Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Техгологии и методы программирования»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

Выполнил:
Михайлик Антон Денисович, студент группы N3351

(Подпись)

Проверил:
Ищенко Алексей Петрович

(Отметка о выполнении)

(Подпись)

Санкт-Петербург
2024 г.

Содержание

Содержание **2**

1 Техническое задание **3**

1.1 (A) 3

1.2 (B) 3

2 Выполнение задания A **4**

3 Выполнение задания B **4**

1 Техническое задание

Требуется реализовать следующее:

1.1 (A)

1. Написать программу-инсталлятор sys_doc.exe, которая под видом установки обновления (с отображением строки прогресса обновления) к Pain.exe:
   - Запрашивает у пользователя папку (должен быть вариант использования существующей папки и вариант создания собственной) для установки обновления.
   - Собирает (возможную) информацию о компьютере, на котором устанавливается программа.
   - Кодирует эту информацию и записывает в файл sys.tat.
   - Хеширует ее с использованием личного ключа пользователя программы и записывает это всё, в реестр Windows в раздел HKEY_CURRENT_USER \Software\Фамилия_студента как значение параметра Signature.
   - Защищает файл sys.tat от редактирования, просмотра и копирования, а также делает его невидимым для пользователя
2. Написать программу secur.exe для того, чтобы пользователь смог получить доступ к файлу sys.tat.
3. При неудачной проверке работа защищаемой программы должна прекращаться с выдачей соответствующего сообщения.
4. Собираемая о компьютере информация включает в себя как минимум:
   - Имя пользователя,
   - Имя компьютера,
   - Конфигурацию компьютера (память и процессор, как минимум) и версию ОС.

1.2 (B)

1. Создать скрипт, который удалённо и незаметно для пользователя (пользователь открывает какую-нибудь веб-страничку от создателя скрипта) собирает информацию о нём, его компьютере и системе и записывает её на какой-либо локальный сетевой диск (доступный создателю скрипта) в папку с именем IP или Mac-адреса пользовательской машины.
2. Продумать доступ к этой информации (можно писать на удалённый диск).
3. Протестировать на 3–5 клиентах и получить статистику о них.

2 Выполнение задания A

3 Выполнение задания B

Для того, чтобы можно было получать данные о пользователе, который заходит на страницу, было нписано лёгкое мини приложение, которое расположено на http://188.243.207.170:9999/ и отображает информацию о последних 5-ти запросах.

Интерфейс данного приложения:

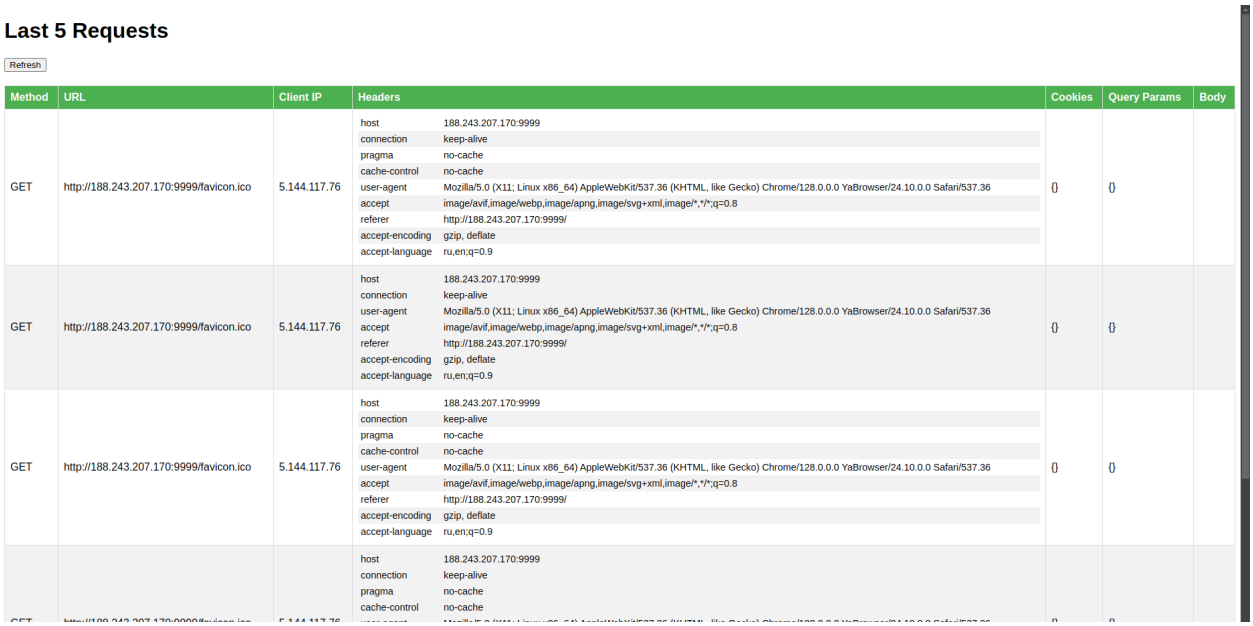


Рис. 1: Приложение, которое ловит запросы

Итак, изначальное приложение представляет из себя игру "змейка". Пользователь заходит на страницу и играет в змейку, а в это время js код отправляет всю информацию, которую он смог вытащить из пользователя на сервер, который ловит запросы.

Интерфейс игры змейки, после которого отправляется запрос с данными юзера:

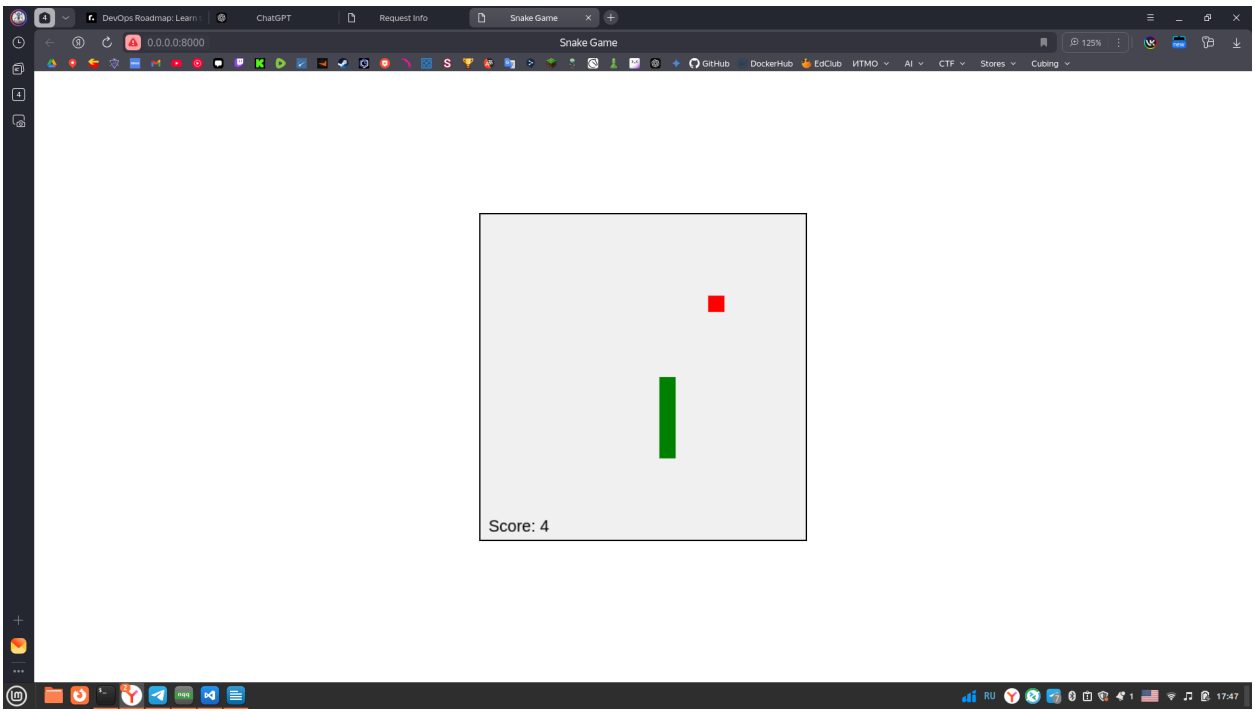


Рис. 2: Приложение, которое ловит запросы

JavaScript в браузере работает в песочнице, это означает, что он не может получить доступ к железу юзера, но всё равно есть способ с помощью JavaScript узнать много информации о пользователе. Приведем изображение запроса, который был пойман.

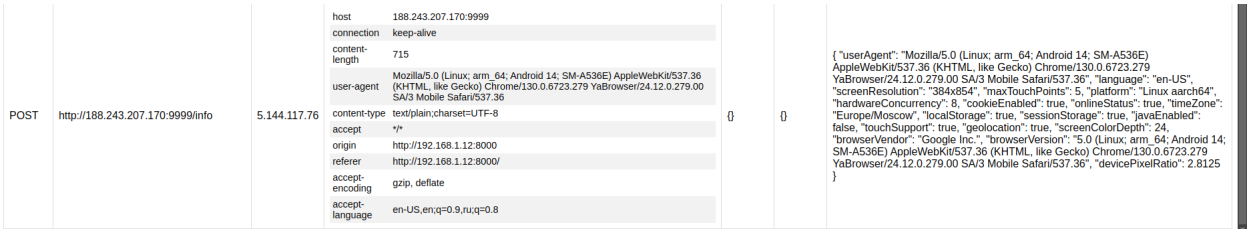
POST	http://188.243.207.170:9999/info	5.144.117.76	host: 188.243.207.170:9999 connection: keep-alive content-length: 633 user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 YaBrowser/24.10.0.0 Safari/537.36 content-type: text/plain;charset=UTF-8 accept: */* origin: http://0.0.0.0:8000 referer: http://0.0.0.0:8000/ accept-encoding: gzip, deflate accept-language: ru,en;q=0.9	{}	{}	{ "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 YaBrowser/24.10.0.0 Safari/537.36", "language": "ru", "screenResolution": "1920x1080", "maxTouchPoints": 0, "platform": "Linux x86_64", "hardwareConcurrency": 16, "cookieEnabled": true, "onlineStatus": true, "timeZone": "Europe/Moscow", "localStorage": true, "sessionStorage": true, "javaEnabled": false, "touchSupport": false, "geolocation": true, "screenColorDepth": 24, "browserVendor": "Google Inc.", "browserVersion": "5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 YaBrowser/24.10.0.0 Safari/537.36", "devicePixelRatio": 1.25 }

Рис. 3: Запрос после игры в змейку

Информация содержащаяся в теле запроса:

```
{ "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/128.0.0.0 YaBrowser/24.10.0.0 Safari/537.36", "
  language": "ru", "screenResolution": "1920x1080", "maxTouchPoints": 0,
  "platform": "Linux x86_64", "hardwareConcurrency": 16, "cookieEnabled":
    true, "onlineStatus": true, "timeZone": "Europe/Moscow", "localStorage
  ": true, "sessionStorage": true, "javaEnabled": false, "touchSupport":
  false, "geolocation": true, "screenColorDepth": 24, "browserVendor": "
  Google Inc.", "browserVersion": "5.0 (X11; Linux x86_64) AppleWebKit
  /537.36 (KHTML, like Gecko) Chrome/128.0.0.0 YaBrowser/24.10.0.0 Safari
  /537.36", "devicePixelRatio": 1.25 }
```

Здесь мы можем увидеть много интересной информации, такой как операционная система, браузер, maxTouchPoints (0 если это компьютер и >0 если это телефон или планшет), timeZone и т.п.



POST	http://188.243.207.170:9999/info	5.144.117.76	host: 188.243.207.170:9999 connection: keep-alive content-length: 715 user-agent: Mozilla/5.0 (Linux; arm_64; Android 14; SM-A536E) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.279 YaBrowser/24.12.0.279.00 SA/3 Mobile Safari/537.36 content-type: text/plain;charset=UTF-8 accept: */* origin: http://192.168.1.12:8000 referer: http://192.168.1.12:8000/ accept-encoding: gzip, deflate accept-language: en-US,en;q=0.9,ru;q=0.8	{}	{}	{ "userAgent": "Mozilla/5.0 (Linux; arm_64; Android 14; SM-A536E) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.279 YaBrowser/24.12.0.279.00 SA/3 Mobile Safari/537.36", "language": "en-US", "screenResolution": "384x854", "maxTouchPoints": 5, "platform": "Linux aarch64", "hardwareConcurrency": 8, "cookieEnabled": true, "onlineStatus": true, "timeZone": "Europe/Moscow", "localStorage": true, "sessionStorage": true, "javaEnabled": false, "touchSupport": true, "geolocation": true, "screenColorDepth": 24, "browserVendor": "Google Inc.", "browserVersion": "5.0 (Linux; arm_64; Android 14; SM-A536E) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.279 YaBrowser/24.12.0.279.00 SA/3 Mobile Safari/537.36", "devicePixelRatio": 2.8125 }

Рис. 4: Запрос, который пришёл с телефона

Информация содержащаяся в теле запроса:

```
{ "userAgent": "Mozilla/5.0 (Linux; arm_64; Android 14; SM-A536E)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.279 YaBrowser
   /24.12.0.279.00 SA/3 Mobile Safari/537.36", "language": "en-US", "
   screenResolution": "384x854", "maxTouchPoints": 5, "platform": "Linux
   aarch64", "hardwareConcurrency": 8, "cookieEnabled": true, "
   onlineStatus": true, "timeZone": "Europe/Moscow", "localStorage": true,
    "sessionStorage": true, "javaEnabled": false, "touchSupport": true, "
   geolocation": true, "screenColorDepth": 24, "browserVendor": "Google
   Inc.", "browserVersion": "5.0 (Linux; arm_64; Android 14; SM-A536E)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.279 YaBrowser
   /24.12.0.279.00 SA/3 Mobile Safari/537.36", "devicePixelRatio": 2.8125
   }
```

Здесь тоже можем обнаружить много полезной информации. Стоит обратить внимание на maxTouchPoints, которое здесь равно 5, что указывает, что это телефон.