METHOD OF PROTECTION OF DATABASES ON THE BASIS OF IMPLEMENTATION SQL AND HARMFUL SCRIPT PROTOCOL

Nikitin D.I.[1], Suvorov K.I.[2] (Russian Federation) Email: Nikitin428@scientifictext.ru

[1]Nikitin Dmitry Igorevich – Student,
DEPARTMENT OF RARE METALS AND NANOMETER MATERIALS,
PHYSICS AND TECHNOLOGY INSTITUTE,
URAL FEDERAL UNIVERSITY NAMED AFTER THE FIRST PRESIDENT OF RUSSIA B.N. YELTSIN,
EKATERINBURG;
[2]Suvorov Konstantin Igorevich – Engineer,
INFORMATION SECURITY DEPARTMENT
PERM FILIAL AGENCY «MAJROMDO»,
PERM

Abstract: *the problem of protection of the integrated information space is delivered before the leading programmers quite recently. In this operation protection on the basis of a structured query language is considered. Information security is considered as the analysis of vulnerabilities of protocols of different level. Usually for data acquisition use attempts of implementation of SQL of requests. Implementation is made due to execution of scripting scenarios, and a fake of internetwork requests. The method of protection against implementation of harmful SQL is offered.*
Keywords: *information security, sql, gateway skripting, duplication of inquiries, SQL of vulnerability, introduction of inquiry, SQL analysis, PSM analysis.*

МЕТОД ЗАЩИТЫ БАЗ ДАННЫХ НА ОСНОВЕ SQL ВНЕДРЕНИЯ И СРИПТИНГА

Никитин Д.И.[1], Суворов К.И.[2] (Российская Федерация)

[1]Никитин Дмитрий Игоревич – студент,
кафедра редких металлов и наноматериалов,
Физико-технологический институт
Уральский федеральный университет им. первого Президента России Б.Н. Ельцина,
г. Екатеринбург;
[2]Суворов Константин Игоревич – инженер,
департамент информационной безопасности,
Пермский филиал компании «Majromdo»,
г. Пермь

Аннотация: *проблема защиты интегрированного информационного пространства поставлена перед ведущими программистами совсем недавно. В данной работе рассматривается защита на базе языка структурированных запросов. Защиту информации рассматривают как анализ уязвимостей протоколов различного уровня. Обычно для получения данных используют попытки внедрения SQL запросов. Внедрение производится за счет выполнения скриптовых сценариев и подделки межсетевых запросов. Предложен метод защиты от внедрения вредоносных SQL.*
Ключевые слова: *информационная безопасность, SQL, межсетевой скриптинг, дублирование запросов, SQL уязвимости, внедрение запроса, SQL анализ, PSM анализ.*

Интенсивное развитие различных веб-сервисов показывает отсутствие единых стандартов безопасного программирования. Это дает почву для развития киберпреступности. Что в свою очередь не влечет никакой ответственности, потому что сеть гарантирует полнейшую анонимность взломов. Структура построения функционала веб-приложения представляет собой компоненты управления базами данных (СУБД), хранилища XML. Многосторонний анализ серверной стороны уязвимостей протоколов различных уровней, в том числе и прикладного, показал, что основные уязвимости базируются на SQL инъекциях. Атака данного типа может дать атакующему хакеру или роботу выполнить произвольный SQL запрос к базе данных (например, чтение, редактирование или создание новых данных) это могут быть персональные данные, номера банковских карточек, пароли от входа в систему и многие другие. Атаку можно устроить, основываясь на некорректной обработке SQL запроса или некорректной обработке входящих данных SLM. Попытка попадания в поток выполнения определенных команд, которые выполняют на стороне сервера. Цель данной атаки есть выполнение произвольных команд на операционной системе с помощью уязвимого приложения, в том числе и когда приложение передает небезопасные пользовательские данные (например, cookies, TRI). Другой очень большой уязвимостью на стороне сервера является fileinclusion. Это возможность подключить и исполнять файлы не только в

пределах уязвимого сервера, но и по относительному пути. Данный ход позволяет хакеру удаленно получить доступ с помощью специально-сформированного запроса к произвольным файлам на сервере. Еще существуют RFI уязвимости, которые позволяют удаленно подключить файлы с других серверов с помощью URL адресов. Учитывая это, уязвимости серверной стороны позволяют выполнять произвольные SQL запросы, выполнение произвольных команд, и проникновение команд в поток. Не маловажными являются уязвимости клиентской стороны. Здесь часто используют скриптовые языки, которые позволяют выполнить на стороне клиента сценарий. Самый распространенный вид атаки на стороне клиента является межсетевой скриптинг. Целью данных операций является вставка в веб страницу скриптов, которые выполняют нужные сценарии в браузере. В результате при загрузке страницы при определённом событии будет выполняться скрипт (например, при попытке открыть гиперссылку открывается запрос на страницу, которая не позволяет прекратить передачу данных). Или хакер прячет скрипт в URL ссылку реально действующего, доверенного сайта, который перенаправляет пользователя на поддельный сайт. На этом сайте спрятан скрипт, который перехватывает cookie пользователя который перешел на данную подделку. Затем cookie передается хакеру, который использует его для перехвата сессии пользователя [1, с. 6]. В данном случае реальный и доверенный сайт не подвергался хакерской атаке, но злоумышленник использует уязвимое место скрипта, чтобы получить контроль над его сессией. В данную стезю можно отнести кликбайт, в данном случае хакер использует популярные запросы на поддельных оптимизированных сайтах. Эти запросы перенаправляют пользователя на вредоносный сайт, на котором исполняется опасный сценарий. В итоге злоумышленник перехватывают сессию пользователя. Еще один вид атаки на стороне клиента это межсетевая подделка запроса, этот вид атаки направлена на посетителей веб сайтов. К примеру, пользователь заходит на вредоносный сайт, и от его имени по сценарию отправляется запрос на другой сайт. Происходит вполне реальная операция, в которой пользователь не увидит проблем. Но в итоге хакер получает нужные ему данные, которые были пересланы реальному сайту (например, номер карты). Данная атака возможна, если жертва аутентифицирована без обратного ответа/запроса. Самыми распространенными рекомендациями по защите клиента являются: использование актуальны версий информационных потоковых программ, последние версии браузеров, дополнительное ПО, проверяющее поле загрузки, URL запросы и JavaScript. Все данные хранятся в специальных базах, обращение к которым происходит с помощью SQL запросов. Если данные не проходят проверку от клиента, хакер не сможет внедрить код, который будет содержать часть запроса или сценария. Все-таки основной защитой должна обладать серверная сторона, а именно: SQL инъекции, направленные на дестабилизирующую работу СУДБ, задачей которой является получение несанкционированного доступа к данным сервера.

Список литературы / References

1. *Кайли Д.* SQL Server 2012: совершенствуем защиту данных // WINDOWS it pro/re - Открытые системы, 2012. № 6. С. 1-36.

Список литературы на английском языке / References in English

1. *Kylie D.* SQL Server 2012: improve data protection // WINDOWS it pro/re - Open Systems, 2012. № 6. С. 1-36.