На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

ім'я ресурсу. Зазвичай має такий вигляд: http://site.ua/category/3. Завдяки HTML я зробив структуру сайту, яку оформив таблицями стилів CSS. PHP робить сайт динамічним, дозволяє створювати автоматичні сторінки сайту з шаблонами HTML + CSS для відповідних розділів.

Таким чином, шляхом створення інтернет-магазину будівельних матеріалів, ми забезпечуємо максимальний зручний доступ покупців до вибору та купівлі безлічі товарів для будівництва за низькими цінами.

МЕЖСАЙТОВЫЙ СКРИПТИНГ. ОПАСНОСТЬ XSS-АТАК И ИНСТРУМЕНТЫ ЗАЩИТЫ

Болтач С. В., асистент кафедры ИТиКБ, ОНАПТ, Одесса

Развитие технологического прогресса и повышение социальной вовлеченности в использование веб-ресурсов имеет позитивные и негативные стороны. Веб-ресурсы проникают в разные стороны нашей жизни, содержат всё разнообразие информации, являются нашим инструментом и для нас же представляют опасность. Наличие информации, чаще конфиденциальной, предполагает тех, кто в ней заинтересован и соответственно, разработку методов доступа к ней. К последним относится XSS (Cross Site Scripting) или межсайтовый скриптинг, один из самых распространенных видов хакерской атаки реализуемой с помощью скриптов. Данный вид атаки возможен если пользователь может вводить на сайте информацию: обсуждения, записи, сообщения. При отсутствии соответствующей защиты вместо них вводится скрипт.

В чем опасность? С помощью XSS-атаки преступники могут достичь следующих целей: нарушение работы веб-приложения (потеря доверия), кража защищённой и конфиденциальной информации (информация о кредитных картах), кража аккаунта, похищение учетных данных пользователя устройства и т. д.

За 2015 год компания Wallarm зафиксировала более 100 миллионов атак на веб-ресурсы своих клиентов. Второе место занимают атаки, направленные на клиентские уязвимости, так называемый межсайтовый скриптинг или “XSS” (28,73%).

Для XSS-атак не имеет значения, какой ресурс взламывается, так как проблема безопасности заключается не в недостатке средств, а в отсутствии понимания сути угрозы. Конфликт в необходимости создания условий, при которых будет невозможна XSS-атака, то есть реализация фильтрации данных при отклонении ограничений для пользователя. Данное условие трудно выполнимо, по статистике, 42% процента веб-приложений, требующих проверки безопасности, уязвимы к XSS-атакам, которые продолжают представлять высокую опасность.

Такой высокий процент предполагает большую актуальность проблемы, а значит и нахождение разных способов её решения. Разработано уже достаточно

инструментов для тестирования веб-приложений для нахождения в нём уязвимостей и недостатков, использующих в своей работе разные подходы:

- Wapiti – проводит сканирования веб-приложений методом «чёрного ящика»;
- Concept Feedback – это веб-сайт, на котором другие пользователи могут протестировать ваш веб-сайт и оставить отзыв;
- Netsparker Community Edition выполняет сканирования веб-приложений на предмет возможности внедрения SQL кода;
- Wallarm разрабатывает решения для защиты веб-ресурсов, совмещающие в себе функции фаервола для веб-приложений (WAF) и активный сканер уязвимости;
- OWASP WebScarab Project – это Фреймворк, используется для анализа приложений, осуществляющих передачу данных через протоколы HTTP и HTTPS.

Каждая программа по-своему уникальна и имеет свои плюсы и минусы, но ни одна не дает 100% гарантии безопасности за счёт своей сосредоточенности на едином подходе.

Тестирование веб-приложений на предмет выявления уязвимых мест – это хорошая превентивная мера. Она предоставляет возможность еще на этапе разработки найти все недостатки приложения, обеспечив в конечном итоге выход надежного продукта [3]. Однако большинство сайтов подобное тестирование не проходят и представляют опасность для пользователя.

Суммируя вышеизложенное XSS-атаки бесспорно представляют одну из главных опасностей современного интернет-пространства. Разработанные инструменты, рассмотренные выше в большинстве своем не предназначены для обычного пользователя и больше подходят для проверки веб-приложения перед выкладкой на сервер. Лучшим же решением для большинства пользователей было бы расширение функционала антивирусов на предмет нахождения уязвимостей и недостатков веб-приложений.

Литература:

1. Вся правда об XSS или почему межсайтовое выполнение сценариев не является уязвимостью? (Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/post/149152/

2. Тренды 2015 года в области интернет-безопасности в России и в мире. Основные угрозы: DDoS-атаки и взлом веб-приложений. Январь 2016.

3. Тестирование безопасности веб-приложений (Электрон.ресурс)/Способ доступа: URL :http://www.rootfront.com/article/5869491/2013-02-18/testirovanie-bezopasnosti-veb-prilozhenij