1. Аутентификация (Authentication)

Раздел, посвященный аутентификации описывает атаки, направленные на используемые Web-приложением методы проверки идентификатора пользователя, службы или приложения.

Аутентификация использует как минимум один из трех механизмов (факторов): "что-то, что мы имеем", "что-то, что мы знаем" или "что-то, что мы есть". В этом разделе описываются атаки, направленные на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации Web-серверов.

1.1. Подбор (Brute Force)

Подбор - автоматизированный процесс проб и ошибок, использующийся для того, чтобы угадать имя пользователя, пароль, номер кредитной карточки, ключ шифрования и т.д.

Многие системы позволяют использовать слабые пароли или ключи шифрования, и пользователи часто выбирают легко угадываемые или содержащиеся в словарях парольные фразы.

Используя эту ситуацию, злоумышленник может воспользоваться словарем и попытаться использовать тысячи или даже миллионы содержащихся в нем комбинаций символов в качестве пароля. Если испытуемый пароль позволяет получить доступ к системе, атака считается успешной и атакующий может использовать учетную запись.

Подобная техника проб и ошибок может быть использована для подбора ключей шифрования. В случае использования севером ключей недостаточной длины, злоумышленник может получить используемый ключ, протестировав все возможные комбинации.

Существует два вида подбора: прямой и обратный. При прямом подборе используются различные варианты пароля для одного имени пользователя. При обратном - перебираются различные имена пользователей, а пароль остается неизменным. В системах с миллионами учетных записей вероятность использования различными пользователями одного пароля довольно высока. Не смотря на популярность и высокую эффективность, подбор может занимать несколько часов, дней или лет.

Пример:

Имя пользователя = Jon
Пароли = smith, michael-jordan, [pet names], [birthdays], [car names], ...

Имена пользователей = Jon, Dan, Ed, Sara, Barbara,
Пароль = 12345678

Ссылки:

"Brute Force Attack", Imperva Glossary
http://www.imperva.com/application_defense_center/glossary/brute_force.html

"iDefense: Brute-Force Exploitation of Web Application Session ID's", By David Endler - iDEFENSE Labs
http://www.cgisecurity.com/lib/SessionIDs.pdf

1.2. Недостаточная аутентификация (Insufficient Authentication)

Эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации. Интерфейсы администрирования через Web - яркий пример критичных систем.

В зависимости от специфики приложения, подобные компоненты не должны быть доступны без должной аутентификации. Чтобы не использовать аутентификацию некоторые ресурсы "прячутся" по определенному адресу, который не указан на основных страницах сервера или других общедоступных ресурсах. Однако, подобный подход не более чем "безопасность через сокрытие". Важно понимать, что, не смотря на то, что злоумышленник не знает адреса страницы, она все равно доступна через Web.

Необходимый URL может быть найден перебором типичных файлов и директорий (таких как /admin/), с использованием сообщений об ошибках, журналов перекрестных ссылок или путем простого чтения документации. Подобные ресурсы должны быть защищены адекватно важности их содержимого и функциональных возможностей.

Пример:

Многие Web-приложения по умолчанию используют для административного доступа ссылку в корневой директории сервера (/admin/). Обычно ссылка на эту страницу не фигурирует в содержимом сервера, однако страница доступна с помощью стандартного браузера. Поскольку пользователь или разработчик предполагает, что никто не воспользуется этой страницей, так как ссылки на неё отсутствует, зачастую реализацией аутентификации пренебрегают. И для получения контроля над сервером злоумышленнику достаточно зайти на эту страницу.

1.3. Небезопасное восстановление паролей (Weak Password Recovery Validation)

Эта уязвимость возникает, когда Web-сервер позволяет атакующему несанкционированно получать, модифицировать или восстанавливать пароли других пользователей.

Часто аутентификация на Web-сервере требует от пользователя запоминания пароля или парольной фразы. Только пользователь должен знать пароль, причем помнить его отчетливо. Со временем пароль забывается. Ситуация усложняется, поскольку в среднем пользователь посещает около 20 сайтов, требующих ввода пароля.

(RSA Survey: http://news.bbc.co.uk/1/hi/technology/3639679.stm). Таким образом, функция восстановления пароля является важной составляющей предоставляемой Web-серверами сервиса.

Примером реализации подобной функции является использование "секретного вопроса", ответ на который указывается в процессе регистрации. Вопрос либо выбирается из списка или вводится самим пользователем. Еще один механизм позволяет пользователю указать "подсказку", которая поможет ему вспомнить пароль. Другие способы требуют от пользователя указать часть персональных данных, таких как номер соц. страхования, ИНН, домашний адрес почтовый индекс и т.д., которые затем будут использоваться для установления личности. После того как пользователь докажет свою идентичность, система отобразит новый пароль или перешлет его по почте.

Уязвимости связанные с недостаточной проверкой при восстановлении пароля возникают, когда атакующий получает возможность используемый механизм. Это случается, когда информацию, используемую для проверки пользователя, легко угадать или сам процесс подтверждения можно обойти. Система восстановления пароля может быть скомпрометирована путем использования подбора, уязвимостей системы или из-за легко угадываемого ответа на секретный вопрос.

Примеры:

Слабые методы восстановления паролей

Проверка информации

Многие серверы требуют от пользователя указать его e-mail в комбинации с домашним адресом и номером телефона. Эта информация может быть легко получена из сетевых справочников. В результате, данные, используемые для проверки, не являются большим секретом. Кроме того,

эта информация может быть получена злоумышленником с использованием других методов, таких как “межсайтовое выполнение сценариев ” (Cross-Site Scripting) или “фишинг” (Phishing).

Парольные подсказки

Сервер, использующий подсказки для облегчения запоминания паролей, может быть атакован, поскольку подсказки помогают в реализации подбора паролей. Пользователь может использовать стойкий пароль, например, "221277King" с соответствующей подсказкой: "д-р+люб писатель". Атакующий может заключить, что пользовательский пароль состоит из даты рождения и имени любимого автора пользователя. Это помогает сформировать относительно короткий словарь для атаки путем перебора.

Секретный вопрос и ответ

Предположим, ответ пользователя "Бобруйск", а секретный вопрос "Место рождения". Злоумышленник может ограничить словарь для подбора секретного ответа названиями городов. Более того, если атакующий располагает некоторой информацией о пользователе, узнать его место рождения не сложно.

Ссылки:

"Protecting Secret Keys with Personal Entropy", By Carl Ellison, C. Hall, R. Milbert, and B. Schneier
http://www.schneier.com/paper-personal-entropy.html

"Emergency Key Recovery without Third Parties", Carl Ellison
http://theworld.com/~cme/html/rump96.html