Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А. Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОМ ЗАДАНИИ № 5.2

по дисциплине «Проектный семинар»

по теме «Управление сеансом»

Выполнил:
Студент гр. БИБ202
Кудайбергенов Амиржан

Москва 2022

1. **Аутентификация (login)**

Аутентификация пользователя – проверка логина и пароля, открытие сессии для авторизованного пользователя. Методом POST передается пароль или логин. Если одного из элементов не хватает, в ответ отправляется malformed request. Если user не существует, в ответ отправляется no such user. Если user существует, но пароль не верен, в ответ отправляется Invalid credentials. Если указан неверный логин или пароль, события также записываются в лог безопасности. Если сессия уже авторизована, событие записывается в лог безопасности. При успешной авторизации событие заносится в лог безопасности.

```
curl --request POST \
  --url http://localhost:8006/login.php \
  -F 'username=root' \
  -F 'password=arch'
```

2. **Завершение сеанса (logout)**

Завершение сессии авторизованного пользователя. Событие заносится в лог безопасности.

```
curl --request POST \
  --url http://localhost:8006/logout.php \
  --cookie ''
```

3. **Авторизованный запрос (api)**

Запрос доступен только авторизованному пользователю. Если сессия не авторизована, событие заносится в лог безопасности.

```
curl --request GET \
  --url http://localhost:8006/api.php \
  --cookie securecookie=
```

4. **Неавторизованный запрос (public-api)**

Запрос доступен любому пользователю.

```
curl --request POST \
  --url http://localhost:8006/public.php
```

Описание механизмов безопасности:

- strict_mode - в случае, если пользователь отправляет свой (кастомный) session id, скрипт не принимает этого и создает новую (случайную сессию). Защищает от sql injection.
- only_cookies - сессия отправляется только через cookies
- maxlifetime - ограничивает время жизни сессии. После этого сессия удаляется. Защищает от утечки сессии к злоумышленнику (в том числе авторизованные)
- session_regenerate_id - генерирует и обновляет идентификатор текущей сессии.
- name -- используем кастомное имя, чтобы усложнить session hijacking
- samesite -- запрет на передачу кук в междоменный запрос
- хранение паролей в hash виде

Журналирование:

- Запись ведется в error.log
- Ошибка авторизации.
- Ошибка доступа
- Метод запроса
- Ошибка подключения к базе данных