Отчет о проведении анализа защищенности веб-приложения ООО «Экспрессо»

Содержание

1.Введение.....2
2.Обзорный отчет.....3
3. Подробный отчет о уязвимостях.....4

1.Введение

Цель данного анализа - симуляция атаки потенциального злоумышленника на веб-приложение, оценка уровня его защищенности, обнаружение уязвимостей, анализ и разработка рекомендаций по их устранению.

1.2 Объект тестирования

Для анализа предоставили границы работ по анализу защищённости, которые включают в себя:

- Исполнение произвольного кода
- Утечку персональных данных пользователей
- Получение доступа к панели администрирования веб-приложения.

1.3. Основная классификация

Каждой уязвимости, обнаруженной в ходе проведения тестирования, присваивается определенная степень риска. Критерии данной классификации указаны ниже.

Высокий
Уязвимости присваивается высокая степень риска, если ее использование может привести к компрометации данных, доступности сервера или сервисов, выполнению произвольного кода, манипуляции с данными. Сюда же входят уязвимости связанные с отказом в обслуживании, слабые или стандартные пароли, отсутствие шифрования, доступ к произвольным файлам или конфиденциальных данных.
Средний
Уязвимость средней степени риска не приводит напрямую к компрометации или неавторизованному доступу, но предоставляют возможность или информацию, которая может быть использована потенциальным злоумышленником для дальнейшего использования в совокупности с другими уязвимостями для компрометации ресурса. Например незащищенный доступ к некритичным файлам, листинг некритичных директорий, раскрытие полных путей.
Низкий
Все остальные уязвимости, которые не могут привести к компрометации ресурса, но которые могут быть использованы потенциальным злоумышленником, для сбора информации, формировании векторов атаки и т.д.

2.Обзорный отчет

2.1 Общая оценка

По результатам проведенного тестирования веб-приложения оценивается как высоко критичная, так как были обнаружены несколько уязвимостей высокой степени риска, позволяющие получить удаленный доступ к конфиденциальным данным и панели администрирования.

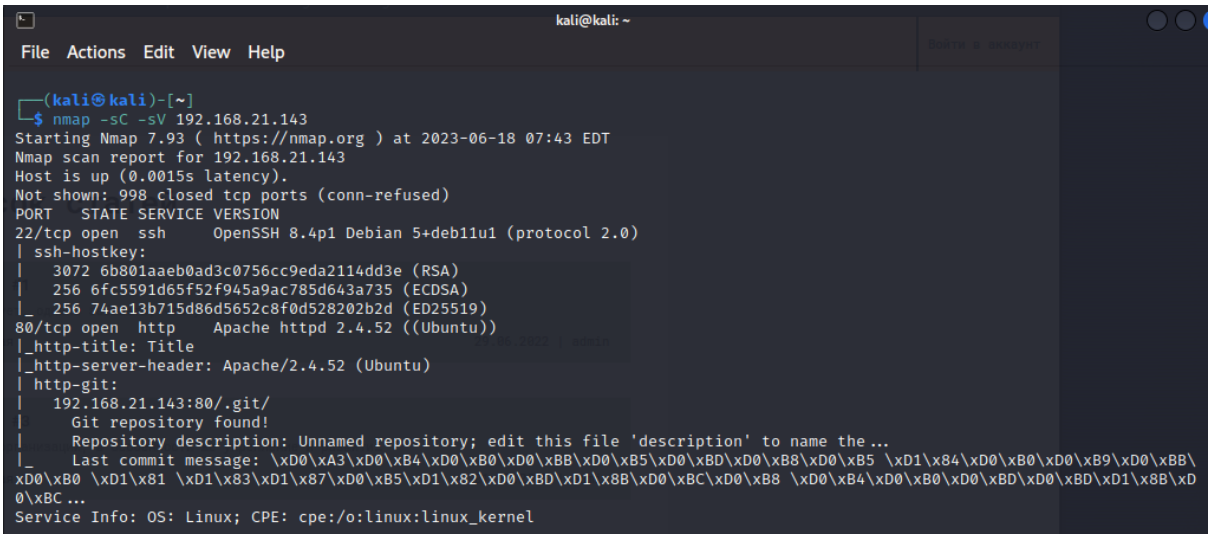
2.2 Уязвимости

Воздействия на инфраструктуру были высчетаны с помощью калькулятора общей системы оценки уязвимостей версии 3.1 (https://www-first-org.translate.goog/cvss/calculator/3.1?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc#CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

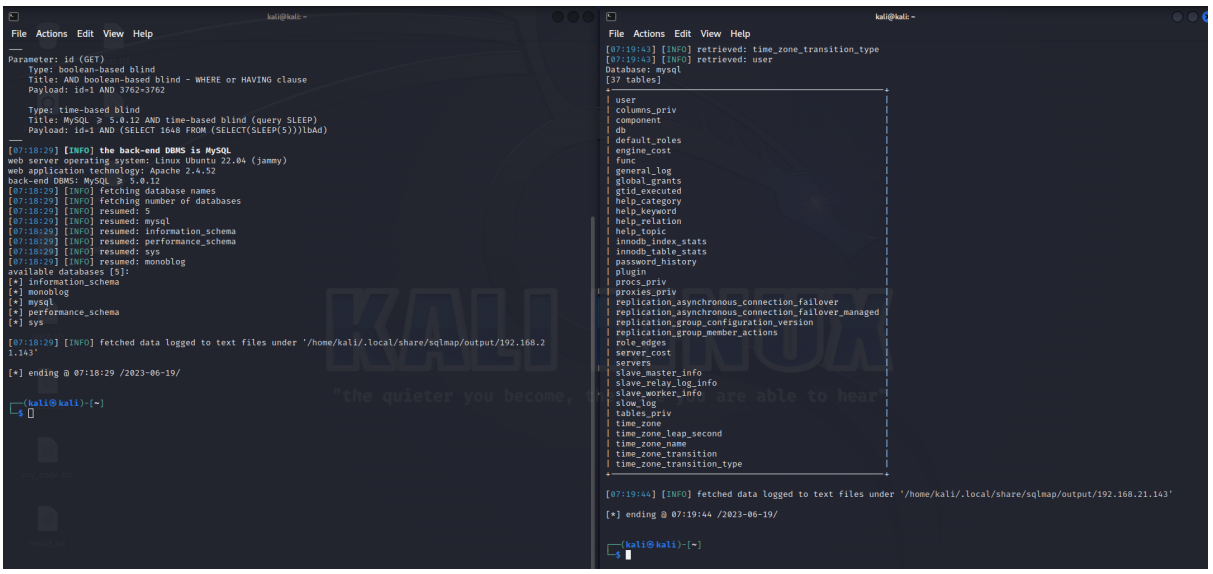
Название	**Описание**	**Воздействие (CVSS v3.1)**	**Классификация**	**Советы по исправлению**
SQL Injection	**Уязвимость к SQL инъекциям позволила получить доступ к огромному количеству конфеденциальной информации, в том числе логину и паролю администратора.**	**10**	**OWASP SQL Injection** https://owasp.org/www-community/attacks/SQL_Injection	Добавление столбца при каждой итерации проверки и/или использование оператора ORDER BY для определения количества столбцов.
Weak two-factor authentication	**Очень слабая, почти бессмысленная двухфакторная защита, которая, по сути, является “вторым паролем”**	**10**	**Owasp latest** https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy	Смена кода каждые 3-5 провальных проверки с отправкой кода на мобильное устройство администратора.

3. Подробный отчет о уязвимостях

Начинаем, как всегда, с nmap



Заходим на сайт, проверяем код страницы на наличие забытых комментов с инфой. Не находим. Запускаем Burp suite. Смотрим на сайт и “соседние страницы”. Запускаем sqlmap и проверяем на уязвимость к SQL инъекциям. В итоге уязвимость имеется, и я начинаю “купаться” в информации.

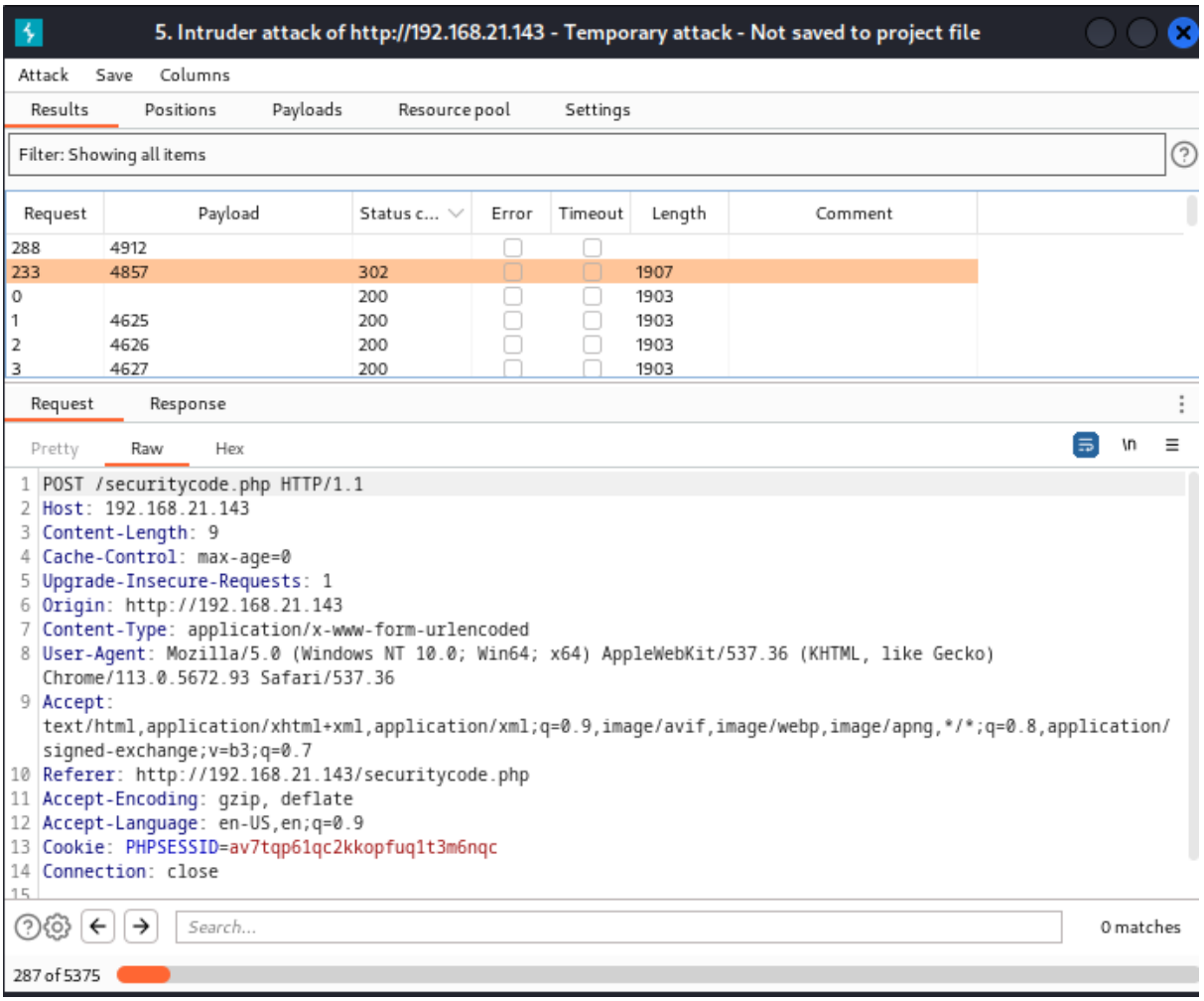


Находим логин и пароль от администратора.

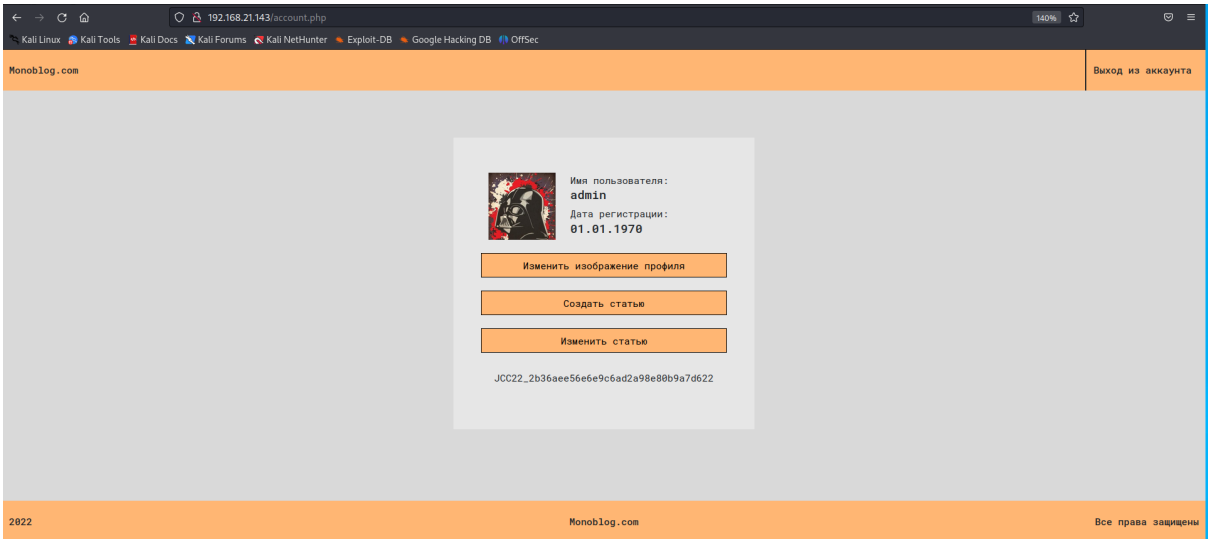
```
Table: users
[1 entry]
+----+------+-----------------------------------+----------+-----------------------------------+----------+
| id | code | image                             | is_admin | password                          | username |
+----+------+-----------------------------------+----------+-----------------------------------+----------+
| 0  | 4857 | 1546a8563dd8716f61b0ebe02db4ad1f.jpg | 1        | 21232f297a57a5a743894a0e4a801fc3 (admin) | admin    |
+----+------+-----------------------------------+----------+-----------------------------------+----------+

[11:12:57] [INFO] table 'monoblog.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.21.143/dump/monoblog/users.csv'
[11:12:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.21.143'
```

Возвращаемся в Burp suite и логинимся по найденным данным, видим “двухфакторную аутентификацию”(второй пароль). Там же видим что максимальное значения кода - 9999. Брутфорсим через Burp suite(была попытка брутфорсить через другие сервисы, в связи с очень низкой скоростью перебора в бесплатной версии, это очень сильно ударило по желаемым объемам тестирования). Получаем желаемый код.



Логинимся.



Получаем доступ к панели администратора. Тут же видим возможность изменить изображение профиля. Я на 90% уверен что там не стоит проверка на формат файла и можно закинуть веб-шел, получив полный контроль над веб-приложением, но времени на тестирование не хватило.