CERT-UA

CSRF

“Cross-Site Request Forgery”

Автори:
Міснік Олексій
Антонішин Михайло
Computer Emergenscy Response Team of Ukraine – CERT-UA
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

"CSRF" расшифровывается как “**Cross-Site Request Forgery** (меж-сайтовая подделка запроса)”. Данный тип атак направлен на имитирование запроса пользователя к стороннему сайту. CSRF-уязвимости достаточно широко распространены среди сегодняшних веб-приложений из за того, что многие из них не чётко определяют - действительно ли запрос сформирован настоящим пользователем. Хотя в некоторых ситуациях определить это просто невозможно. Как пример можно взять процедуру изменение профиля в форумах IPB или phpBB - при изменении номера ICQ или адреса домашней странички у Вас не спрашивают ни пароля, ни кода с какой ни будь картинки. Единственным средством распознавания клиента являются cookies или идентификатор сессии. Соответственно если с помощью определённого кода заставить браузер отправить нужный нам запрос на сторонний сайт, то он сможет вполне нормально пройти даже к тем скриптам, в которых нужна авторизация – ведь браузер при запросах к сайту отправляет ему и cookies. Главное чтоб пользователь заранее был авторизирован. В свете того, что большую популярность приобретает технология AJAX, основывающаяся на формировании и отправке HTTP запросов на стороне пользователя, данная атака становится более распространённой. Хотя уже и сейчас можно производить CSRF-нападения практически на любой сайт. Странно только то что в последнее время интерес к уязвимостям подобного вида всё больше и больше угасает. Скорее всего это отголоски нежелания учиться новому. Для лучшего понимания подобных атак рассмотрим CSRF-уязвимость, обнаруженную нашей командой, в SLAED CMS. Суть обнаруженной уязвимости в следующем - скрипт администрирования никак не убеждается в том что запрос к админ-панели осуществлён самим администратором. Как пример, в описании уязвимости мы рассматривали ссылку на удаление блока No1. Она имеет следующий вид:

http://slaed/admin.php?op=BlocksDelete&bid=6&ok=1

То есть команда на удаление определённого блока отдаётся через данные передающиеся в ссылке. Для удаления этого блока злоумышленник может оставить в каком-либо комментарие изображение, ссылающееся на этот адрес. Соответственно, при просмотре администратором странички с опасным изображением, браузер обратится по этой ссылке для загрузки картинки и, если администратор уже зашёл в админ-панель, вызовет удаление первого блока. Это достаточно яркий пример использования CSRF-нападений. Так же смысл подобных атак не всегда основывается на таких действиях как редактирование или отправка форм.

В конце главы мы рассмотрим примеры использования CSRF-атак для подбора паролей или CGI-сканирования. Что же мы будем рассматривать в этой главе? Ниже мы рассмотрим различные варинаты имитирование отправки запроса пользователем на сторонние сайты с какой либо целью. Осуществлять это мы будем с помощью трёх инструментов:

1. С помощью уже знакомого нам тэга “IFrame”
2. С помощью компонента XMLHTTP.
3. С помощью Flash-ролика.

Мы будем работать с POST и HEAD запросами. Думаю имитация GET-запроса не составит особого труда, хотя бы с помощью тэга <img>

Первый вариант проведения CSRF-атак (через <iframe>) может быть использован со всеми браузерами. Что, в принципе нам только на руку. А вот со вторым вариантом есть один нюанс: многие браузеры не разрешают формировать запросы, идущие на другие сайты, с помощью компонента XMLHttpRequest. Сделано это из соображений безопасности. То есть во всех браузерах кроме IE запросы с помощью данного компонента можно отправлять только в пределах одного домена.