет произвести любой запрос. Пример:

    ```
    http://www.example.com/redirect.jsp?url=evil.com
    ```

1.3 Практическое задание

Подготовка Скачаны WebGoat, OWASP Mantra, OWASP Zed Attack Proxy.
Запуск WebGoat:

```
java -jar WebGoat-6.0.1-war-exec.jar
```

Проверка работоспособности: Переход по ссылке "http://localhost:8080/WebGoat".

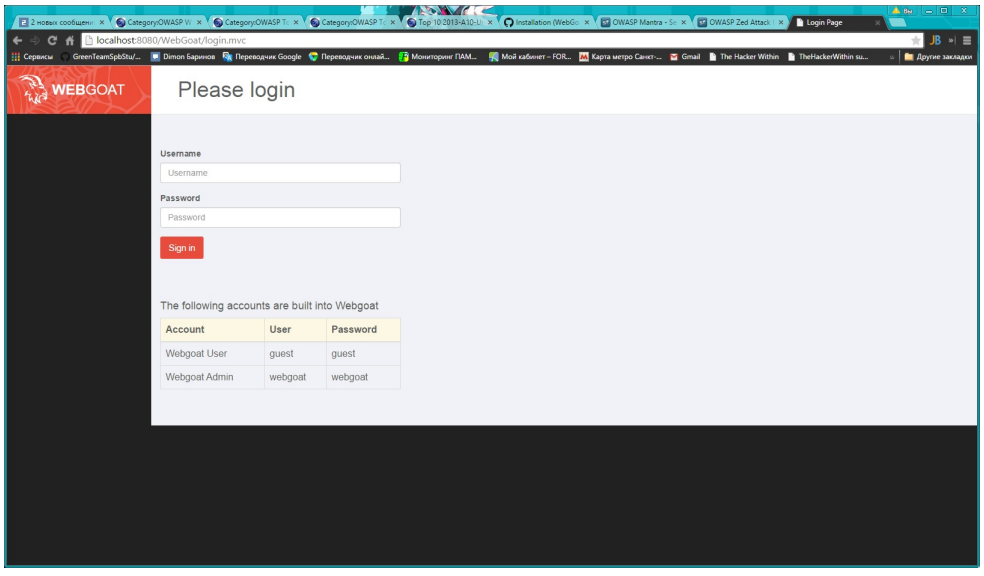

Рис. 1: Запуск WebGoat

Запуск OWASP ZAP:
Запуск OWASP MANTRA:

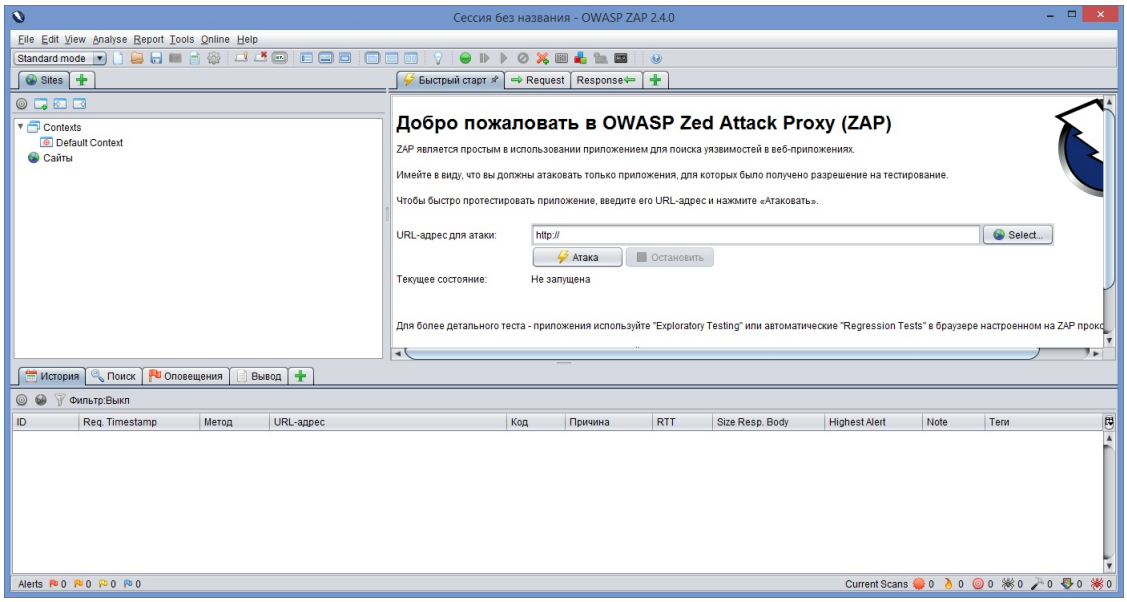

Рис. 2: Запуск ZAP

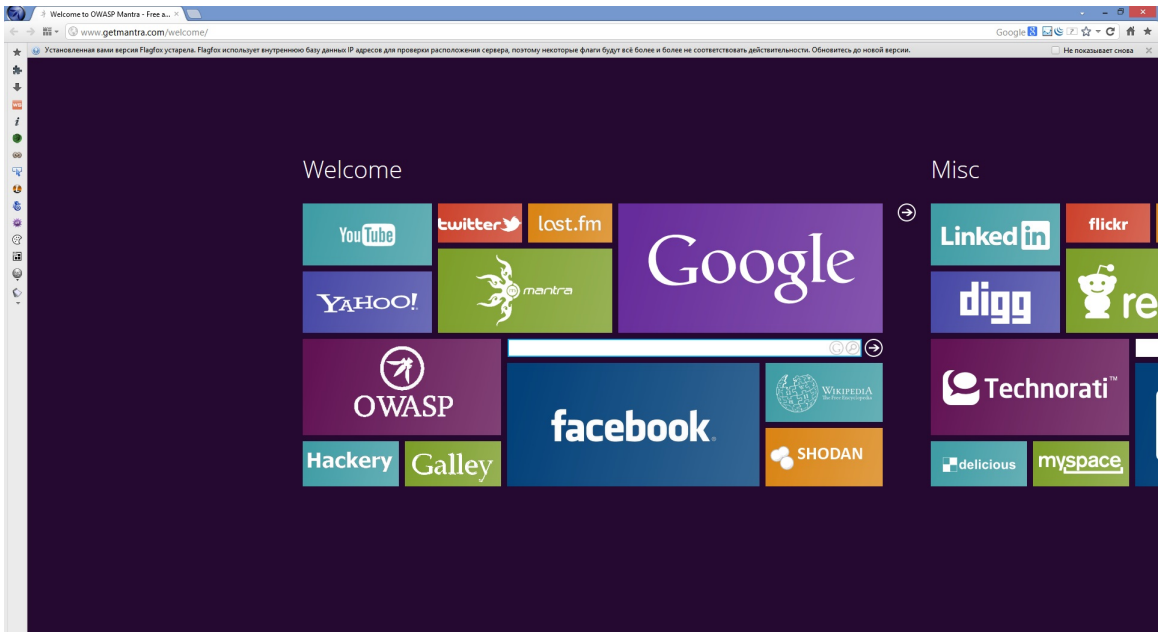

Рис. 3: Запуск MANTRA