ФСТЭК РОССИИ

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

Красный проспект, д. 41, г. Новосибирск, 630091
тел./ факс: (383) 203-54-07
E-mail: sfo@fstec.ru
ОКПО 56009786, ОГРН 1025401918761
ИНН/КПП 5405213849/540601001

20 сентября 2023 № 1902

Руководителям штабов
по обеспечению кибербезопасности
субъектов Российской Федерации

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются уязвимости веб-приложений.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения уязвимостей веб-приложений официальных сайтов, связанных с реализацией атак на основе SQL-инъекций.

В целях предотвращения возможности реализации атак на основе SQL-инъекций на официальные сайты органов государственной власти рекомендуется принять следующие дополнительные меры:

1. В случаях, когда возможные значения пользовательского ввода известны заранее, рекомендуется использовать механизмы «белого списка» для проверки входных данных.

Например, в случае реализации на сайте возможности отображения данных по 10, 50 или 100 записей на странице и передаче соответствующего ограничения в переменной «size» на стороне сервера должна быть реализована проверка значения переменной по «белому списку» из трех указанных возможных значений.

Если переданное значение будет отличаться от предусмотренных возможных значений, то переменной «size» присваивается заранее установленное стандартное значение.

2. Отказаться (по возможности) от использования метода GET в формах сайта. Если информация представляет важность, необходимо использовать метод POST.

3
020

3. Осуществлять экранирование специальных символов (замена управляющих символов на безопасные подстановки) в отношении всех данных пользовательского ввода, использующихся в динамических SQL-запросах.

При этом должны быть учтены данные, передаваемые всеми методами HTTP-запросов (POST, GET, PUT, DELETE), в том числе, данные передаваемые через скрытые поля форм ввода, поля ввода имени пользователя и пароля, а также данные из заголовков (например, Cookie, Referer). Например, при использовании языка PHP для экранирования специальных символов могут быть использованы такие функции, как addslashes, filter_input, mysql_real_escape_string.

4. Реализовать функцию отслеживания источника поступающих данных путем:

проверки его в $_SERVER['HTTP_REFERER'];

созданием скрытого поля в форме для отслеживания источника;

указывания имени формы при отправке на веб-сервер;

указывания имени кнопки отправки, поля и других структурных элементов формы при отправке на веб-сервер.

5. Использовать параметризованные SQL-запросы.

Например, в веб-приложениях, реализованных на языке PHP, для реализации данной меры защиты информации может быть использован модуль PHP Data Objects (PDO).

6. Запретить прямой доступ к служебным файлам веб-сервера со стороны пользователя путем создания отдельной директории (например, includes) и размещения в ней подключаемых файлов (отдельные блоки сайта, библиотеки пользовательских функций, файл подключения к базе данных, обработчики форм) и запрета к ней прямого доступа через добавление в файл .htaccess строки deny from all.

7. Отключить вывод ошибок веб-приложения пользователю. Например, в веб-приложениях, реализованных на языке PHP, путём добавления в файл .htaccess следующей строки: php_flag display_errors offphp_value error_reporting 0.

8. Минимизировать права доступа пользователей сайтов к базам данных.

В частности, у пользователей сайта (базы данных) одного веб-приложения не должно быть доступа к базам данных других веб-приложений, функционирующих под управлением одной системы управления базами данных. Пользователи сайта должны получать доступ к базе данных с использованием учетных записей системы управления базами данных с минимальными необходимыми привилегиями.

9. Отключить неиспользуемые учетные записи пользователей сайта (в том числе, учетные записи служб, задействованных в функционировании веб-приложений, например, FTP-сервер, SSH-сервер) и предоставить им минимальные необходимые привилегии.

10. Использовать хранимые процедуры (или аналогичные конструкции программного кода), не позволяющие пользователям напрямую обращаться к серверу базы данных через поля ввода данных.

11. Использовать межсетевые экраны уровня веб-приложений.

12. Использовать механизмы двухфакторной аутентификации для привилегированных пользователей.

13. По возможности осуществлять проверку исходного кода веб-приложений на предмет наличия потенциальных уязвимостей веб-приложений, таких как SQL-инъекции, с использованием инструментов анализа кода веб-приложения (например, Solar appScreener, Solar inCode, Appchecker, Rips, Findbugs, Yasca, Visual Code Grepper, Code Warrior).

14. По возможности осуществлять проверку веб-приложения на наличие уязвимостей с использованием инструментов тестирования веб-приложений (например, Sqlmap, PT Application Inspector, Metasploit, OWASP ZAP, Burp Suite).

По результатам выполнения указанных рекомендаций просим проинформировать Управление ФСТЭК России по Сибирскому федеральному округу до 25 ноября 2023 г.

Исполняющий обязанности
руководителя Управления  И.Косинский