1. Атаки на основе внедрения кода

Введение в атаки на основе внедрения кода

Уязвимости, связанные с внедрением кода, на протяжении долгого времени остаются одной из наиболее актуальных и распространенных проблем безопасности. Они включались в OWASP Топ-10 каждый раз с момента его первого выхода в 2003 году. Хотя некоторые уязвимости внедрения достаточно хорошо известны, например SQL-инъекции, внедрения команд или межсайтовый скриптинг (XSS), существует значительно больше уязвимостей, связанных с внедрением, большинство из которых менее известны. Более известные типы уязвимостей внедрения, разумеется, встречаются чаще, однако, с другой стороны, большинство разработчиков осведомлены о них, и распространенные фреймворки для разработки веб-приложений по умолчанию эффективно предотвращают их. Поскольку осведомленность о менее распространенных уязвимостях внедрения ниже, механизмы защиты часто реализуются неправильно или не реализуются вовсе, что приводит к появлению простых векторов атак, которые могут быть использованы без необходимости обхода средств защиты или применения продвинутых техник эксплуатации.

Атаки с внедрением

XPath-инъекции

XML Path Language (XPath) - это язык запросов для данных в формате Extensible Markup Language (XML), подобно тому, как SQL является языком запросов для баз данных. XPath используется для выполнения запросов к данным из XML-документов. Веб-приложения, которым необходимо извлекать данные, хранящиеся в формате XML, соответственно полагаются на XPath для получения требуемых данных. Уязвимости внедрения в XPath возникают, когда пользовательский ввод вставляется в XPath-запросы без надлежащей очистки. Как и в случае с уязвимостями SQL-инъекций, XPath-инъекции ставят под угрозу все данные, поскольку успешная эксплуатация внедрения в XPath позволяет атакующему извлечь весь XML-документ.

LDAP-инъекции

Lightweight Directory Access Protocol (LDAP) - это протокол, используемый для доступа к серверам каталогов, таким как **Active Directory (AD)**. Веб-приложения часто используют LDAP-запросы для обеспечения интеграции с сервисами AD. Например, LDAP может позволять пользователям AD

аутентифицироваться в веб-приложении. Уязвимости внедрения в LDAP возникают, когда пользовательский ввод вставляется в фильтры поиска без надлежащей очистки. Если аутентификация LDAP реализована некорректно, это может привести к обходу аутентификации. Кроме того, внедрение в LDAP может привести к потере данных.

HTML-инъекции в генераторах PDF

Файлы в формате Portable Document Format (PDF) широко используются для распространения документов. В связи с этим во многих веб-приложениях реализована функциональность преобразования данных в формат PDF с помощью библиотек для генерации PDF. Эти библиотеки принимают HTML-код в качестве входных данных и генерируют из него PDF-файл. Это позволяет веб-приложению применять кастомные стили и форматирование к создаваемому PDF-файлу. Это делается за счет применения таблиц стилей к входному HTML-коду. Зачастую пользовательский ввод напрямую включается в генерируемые PDF-файлы. Если пользовательский ввод не очищается надлежащим образом, то может существовать возможность внедрения HTML-кода во входные данные для библиотек генерации PDF, что может привести ко множеству уязвимостей, включая **подделку запроса на стороне сервера (SSRF)** и **включение локальных файлов (LFI)**.