CERT-UA

SQL-injection

Автори:
Міснік Олексій
Антонішин Михайло
Computer Emergenscy Response Team of Ukraine – CERT-UA
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

SQL-injection (SQL-инъекция) представляет из себя уязвимость которая позволяет подделать определённый запрос скрипта к базе данных. Очень часто, при использовании подобной уязвимости, взломщик может читать любые данные из доступных ему таблиц. В редких случаях дело может дойти и до модификации данных в доступных взломщику таблицах. Ещё реже взломщик может производить операции с файловой системой – чтение/запись файлов, листинг директорий и т.д. Но всё же иногда бывают ситуации в которых взломщик вообще ничего не может сделать, хоть и имея на руках SQL-инъекцию. Скрипты могут страдают данной уязвимостью из-за того, что многие программисты не заботятся о фильтрации входных параметров которые напрямую попадают в запрос. А большинство из тех кто заботится ограничиваются введением простенькой фильтрацией опасных символов которую давно уже научились с обходить. Где же можно встретить подобного рода уязвимости? Да почти везде если хорошо покопаться. Сейчас 90% сайтов работают с базами данных. С базой данных может работать форум, лента новостей, гостевая книга, он-лайн магазин, голосования и ещё много различных веб-приложений. Но чаще всего SQL-инъекции можно обнаружить в самых неожиданных местах. Например на каком-либо сайте при загрузке файла может не подвергаться фильтрации его имя и иньекция будет возможна при специально-сформированном имени файла (подобная уязвимость была обнаружена нашей командой в SmartCMS). Или же программисты могут не учитывать фильтрацию различных HTTP-заголовков. Вообще с HTTP-заголовками ситуация сейчас очень интересная – если раньше многие программисты не фильтровали данные передающиеся в cookies, то теперь они не фильтруют различные HTTP-заголовки. Но об этом позже, в 6 главе. Теперь обсудим ПО которое нам понадобится для наших экспериментов. Веб-сервер у нас уже установлен. Далее, так как мы будем работать с базами данных, нам нужны различные СУБД:

1. MySQL
2. PostgreSQL
3. SQLite
4. MSSQL.

При работе со всеми этими СУБД есть очень много одинаковых моментов. Различия встречаются лишь в названиях некоторых функций.