Лекция 3.2. Защита от перебора паролей

В данной лекции будут рассмотрены следующие вопросы:  
1. Какие пароли можно считать надёжными?  
2. Какие механизмы могут защитить пароли от перебора?  
3. Чем поможет тестирование продукта на проникновении?

Глава 1. Защита от перебора паролей

Защита от перебора паролей  
Кражи паролей, похищения личных данных пользователей регулярно попадают в заголовки новостей. Почтовые сервисы, аккаунты в социальных сетях, даже сами смартфоны — хакеры ставят под угрозу любые пользовательские данные.

Какие пароли можно считать надёжными?

Какие механизмы могут защитить пароли от перебора?

Чем поможет тестирование продукта на проникновение?

КАК ЗЛОУМЫШЛЕННИКИ УЗНАЮТ ПАРОЛИ?  
Прежде чем говорить о самих паролях разберёмся, как они могут быть украдены. Украсть пароль можно у самого пользователя, у сервиса или на пути от клиента к сервису.  
Нас интересует только первый вариант, поскольку только он относится непосредственно к парольной безопасности. Два других варианта связаны с уязвимостями веб-приложений и шифрованием данных, при этом вероятность похищения пароля никак не зависит от его сложности.  
Итак, каким образом злоумышленник может украсть пароль у пользователя?  
1. Прямым перебором аутентификационных данных жертвы (guessing, cracking, brute force attack и т. д.). Это самый простой способ.  
2. Методами социальной инженерии, которые позволяют узнать аутентификационные данные пользователя (например, позвонить и представиться администратором, рассылка писем от лица того же администратора и т. д.). Этот способ более изощренный и требует определённых усилий от атакующего (сбор информации о жертве и его окружении). Для этого злоумышленник должен владеть специальными навыками и инструментами и обладать определёнными познаниями в психологии.  
3. Подсмотреть пароль при прямом общении с жертвой или на его / её рабочем месте (установить кейлогер в компьютер жертвы, найти стикер с паролем).  
МЕХАНИЗМЫ ЗАЩИТЫ ПАРОЛЕЙ  
Если успешность проведения двух последних пунктов зависит не от разработчика продукта, а от самого пользователя, то воспрепятствовать автоматическому перебору паролей можно на стадии разработки, внедрив следующие механизмы:  
1. CAPTCHA (капча). При аутентификации пользователю необходимо дополнительно ввести символы с картинки.  
2. Двухфакторная аутентификация с использованием различных средств. Например, отправка SMS с кодом на мобильное устройство пользователя для авторизации в приложении или использование генераторов одноразовых паролей.  
3. Временная блокировка пользователя после определённого количества неудачных попыток аутентификации. Например, аккаунт пользователя блокируется на 30 минут после пяти неудачных попыток.  
4. Определение требований к паролю.  
На этом моменте остановимся поподробнее.

Глава 2. Защита от перебора паролей

НАДЕЖНЫЕ ПАРОЛИ: КАКИЕ ОНИ?  
1. Оптимальное количество символов в пароле: 8—12.  
2. В состав пароля входят цифры, латинские буквы и специальные символы («$», «?», «!», «<», «>». «”», «#», «%», «@» и другие).  
3. Сочетание цифровых и буквенных символов (заглавных и строчных) — самое надёжное.  
НЕ рекомендуется использовать в качестве пароля:  
1. Устойчивые словосочетания.  
2. Наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре: qwerty, 123456789, qazxsw и т. д.  
3. Персональные данные: имена и фамилии, даты рождения (свою и родственников), клички домашних животных, адреса, номера паспортов, страховых свидетельств и т. п., пароли, созданные для доступа к другим сервисам.  
Важным моментом при составлении пароля является соблюдение баланса между его сложностью и запоминаемостью для пользователя. Дело в том, что при составлении очень длинных и трудно запоминаемых паролей, у пользователя может возникнуть соблазн записать его на бумажном носителе (например, на стикере, который наклеен на монитор или лежит под клавиатурой), что повышает вероятность кражи пароля у пользователя злоумышленником.  
Также вы можете предусмотреть принудительную смену пароля с определённой периодичностью (например, раз в 90 дней). Если для подбора пароля требуется время, превышающее данный период, то риск подбора пароля заметно сокращается.  
Наконец, пользователь должен знать, какую последовательность действий предпринять, если пароль был похищен или есть подозрения на это.

В криптографии соль-это случайные данные, которые используются в качестве дополнительного ввода в одностороннюю функцию, хэширующую данные, пароль или парольную фразу. Соли используются для защиты паролей в хранилище.

1. Что нужно учитывать для создания надёжных паролей?
   1. Длину, сложность, избегание личной информации
   2. Длину, уникальность, избегание личной информации
   3. Сложность, уникальность, наличие определенных символов
2. Выберите все существующие стратегии создания надёжных паролей:
   1. Регулярная смена паролей
   2. Резервирование паролей
   3. Парольные фразы
   4. Парольные менеджеры
3. Какие механизмы защиты паролей сегодня существуют?
   1. Двухфакторная аутентификация, парольные фразы, блокировка аккаунта
   2. Двухфакторная аутентификация, CAPTCHA, блокировка аккаунта
   3. Двухфакторная аутентификация, парольные менеджеры, CAPTCHA
4. Какой механизм защиты паролей позволяет отличить человека от автоматизированных инструментов для перебора паролей?
   1. CAPTCHA
   2. Двухфакторная аутентификация
   3. Блокировка аккаунта
5. Какой механизм защиты паролей предполагает проверку личности пользователя, который включает два шага, чтобы убедиться в его подлинности?
   1. CAPTCHA
   2. Двухфакторная аутентификация
   3. Блокировка аккаунта
6. Выберите все методы и инструменты, которые используются в рамках двухфакторной аутентификации:
   1. Аппаратные токены
   2. SMS-коды
   3. Смена пароля
   4. Биометрические данные
   5. Приложения аутентификации
7. В рамках какого метода двухфакторной аутентификации пользователь использует физическое устройство, такое как USB-ключ или смарт-карту, которые генерируют временные коды для аутентификации:
   1. Приложения аутентификации
   2. Аппаратный токен
   3. SMS-коды
8. Как называется случайная дополнительная информация, которая добавляется к паролю перед его хэшированием?
   1. Хэширование
   2. SMS-код
   3. Соль