Что такое XSS, CSRF, IDOR и RCE простыми словами

Эти четыре типа брешей относятся к критическим уязвимостям веб-приложений. Они эксплуатируются чаще других, входят в OWASP Top 10, поэтому разработчикам, администраторам и владельцам бизнеса важно понимать их механику и последствия.

XSS — это уязвимость, при которой веб-приложение вставляет непроверенные данные пользователя в страницу, а браузер воспринимает их как код. Чаще всего речь идёт о JavaScript, который выполняется в контексте доверенного сайта. Атакующий может читать cookies, перехватывать ввод форм, изменять отображение страницы или перенаправлять пользователя на вредоносный ресурс.

Примеры XSS-уязвимостей и **разница между отражённым и сохранённым XSS**. Отражённый XSS возникает, когда вредоносный код передаётся в запросе и немедленно возвращается сервером в ответ. Такой баг часто встречается в формах поиска или фильтрации.

Сохранённый XSS опаснее: внедрённый скрипт остается в базе данных или другом хранилище, а затем автоматически выполняется у всех, кто открывает заражённую страницу. Пример — вредоносный комментарий в блоге, который действует до тех пор, пока не будет удалён.

Рассмотрим, что такое CSRF и **пример CSRF-атаки**. CSRF эксплуатирует доверие сайта к авторизованному пользователю. Атакующий формирует поддельный запрос — ссылку или HTML-форму, размещает её на стороннем ресурсе или отправляет по электронной почте. Если жертва переходит по ссылке, браузер

отправляет запрос с активной сессией пользователя, сервер выполняет действие, например, перевод средств или смену пароля.

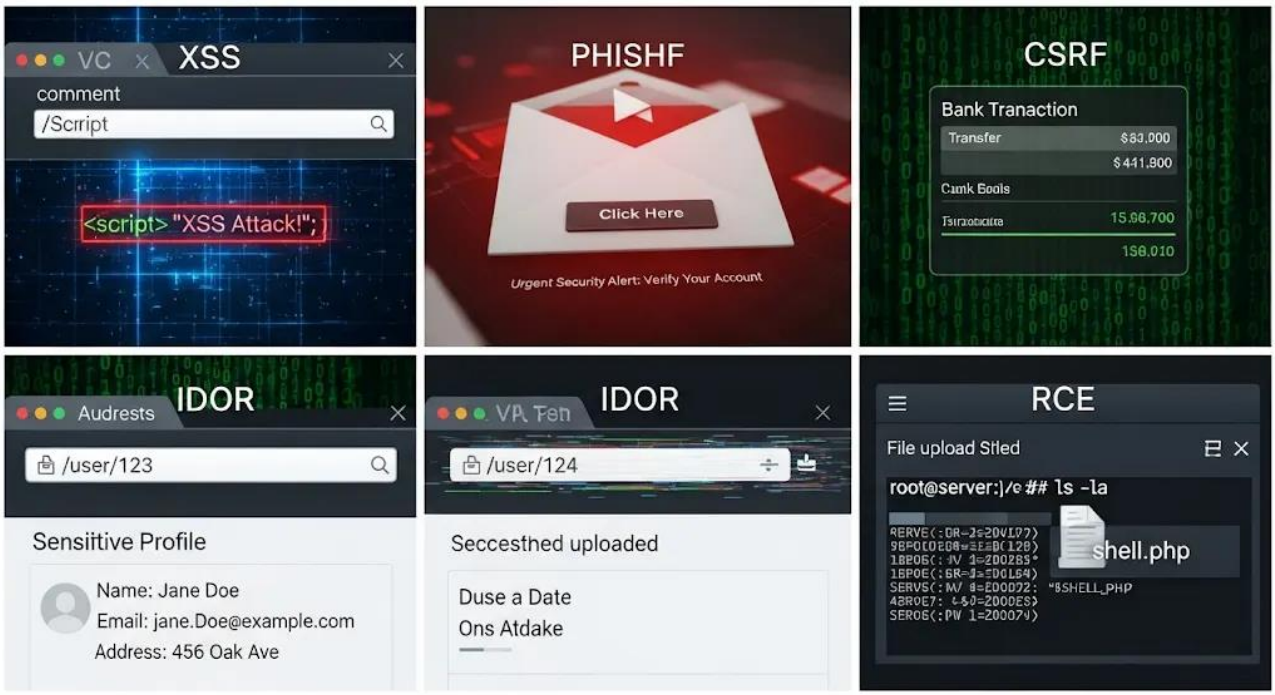
CSRF-защита простыми словами и **чем CSRF отличается от XSS**. Основная защита — уникальные токены, которые сервер добавляет в формы и проверяет при получении запроса. Дополнительно используют флаг SameSite у cookies. Ключевое отличие от XSS: при CSRF код не внедряется и не выполняется в браузере жертвы, а используется механизм автоматической отправки авторизованных запросов.

IDOR — небезопасный прямой доступ к объектам

Что такое IDOR в безопасности и **небезопасный прямой доступ к объектам**. IDOR появляется, когда приложение позволяет обращаться к ресурсам по их идентификатору без проверки прав доступа. Подмена числа или имени в URL, например /user/123 на /user/124, может дать злоумышленнику доступ к чужим данным.

IDOR-уязвимость API: пример и **IDOR exploit tutorial**.
В API интернет-магазина запрос /order/1001 возвращает детали заказа. Если заменить идентификатор на /order/1002 и сервер вернёт данные, значит, проверка прав отсутствует. Эксплуатация часто автоматизируется: через Burp Suite Intruder или скрипты, перебирающие последовательные значения.

RCE даёт атакующему возможность выполнять произвольные команды на сервере. Такая брешь возникает, когда пользовательский ввод попадает в интерпретатор команд, скриптовый движок или функции вроде eval() без фильтрации. Например, загрузка и выполнение PHP-файла через уязвимую форму.



OWASP ZAP: примеры тестирования.
OWASP ZAP — это бесплатный инструмент для тестирования безопасности веб-приложений с открытым исходным кодом. Он работает как прокси-сервер между браузером и приложением, перехватывает трафик, помогает искать уязвимости: XSS, SQLi, CSRF, IDOR и другие.

Чаще его используют для:

- автоматического сканирования сайта на наличие типовых уязвимостей
- ручного тестирования, когда специалист сам модифицирует запросы и проверяет реакцию сервера
- интеграции в CI/CD, чтобы проверка шла при каждом обновлении кода

OWASP ZAP подходит для комплексного поиска XSS, CSRF, IDOR и некоторых RCE. В нём можно запустить автоматический скан или настроить ручную проверку с подменой запросов. Инструмент фиксирует подозрительные ответы, отмечает места, где данные обрабатываются без проверки, с его помощью можно быстро составить список точек для детального анализа.