**ОСНОВЫ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ВЕДОМСТВЕННЫХ ВЕБ-ПОРТАЛОВ ОТ АТАК МЕЖСАЙТОВОГО СКРИПТИНГА**

**Лысанов Иван Юрьевич**

*Сотрудник Академии ФСО России*

**Дмитрова Ксения Алексеевна**

*Сотрудник Академии ФСО России*

Ведомственные веб-порталы создаются и развиваются для обеспечения доступа органов государственной власти Российской Федерации к информационному пространству сообщества сетей Интернет и публикации официальных материалов, относящиеся к деятельности органов государственной власти Российской Федерации. Ведомственные веб-порталы представляют собой сегмент сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации [1].

Основным предназначением создаваемой системы служит организация информационного обмена между объектами ведомственных веб-порталов и доступ пользователей к ресурсам сети Интернет. Внешний информационный обмен по открытым публичным сетям связан с реальными угрозами информационной безопасности. Таким образом, подсистема информационной безопасности является ключевым элементом при построении ведомственных веб-порталов [2].

Межсайтовый скриптинг (XSS) - это атака на веб-приложения, в которой код скрипта внедряется в выходные данные приложения, а затем отправляется в веб-браузер пользователя. В браузере этот код выполняется и используется для передачи конфиденциальных данных третьей стороне (например, злоумышленнику) [3].

Для реализации методики по защите ведомственных веб-порталов от атак типа межсайтового скриптинга разработан прототип автоматизированного рабочего места аудитора защищенности ведомственных веб-порталов от атак межсайтового скриптинга, представляющий собой программный межсетевой экран прикладного уровня. Использование данного приложения позволяет обнаружить и предотвратить атаки межсайтового скриптинга на ведомственные веб-порталы, основанных на методах GET и POST. Данное программное обеспечение может быть применено на оборудовании ведомственных веб-порталов.

Для проверки функционирования программного комплекса запустим приложение в «мягком» режиме (режим обнаружения атак), как показано на рисунке 1 и совершим атаки на веб-портал.

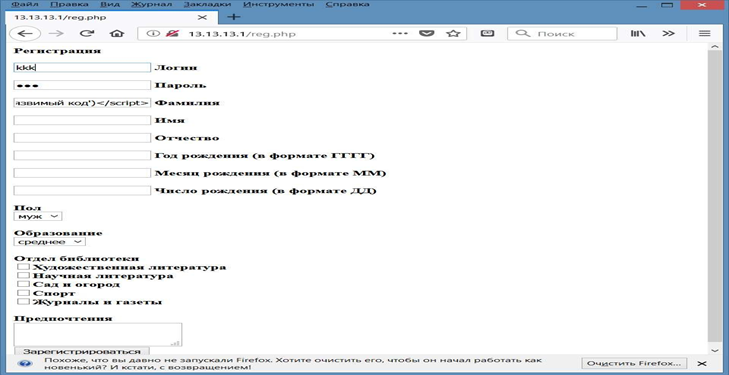


Рисунок 1 – Попытка совершения атаки межсайтового скриптинга

При попытке ввода вредоносного кода в окне отчетов было произведено оповещение об атаке, представленное на рисунке 2.

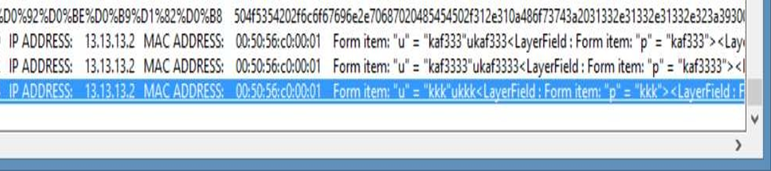


Рисунок 2 – Отчет при совершении атак межсайтового скриптинга в мягком режиме

В мягком режиме программа работает как система обнаружения вторжений, то есть не блокирует трафик, проходящий через эту систему, аналогично и при совершении атак через скрипт с «закладкой», эти атаки будут обнаружены, пример обнаружения этих атак представлен на рисунке 3.

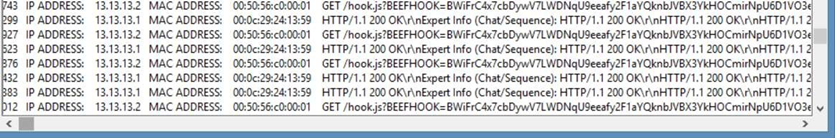


Рисунок 3 – Пример отчетов об атаках, совершенных через программное обеспечение BeEF

Для проверки работоспособности в «жестком» режиме, при котором атаки межсайтового скриптинга не проходят на веб-портал, необходимо запустить данный режим, как показано в меню, представленном на рисунке 1. Совершим атаки при программе, работающей в жестком режиме, попытка совершения атаки представлена на рисунке 4.

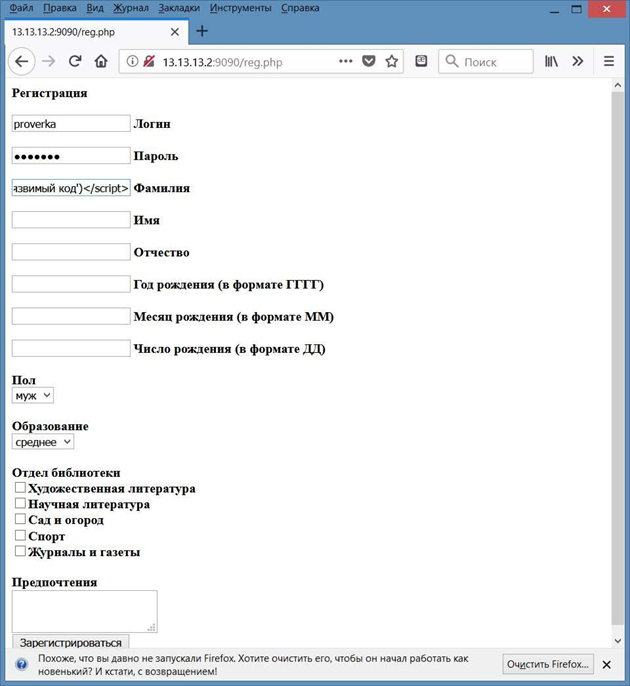


Рисунок 4 – Попытка совершения атаки на веб-портал

Атака не проходит, так как включен «жесткий» режим. Блокирование атаки представлено на рисунке 5.

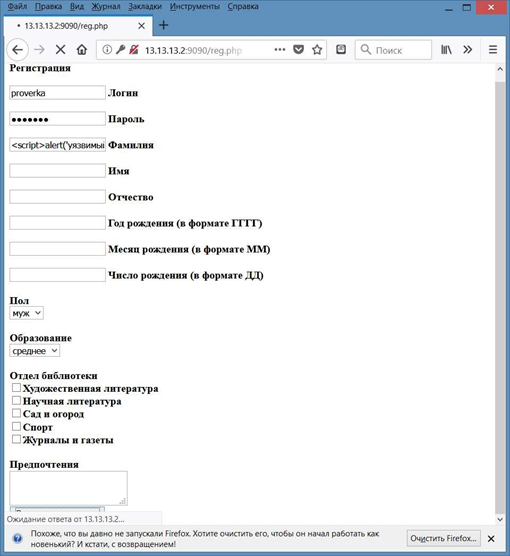


Рисунок 5 – Блокирование атаки межсайтового скриптинга

При блокировании атаки в браузере атакующего появляется значок попытки загрузить или отправить запрос в левом верхнем углу. А потом появляется страница о том, что соединение было сброшено. Программа выдает отчет о заблокированном запросе. Отчет представлен на рисунке 6.

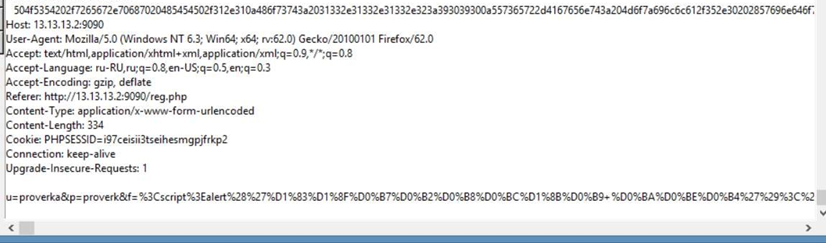


Рисунок 6 – Отчет о блокировке атаки межсайтового скриптинга

В настоящее время одним из важных направлений защиты автоматизированных систем является защита веб-порталов. В данной области отсутствуют необходимые ведомственные и государственные нормативные документы, вся работа строится вокруг иностранных и международных работ, лишь некоторые частные компании в стране занимаются данной проблематикой. В конечном итоге мы убедились, что рассмотренная программа закрыла уязвимость к атакам межсайтового скриптинга, которые были совершены на веб-портал.

Направлением дальнейших исследований является разработка более глубоких методов обнаружения и предотвращения атак межсайтового скриптинга, а также развитие инструментальных средств и формирование нормативной базы в данной области.

СПИСОК ЛИТЕРАТУРЫ

1. **ФСТЭК. Приказ №17: Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах** [Текст]. – Москва: Стандартинформ, 2017. – 27 с.

2. **ФСТЭК. Методический документ: Меры защиты информации в государственных информационных системах** [Текст]. – Москва: Стандартинформ, 2017. – 122.

3. **МЕЖСАЙТОВЫЙ СКРИПТИНГ XSS И МЕТОДЫ ЗАЩИТЫ** [Электронный ресурс] // МЕЖСАЙТОВЫЙ СКРИПТИНГ XSS И МЕТОДЫ ЗАЩИТЫ [сайт]. URL: https://www.elibrary.ru/item.asp?id=46168827 (дата обращения 05.11.2021 г