Лабораторная работа 11

ПвИ

**Задание 01**

1. Разработайте приложение **11-01**, представляющее собой EXPRESS-HTTP-сервер, прослушивающий порт ***3000***.
2. Приложение **11-01** предназначено для предоставления аутентифицированного http-доступа к ресурсу.
3. Приложение **11-01** должно обеспечивать BASIC-аутентификацию с помощью пакета **passport**.
4. Приложение **11-01** должно реагировать на запросы к следующим ресурсам.

|  |  |
| --- | --- |
| GET /login | Ввод имени и пароля для аутентифицированного доступа к ресурсу |
| GET /logout | Отключить аутентифицированный доступ к ресурсу |
| GET /resource | Ресурс отправляет сообщение RESOURCE  При попытке неаутентифицированного доступа выполняет переадресацию на GET /login |
| Остальные URI | Сообщение со статусом 404 |

1. Список разрешенных данных для аутентификации (имя, пароль) в приложении должен быть представлен в виде json-объекта, доступ к которому осуществляется с помощью функции **require**.
2. Тестирование выполнить с помощью браузера.

**Задание 02**

1. Разработайте приложение **11-02**, представляющее собой EXPRESS-HTTP-сервер, прослушивающий порт ***3000***. Приложение **11-02** должно быть функционально подобно приложению **11-01**, но при этом использовать DIGEST- аутентификацию (пакет **passport**).

**Задание 03** Ответьте на следующие вопросы

1. Что такое аутентификация?

Аутентификация — это процесс проверки удостоверения личности пользователя или устройства, пытающегося получить доступ к системе, сети или устройству. В контексте информационной безопасности это означает подтверждение того, что пользователь действительно является тем, за кого себя выдает.

1. Перечислите все известные виды аутентификации. Какие из них описаны в RFC?

Виды аутентификации:

* BASIC (описана в RFC 7617)
* DIGEST (описана в RFC 7616)
* Форма (Form-based)
* Токен (Token-based), включая JWT
* OAuth
* SAML
* Многофакторная (MFA) или 2FA
* Биометрическая
* Сертификаты (Certificate-based)

Из них в RFC описаны BASIC и DIGEST.

1. Опишите схему BASIC-аутентификации.

* Простейшая схема, при которой имя пользователя и пароль передаются от клиента к серверу в заголовке HTTP-запроса.
* Учетные данные кодируются в base64, что не обеспечивает надежную защиту, если не использовать защищенное соединение (например, HTTPS).
* Сервер интерпретирует и проверяет эти учетные данные, после чего предоставляет доступ к ресурсу или возвращает ошибку аутентификации.

1. Опишите схему DIGEST-аутентификации.

* Более безопасный вариант по сравнению с BASIC.
* Вместо отправки открытых учетных данных клиент отправляет "отпечаток" пароля, полученный с помощью хеширования. В процессе используется nonce (одноразовое случайное число, отправляемое сервером), что делает каждый запрос уникальным.
* Помимо учетных данных, в процесс могут включаться URL и метод запроса, что увеличивает безопасность.
* Аутентификация основана на подтверждении знания клиентом секрета (пароля), не требуя его открытой передачи.