Что такое брутфорс атака и принцип ее работы

Брутфорс (в переводе – грубая сила) – это вид атаки на приложения, основанный на переборе всех возможных вариантов логина и(или) пароля.

Данный тип атаки популярен, потому что зачастую неопытные пользователи не придают значения сложности пароля или используют один и тот же пароль в нескольких аккаунтах. Это приводит к тому, что хакер, вооружившись списком паролей из специальных словарей, может взломать учетную запись человека и незаконно проникнуть на его аккаунт. Это становится возможным благодаря автоматизированным инструментам, которые проверяют миллионы комбинаций и выводят подходящие.

Существует два основных типа таких атак:

- Онлайн-брутфорс: Атака напрямую на интерфейс входа (веб-форму). Защита от него ложится на плечи разработчиков приложения.
- Офлайн-брутфорс: Атака на украденную базу данных хешей паролей. Для этого могут использоваться радужные таблицы — заранее рассчитанные таблицы хешей для ускорения взлома. Защита от него — это правильное хеширование паролей на стороне сервера.

  При офлайн-брутфорсе злоумышленник не взаимодействует с сервером приложения. Он локально на своей мощной машине (или ботнете) перебирает пароли, хеширует их по тому же алгоритму и сравнивает с украденными хешами из базы данных. Радужные таблицы ускоряют этот процесс, предоставляя цепочки предварительно рассчитанных хешей

Реальные риски от такой атаки

Злоумышленник, которому удалось проникнуть на аккаунт жертвы может делать, что ему вздумается, ведь у него есть доступ ко всей информации о человеке, которая есть на его аккаунте. Он также может заниматься рассылкой от имени жертвы и просить деньги. Обычно это не вызывает подозрения у знакомых взломанного человека: все выглядит обыденно: друг просто просит некоторую сумму в долг и ручается ее вернуть, но на самом деле за маской друга скрывается хакер, который получит деньги и бесследно исчезнет

Как предотвратить риск брутфорс атаки

В первую очередь пользователю при регистрации критически важно придумать сложный пароль, состоящий более чем из десяти символов, содержащий как строчные, так и заглавные буквы, а также цифры и специальные символы.

Также рекомендуется использовать разные пароли на разных сайтах, стараться не регистрировать свои реальные и важные данные на «одноразовых» сайтах. На них вы

больше не вернетесь, но если будет слив бд, то и эти данные будут в открытом доступе. Также критически важно включить 2FA, она защитит не только от брутфорс атаки.

В процессе разработки необходимо максимально ограничить информационные утечки, например, сделать одинаковые HTTP статусы как для верного ввода пароля, так и для ошибки, задать фиксированную длину ответов, одинаковый текст при успешной или неуспешной авторизации, одинаковое время на обработку данных. Также показывать капчу после n неверных попыток входа, требовать от пользователя пароль, отвечающий критериям безопасного и блокировать IP, с которого поступает слишком много попыток входа за короткий промежуток времени, добавить «соль» к паролям при создании их хэша (защита от радужных таблиц), добавление двухфакторной аутентификации, например, с помощью *bcrypt*

Хоть брутфорс становится все менее опасной атакой в связи с развивающимися методами информационной безопасности, сбрасывать ее со счетов чревато кражей аккаунтов и сливами информации. Взлом может занять как от пары минут, так и до многих лет. Все зависит от степени защищенности приложения. Однако, несмотря на все меры защиты самым слабым звеном остается человек. Даже если атака брутфорс не удалась, всегда есть социальная инженерия, XSS, SQL-injection, кейлогеры и другие вирусы.