ТЕСТИРОВАНИЕ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ XSS-АТАК

Д.С. Сацукевич

XSS (Cross-Site Scripting) – уязвимость веб-сайта, при которой совершается внедрение злоумышленником вредоносного скрипта в структуры веб-приложения, в результате чего может быть установлено вредоносное программное обеспечение (ПО) в клиентское приложение. Используя XSS-атаки, злоумышленники не нацеливаются на конкретных пользователей, а распространяют свой вредоносный код. В рейтинге OWASP «Топ 10 главных угроз WEB-приложениям» за 2020 год данная атака занимает 7 место. В результате реализации данной атаки может быть получен доступ к Cookie, хранимым браузером пользователя, в которых хранится различная персональная

информация. Выделяют два вида XSS: отраженная (непостоянная) и хранимая (постоянная) XSS атаки.

Для реализации отраженной атаки не обязательно хранить вредоносный скрипт на сервере, но необходимо, чтобы пользователь совершил какое-то действие, к примеру, перешел по ссылке вида http://Сайт.com/search.php?q=<script> Функция</script>. В ситуации, если на сайте не реализовано экранирование символов, данный GET-запрос будет исполнен как скрипт, в результате которого злоумышленник получит себе данные, хранимые в Cookie пользователя. При реализации хранимой XSS атаки вредоносный скрипт уже хранится на сервере и автоматически исполняется.

В рамках данного исследования было проведено тестирования системы электронного обучения учреждения образования на возможность реализации XXS-атак.

Изначально необходимо было произвести аутентификацию в тестируемой системе электронного обучения по известной учетной записи и изучить содержание Cookie пользователя. Было обнаружено, что значения Cookies хранятся в поле MoodleSession. Если предположить, что злоумышленник может реализовать перехват значений Cookies, то он получит доступ к профилю пользователя, что было и протестировано в данной работе. Для этого с другого компьютера был осуществлена попытка доступ к тестируемой системе электронного обучения, при реализации которой значения поля MoodleSession было вручную изменено на значения другого пользователя, которые предположительно ранее были перехвачены злоумышленником. В результате доступ к системе электронного обучения был успешно получен злоумышленником.

Необходимо отметить, что в тестируемой системе использован метод защиты от XSS-атак, суть которого в том, что все Cookie, необходимые для авторизации, имеют флаг HttpOnly, из-за чего JavaScript не имеет доступа к данным, содержащимся в данных полях [1–4].

Литература

1. OWASP Top Ten [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/ – Дата доступа: 20.04.2021.

2. Cross-Site Scripting (XSS) [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS). – Дата доступа: 20.04.2021.

3. XSS атака – межсайтовый скриптинг [Электронный ресурс]. – Режим доступа: https://insafety.org/xss.php – Дата доступа: 20.04.2021.

4. JavaScript и куки (cookie) [Электронный ресурс]. – Режим доступа: https://ruseller.com/lessons.php?id=593 – Дата доступа: 20.04.2021.