DPA Frontend Threat Modeling Framework

Фреймворк моделирования угроз для frontend-приложений

DPA ANALYTICS

Frontend Kill Chain

Тип вектора

- Зависимости js-приложения
- Внешние сервисы
- Тег-менеджеры
- Компрометация веб-сервера
- Инсайдеры
- Атаки
- Расширения браузера

Вектор

T-01	Компрометация сервера приложения, добавление вредоносного скрипта (file/inline) в код страниц
T-02	Компрометация сервера приложения, добавление вредоносного активного элемента (iframe, form и другие)
T-03	Компрометация сервера приложения, добавление вредоносного кода в js-файлы (без изменения логики приложения/заголовков CSP/атрибутов integrity)
T-04	Компрометация сервера приложения, добавление вредоносного кода в js-файлы (с изменением логики приложения/заголовков CSP/атрибутов integrity)
T-05	Компрометация CDN, добавление вредоносного кода в js-файлы
T-06	Целевая атака / фишинг. Злоумышленники предложили маркетологам попробовать инновационную систему аналитики для сайта. Скрипт злоумышленников подключен к приложению по запросу маркетологов
T-08	Stored XSS. Вредоносный код выполняется у значительного числа пользователей
T-09	Reflected XSS
T-10	Добавление вредоносного кода в стороннюю opensource-библиотеку (зависимость)
T-11	Добавление вредоносного кода в стороннюю проприетарную библиотеку (зависимость)
T-12	Добавление вредоносного кода в библиотеку для сборки / минификации / обфускации / автоформатирования кода
T-13	Добавление НДВ в стороннюю библиотеку (зависимость) авторами библиотеки
T-14	Компрометация доверенного внешнего js-сервиса (например, сторонняя система аналитики)
T-15	Компрометация учетной записи системы управления тегами (Google Tag Manager (GTM) и аналоги), злоумышленник добавляет вредоносный код на страницы приложения при инициализации тег-менеджера
T-18	Доверенный внешний js-сервис выполняет разные действия в зависимости от IP/региона/устройства/часового пояса пользователя
T-19	Разработчик добавил вредоносный код в приложение умышленно
T-20	Разработчик добавил вредоносный код в приложение по ошибке (например, скопировал код из ненадежного источника, в том числе код, сгенерированный нейросетями/AI-ассистентами)
T-21	Сотрудник с целью личной выгоды умышленно разместил на страницах js-майнер
T-22	Сотрудник с целью личной выгоды умышленно разместил на страницах трекер/пиксель/ретаргетинг конкурентов
T-23	Сотрудник с целью личной выгоды умышленно разместил на страницах ссылки на сторонние сайты (торговля ссылками в SEO)
T-24	Расширения браузера, либо код, внедренный через расширения (например, Tampermonkey), похищают данные со страницы и отправляют на хост злоумышленника
T-25	Расширения браузера, либо код, внедренный через расширения (например, Tampermonkey), выполняют изменение страниц приложения (с сохранением активных элементов на странице)

Технический вектор

- Внедрён вредоносный js-код
- Внедрён активный элемент (iframe, form...)

Способ реализации / монетизации

T-07	Злоумышленник добавляет дополнительный скрипт системы аналитики, к которой он имеет доступ, при наличии легитимного скрипта данной системы аналитики на страницах
T-16	Доверенный внешний js-сервис (например, сторонняя система аналитики) злоупотребляет доступом к данным посетителя web-страницы (избыточный сбор данных)
T-17	Использование функции системы аналитики, собирающей полный код web-страниц, нажатия клавиш пользователем и другие действия
T-26	Кража токенов/секретов/учетных данных и отправка на хост злоумышленника
T-27	Кража персональных данных в "явном" виде (ФИО, телефон, электронная почта и т.п.) и отправка на хост злоумышленника
T-28	Кража персональных данных в виде данных о поведении, геолокации, уникальном идентификаторе пользователя, цифровом отпечатке браузера и отправка на хост злоумышленника
T-29	Скрипт выполняет загрузку (имитацию загрузки) файла (pdf, docx, xlsx и др.) с эксплойтом для заражения устройства пользователя. Пользователь доверяет frontend-приложению, открывает загруженный файл - выполняется эксплуатация уязвимости ПО для просмотра данного файла, происходит заражение устройства пользователя
T-30	Скрипт выполняет майнинг криптовалюты за счет вычислительных ресурсов устройства пользователя.
T-31	Несанкционированная запись в буфер обмена
T-32	Подмена данных при копировании данных в буфер обмена
T-33	Снятие цифрового отпечатка (фингерпринта) браузера/устройства пользователя
T-34	Несанкционированный доступ к геолокации пользователя
T-35	Несанкционированный доступ к микрофону, веб-камере, захвату экрана
T-36	Несанкционированный доступ к показу браузером уведомлений операционной системы (Notification API)
T-37	Несанкционированный доступ к показу браузером push-уведомлений в мобильном устройстве
T-38	Несанкционированное чтение cookie
T-39	Несанкционированное чтение localstorage
T-40	Несанкционированное чтение буфера обмена
T-41	Несанкционированное обращение к другим критичным WebAPI браузера
T-42	Выполнение редиректа пользователя на вредоносный / фишинговый /рекламный сайт
T-43	Показ фишинговых баннеров / форм оплаты / форм сбора данных / форм привязки криптокошелька
T-44	Показ фишинговых уведомлений ОС / push-уведомлений на мобильном устройстве через Notification API браузера
T-45	Вредоносный код выполняется только при определенном действии (клик по кнопке логин/оплатить/отправить)
T-46	Вредоносный код производит отправку украденных данных в момент закрытия вкладки (событие unload), чтобы затруднить обнаружение при ручном анализе
T-47	Вредоносный код выполняется только при определенных условиях/триггерах в js-коде (часовой пояс, время, дата, язык, размер экрана, тип устройства, браузер и другие)
T-48	Clickjacking. Злоумышленник (или вредоносный скрипт) добавляет на страницу невидимый iframe, в котором открыта страница социальной сети / интернет-магазина / банка / другого ресурса, в котором пользователь авторизован в данном браузере. При выполнении клика по такому iframe пользователь делает клик, например, по кнопке Подписаться/поставить лайк в социальной сети
T-49	CSRF. Злоумышленник (или вредоносный скрипт) добавляет на страницу приложения элемент (iframe, img и т.п.) для выполнения в браузере пользователя сетевого запроса к другому web-приложению с целью выполнить определенное действие от имени пользователя

Последствия

- Утечка персональных данных
- Frontend-фишинг
- Js-майнинг
- Действия от имени пользователя
- Заражение устройства пользователя
- "Чёрное" SEO

Ущерб

- Финансовый ущерб клиентам
- Снижение прибыли
- Участие в уголовном деле
- Репутационный ущерб
- Штрафы по 152-ФЗ
- Санкции регуляторов (ЦБ, GDPR и т.д.)

Онлайн-сервис для моделирования угроз для frontend-приложений

Бесплатный сервис для создания модели угроз для Вашего frontend-приложения с оценкой рисков, подробным перечнем мер противодействия, обоснованием их эффективности и планом внедрения.

https://dpa-analytics.ru/frontend-threat-model

Telegram-канал FrontSecOps

В канале публикуются разборы инцидентов, лучшие практики по безопасной разработке frontend-приложений, обзоры инструментов, аналитика угроз, а также актуальные риски и методы защиты современных js-приложений.

https://t.me/FrontSecOps

Невыполнение требований регуляторов

T-64	(РКН) Трансграничная передача ПД пользователя со страниц frontend-приложения без предварительного уведомления регулятора
T-65	(РКН) Несоответствие политики конфиденциальности, политики обработки ПД, согласий на сайте фактически выполняемым действиям в frontend-приложении (передача данных третьим лицам, трансграничная передача)
T-66	(РКН) Использование зарубежных сервисов / БД за пределами РФ
T-67	(РКН) Повышение вероятности / частоты проверок регулятора (при использовании на сайте иностранных сервисов и трансграничной передаче ПД)
T-68	(HCПК, PCI DSS) Отсутствие актуальной инвентаризации скриптов с письменным обоснованием необходимости каждого из них
T-69	(HCПК, PCI DSS) Отсутствие контроля целостности каждого скрипта (не реже, чем 1 раз в 7 дней)
T-70	(HCПК, PCI DSS) Отсутствие контроля изменений HTTP-заголовков на платежных страницах (в том числе Content Security Policy (CSP)) (не реже, чем 1 раз в 7 дней)
T-71	(HCПК, PCI DSS) Отсутствие контроля изменений активных элементов на платежных страницах (script, iframe, form и других) (не реже, чем 1 раз в 7 дней)
T-72	(HCПК, PCI DSS) Отсутствие оповещения персонала о несанкционированных изменениях
T-73	(рекомендации НКЦКИ) Отсутствие проверки перед использованием js-кода на предмет вредоносного воздействия на отображаемую в браузерах информацию и возможность кражи аутентификационных данных и файлов-cookie пользователей
T-74	(рекомендации НКЦКИ) Отсутствие периодической проверки хэш-сумм js-кода
T-75	(рекомендации НКЦКИ) Отсутствие повторной проверки функциональности (безопасности) js-кода при изменении хэш-сумм

Снижение защищённости

T-50	Несанкционированное изменение HTTP-заголовков: Content-Security-Policy (CSP)
T-51	Несанкционированное изменение HTTP-заголовков: Strict-Transport-Security, X-Frame-Options и других
T-52	Разработчик использует в коде функции динамической интерпретации (eval(), конструктор function() и другие)
T-53	Неработоспособность frontend-приложения в связи с блокировкой в РФ IP-адресов серверов с подключенными к приложению внешними скриптами и другими ресурсами (CDN, системы аналитики, тег-менеджеры, внешние js-сервисы, файлы CSS, изображения и т.п.)
T-54	Выполнение вредоносного js-кода в inline-скриптах до обнаружения и реагирования
T-55	Выполнение вредоносного js-кода в file скриптах до обнаружения и реагирования
T-56	Неработоспособность приложения вследствие неверной настройки CSP
T-57	Неработоспособность приложения вследствие неверной настройки SRI
T-58	Избыточное раскрытие чувствительных данных на странице (OWASP Excessive Data Exposure / Sensitive Data Exposure)
T-59	Избыточное раскрытие данных в API (OWASP Excessive Data Exposure / Sensitive Data Exposure)
T-60	Аномалии в появлениях чувствительных данных на страницах (например, множество записей различных данных у одного пользователя (признаки IDOR, SQL Injection) или множество записей различных данных на одной странице)
T-61	Раскрытие чувствительных данных в комментариях на веб-странице
T-62	Запись конфиденциальных данных в постоянные хранилища браузера (cookie, local storage, indexed DB и др.)
T-63	Отправка конфиденциальных данных на сторонний хост