УДК 537.531

МЕТОДИКА РАЗРАБОТКИ ЗАЩИЩЕННОГО ПРИЛОЖЕНИЯ ДЛЯ СИСТЕМЫ ИНТЕРНЕТ-БАНКИНГА

Кукла Д.С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

За последние несколько лет в сфере информационной безопасности наметилась четкая тенденция, большая доля веб-приложений находятся под атакой. Веб-приложения продолжают оставаться основным вектором атак для преступников, и тенденция не показывает никаких признаков ослабления; злоумышленники все чаще избегают сетевых атак благодаря межсайтовому скриптингу, SQL-инъекциям и многим другим методам проникновения, направленным на прикладной уровень. К уязвимостям веб-приложений можно отнести многие вещи, включая плохую проверку ввода, небезопасное управление сеансом, неправильно настроенную систему настройки и недостатки операционных систем и программного обеспечения веб-сервера.

Взлом веб-приложений является одним из наиболее часто используемых методов кибератак как на организации, так и на частных лиц. Взломанные сайты используются в различных целях – для распространения вредоносного ПО, кражи информации, размещения несанкционированной рекламы или запрещенной информации, мошенничества, проникновения во внутреннюю сеть компании.

Перечень наиболее распространенных атак со временем практически не меняется: на верхних строчках рейтинга традиционно SQL Injection, Path Traversal и XSS. Суммарно они составляют более половины всех выявляемых кибератак на веб-ресурсы компаний.

Основными протоколами обеспечения безопасности процесса взаимодействия информационных систем являются SSH, IPsec и SSL/TLS. Сравнение данных протоколов приведено в таблице 1.

Таблица 1.3.1 - OWASP топ 3 наиболее критических рисков безопасности для веб-приложений

	Название угрозы	Описание
A1	Сломанный контроль доступа	Управление доступом применяет политику таким образом, что пользователи не могут действовать за пределами своих предполагаемых разрешений. Сбои обычно приводят к несанкционированному раскрытию информации, модификации или уничтожению всех данных или выполнению бизнес-функций за пределами возможностей пользователя.
A2	Криптографические сбои	Основное внимание уделяется сбоям, связанным с криптографией (или ее отсутствием)
A3	Инъекция	Некоторые из наиболее распространенных инъекций – SQL, NoSQL, команда ОС, реляционное сопоставление объектов (ORM), LDAP, язык выражений (EL) или библиотека навигации по графу объектов (OGNL).

Наиболее критичными являются уязвимости в сфере финансовых организаций. В первую очередь стоит отметить банковские сервисы, которые предоставляют пользователям возможность распоряжаться их деньгами – оплачивать услуги, открывать вклады и брать кредиты, переводить средства другим пользователям. Именно атаки на клиентов располагаются на первой строчке по

распространенности среди атак на веб-приложения финансовых организаций, в частности «Межсайтовое выполнение сценариев» (Cross-Site Scripting).

Таким образом, веб-приложения финансовых компаний с точки зрения рисков выделяются на фоне сайтов организаций из других отраслей.

Список использованных источников:

1. OWASP Top 10 – 2021 [Электронный ресурс]. – Режим доступа : https://owasp.org/Top10/

2. Исследование актуальных киберугроз 2019 – [Электронный ресурс]. – Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2019/

3. Classification of Web Application Vulnerabilities – [Электронный ресурс]. – Режим доступа : http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_35.pdf