**Практика 1. Безопасность веб-приложений. Ручной базовый анализ.**

Одним из первых этапов анализ веб-приложения является базовый ручной анализ. Первым действием ручного анализа обычно является исследования исходного кода с помощью веб-браузера. Однако, не стоит думать, что будет отображён исходный код серверной части веб-приложения (то есть исходный код языка на котором написана серверная часть веб-приложения, например, PHP, Python и др.). При использовании браузера можно получить только исходный код HTML, JS, CSS элементов веб-приложения, что чаще всего поможет лишь собрать некую информацию, касающуюся клиентской части веб-приложения. Несмотря на это, иногда можно получить информацию об внутреннем устройстве веб-приложения или информацию касающуюся системных файлов (бэкапов, предыдущих версий скриптов и др.).

1. **Анализ исходного кода.**

Для того чтобы открыть исходных код, необходимо в используемом браузере открыть выпадающее меню (с помощью ПКМ) и выбрать пункт “View Page Source”.



После этого в браузере отобразиться исходный код, в котором можно увидеть все HTML заголовки и тэги, а также комментарии, что часто бывает очень полезно, если разработчики оставили там какую-либо информацию, касательно работы веб-приложения.



Также можно просто написать в браузере “view-source:” в строке запроса перед адресом сайта.

Часто в заголовке кода можно заметить секцию подключения сторонних файлов со стилями или JS-кодом для клиентской части. Это могут быть файлы как на данном сайте, так и файлы на удалённых сайтах, на которые ваш браузер должен будет обратиться.



В данных файлах также могут содержаться какие-либо полезные данные, однако не стоит на них зацикливаться, особенно если это часто используемые стили или JS-компоненты.

1. **Robots.txt**

Данный файл может быть очень полезен при анализе большого веб-приложения, часто неопытные разработчики могут оставить там ссылки на файлы, которые хотят скрыть от поисковых роботов, таких как Google, Яндекс и других. Для доступа к этому файлу достаточно обратиться к нему с корня сайта: http://ip-address/robots.txt



Далее можно проверить каждую из ссылок и просмотреть что от нас хотели скрыть, хотя и довольно простым способом.

1. **Исследование элементов. Сеть.**

В меню, через которое открывает исходный код сайта, можно также открыть так называемые” Инструменты разработчика” которые позволяют подробно изучить ответы от веб-приложения, элементы и их составляющие. Чаще всего исследователи пользуется ими для базового анализа ответов от веб-приложения, просмотра заголовков и прочей сетевой информации.



После этого внизу браузера откроется панель с несколькими вкладками, для открытия вкладки отвечающей за ответы от веб-приложения необходимо кликнуть по названию “Network”.



После этого нужно перезагрузить страницу и будут отображены запрос и ответ от веб-приложения.



Слева можно увидеть заголовки запроса от нашего браузера (клиента) и заголовки ответа от веб-приложения (сервера), иногда в заголовках можно найти нестандартные поля, или, например, куки, в которых могут содержаться какие-либо данные. Также куки могут быть уязвимы, если обладают слабой криптографий, при этом храня важные данные, например, данные об уровне доступа аккаунта.

Куки можно увидеть в обоих типах заголовках, однако они будут находится в разных полях. В заголовках клиента это Cookie: xxxx, а в заголовках сервера это поле Set-Cookie: xxxx.

**Задание на практику.**

Произвести базовый анализ 3 различных веб-приложений, найдя контрольные значения на каждом из веб-приложений (на одном веб-приложении может быть не одно контрольное значение, а несколько).

Адреса веб-приложений в локальной сети необходимо получить у преподавателя.

Составить отчёт об анализе веб-приложений с кратким описанием производимых действий, а также контрольными значениями.

За каждое из выполненных заданий практики (всего 3) студент получает + 1 балл.