Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ***ИУК «Информатика и управление»***

КАФЕДРА ***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

ЛАБОРАТОРНАЯ РАБОТА №6

«Оценка безопасности web-страниц и приложений с использованием ручного и автоматизированного анализа наличия уязвимостей типа “SQL Injection”»

ДИСЦИПЛИНА: «Защита информации»

Выполнил: студент гр. ИУК4-72Б _____ (Карельский М.К.)
(Подпись)

Проверил: _____ (Ерохин И.И.)
(Подпись)

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга, 2023

Цель: освоение и систематизация знаний об уязвимостях и инструментах их выявления.

Задачи: ознакомиться с понятием уязвимостей типа «SQL Injection», принципами проверки на наличие уязвимостей и действиями в случае их обнаружения. Освоить принципы инструментального аудита безопасности информационной системы. Понять важность встраивания механизмов защиты от некорректных входных данных на этапе разработки программного обеспечения. Произвести поиск или создать собственный сайт уязвимый для SQL-инъекций. Осуществить проверку на уязвимость, предпринять действия по её устранению.

Задание:

- Найти сайт уязвимый для SQL-инъекций, используя соответствующие методы.
- Для этого же сайта использовать специализированную программу sqlmap для проверки на уязвимость.

Решение:

Обнаруженный потенциально уязвимый сайт: https://zalinux.ru/?p=411

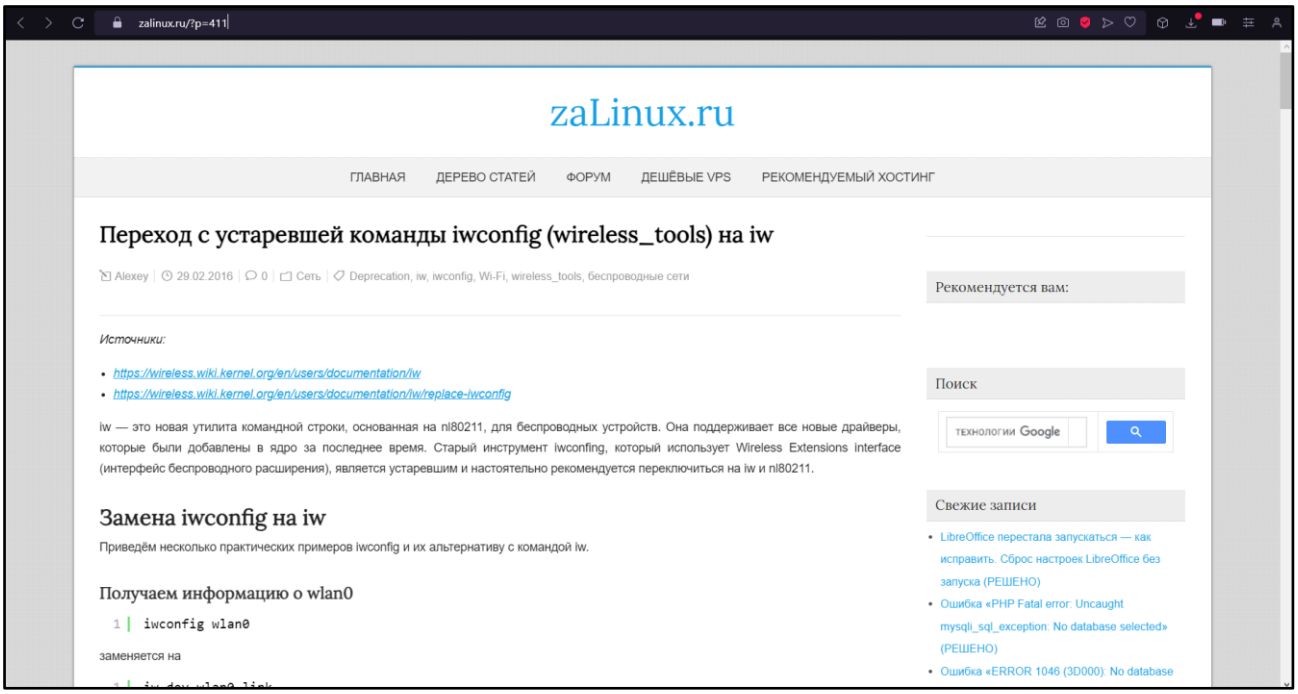

Рис. 1. Потенциально уязвимый сайт

Результат работы suIP.biz:

```
[*] starting @ 14:12:09 /2023-09-23/

[14:12:09] [WARNING] unable to create output directory
'/srv/http/.local/share/sqlmap/output' ([Errno 13] Permission denied:
'/srv/http/.local'). Using temporary directory '/tmp/sqlmapoutput376c9f9b'
instead
[14:12:09] [WARNING] unable to create history directory
'/srv/http/.local/share/sqlmap/history' ([Errno 13] Permission denied:
```

```
'/srv/http/.local'). Using temporary directory '/tmp/sqlmaphistory6s0mut9j'
instead
[1/1] URL:
GET http://zalinux.ru/?p=411
do you want to test this URL? [Y/n/q]
> Y
[14:12:09] [INFO] testing URL 'http://zalinux.ru/?p=411'
[14:12:09] [INFO] using '/tmp/sqlmapoutput376c9f9b/results-09232023_0212pm.csv'
as the CSV results file in multiple targets mode
[14:12:09] [INFO] testing connection to the target URL
[14:12:10] [WARNING] the web server responded with an HTTP error code (403)
which could interfere with the results of the tests
[14:12:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:12:10] [INFO] testing if the target URL content is stable
[14:12:11] [INFO] target URL content is stable
[14:12:11] [INFO] testing if GET parameter 'p' is dynamic
[14:12:11] [WARNING] GET parameter 'p' does not appear to be dynamic
[14:12:12] [WARNING] heuristic (basic) test shows that GET parameter 'p' might
not be injectable
[14:12:13] [INFO] testing for SQL injection on GET parameter 'p'
[14:12:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:12:15] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
[14:12:16] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER
BY or GROUP BY clause (EXTRACTVALUE)'
[14:12:19] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[14:12:22] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[14:12:24] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[14:12:27] [INFO] testing 'Generic inline queries'
[14:12:27] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[14:12:29] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries
(comment)'
[14:12:31] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE -
comment)'
[14:12:33] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[14:12:36] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[14:12:39] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[14:12:41] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one
other (potential) technique found. Do you want to reduce the number of requests?
[Y/n] Y
[14:12:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:12:50] [WARNING] GET parameter 'p' does not seem to be injectable
[14:12:50] [ERROR] all tested parameters do not appear to be injectable. Try to
increase values for '--level'/'--risk' options if you wish to perform more
tests. If you suspect that there is some kind of protection mechanism involved
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--
tamper=space2comment') and/or switch '--random-agent', skipping to the next
target
[14:12:50] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 55 times, 503 (Service Unavailable) - 21 times
[14:12:50] [INFO] you can find results of scanning in multiple targets mode
inside the CSV file '/tmp/sqlmapoutput376c9f9b/results-09232023_0212pm.csv'

[*] ending @ 14:12:50 /2023-09-23/
```

Вывод: в ходе выполнения лабораторной работы были освоены и систематизированы знания об уязвимостях и инструментах их выявления.