УДК 004.057.4

HTTP-ЗАГОЛОВОК XFF КАК ЭЛЕМЕНТА ОСУЩЕСТВЛЕНИЯ НСД К ВЕБ-РЕСУРСАМ

А.М. МАКСИМОВ

Ростовский государственный экономический университет
344002, Российская Федерация, г. Ростов-на-Дону, ул. Б. Садовая, 69
электронная почта: ironmanpc@rambler.ru

Статья посвящена рассмотрению одного из аспектов функционирования современных компьютерных сетей – заголовкам протоколов. Рассмотрение включает в себя краткий анализ документов, в которых представлены стандарты, регулирующие функционирование рассматриваемого протокола HTTP в сети Интернет.
В результате анализа с точки зрения безопасности установлено наличие риска использования заголовка XFF (X-Forwarded-For). Риск представляет собой возможность осуществления несанкционированного доступа (НСД) с повышенными привилегиями к запрашиваемому ресурсу. Помимо этого рассмотрена ситуация, когда данная возможность осуществления НСД с использованием указанного заголовка может быть реализована (в т.ч. ситуации, когда происходит взаимодействие компонентов различных уровней (веб-сервер и веб-приложение). По результатам исследования сформулированы некоторые положения, позволяющие уменьшить вероятность реализации обнаруженной угрозы.
Ключевые слова: XFF, HTTP-заголовок, REMOTE_ADDR.

Используемые в настоящее время протоколы передачи данных регламентированы различными документами. Большинство таких документов имеют название RFC (англ. Request for Comments - Тема для обсуждения) и номер и публикуются организацией IEFT (англ. Internet Engineering Task Force - Инженерный совет Интернета). Помимо смысловой нагрузки аббревиатуры, RFC рассматривается именно как стандарт для сети Интернет и охватывает подавляющее число параметров, так или иначе связанных с её функционированием. Однако не исключено существование некоторых свойств, не описанных в RFC. Более того, такие свойства действительно существуют. Одним из таких стандартов де-факто является проект стандарта, описывающий поле заголовка XFF протокола HTTP.[1]

Данный заголовок поддерживается большинством распространённых продуктов и устройств, реализующих функции прокси-серверов, кэширования, балансировки нагрузки, веб-серверов и т.д. Поддержка присутствует в таких продуктах как Apache, Microsoft IIS, Nginx. Ежемесячные исследования,

проводимые порталом Netcraft.com, по состоянию на 6 июня 2014 года показали следующую статистику: среди 968 882 453 исследованных сайтов, 36,50% использует веб-сервер Apache, 36,35% - веб-сервер Microsoft IIS, 13,81% - веб-сервер Nginx. Таким образом, на долю трёх перечисленных платформ приходится 86,66% исследованных сайтов.[2]

Если предположить, что в схеме подключения не используются заголовки типа XFF, то для веб-сервера все пришедшие подключения из сети интернет будут представлены исключительно внешними IP-адресами (т.е. набор, состоящий из N клиентов частной подсети с прокси-сервером, например, 192.168.0.0/24 будет выглядеть для веб-сервера как один и тот же клиент с внешним IP-адресом).

При использовании заголовков типа XFF, веб-сервер имеет возможность определять не только внешний IP-адрес, но и частный адрес клиента. Частные адреса не повторяются в рамках одной подсети, находящейся за устройством с внешним IP-адресом. Комбинация этих значений позволяет однозначно определить, кто из клиентов внутри частной подсети осуществляет доступ к веб-серверу.

Информацию об исходном адресе подключения используют как способ повысить защищённость веб-ресурса путём ограничения доступа к определённому функционалу ресурса со всех IP-адресов, кроме заранее определённых. Такие рекомендации можно встретить, например, при установке и настройке БД MySQL, где имеется соответствующий пункт меню с пояснением(возможность только лишь локального управления).

Как уже было указано ранее, наиболее распространённые веб-серверы поддерживают обработку заголовка XFF, и в дальнейшем передают полученные данные непосредственно ресурсу, развёрнутому на базе этого веб-сервера. Полученный из заголовка XFF адрес присваивается как значение переменной REMOTE_ADDR, откуда затем и передаётся веб-ресурсу. Данная переменная также поддерживается подавляющим количеством веб-серверов

(например, в Apache посредством модуля mod_rpaf, или в Microsoft IIS средствами из комплекта поставки).

В случае недостаточного внимания к процессу конфигурации веб-сервера в части использования нестандартных заголовков, становится возможным получить несанкционированный доступ путём проведения некоторых предварительных подготовительных действий.

Самым простым вариантом является развёртывание прокси-сервера атакующим. Таким образом, в заголовок XFF можно включить адрес 127.0.0.1. При этом для уязвимого веб-ресурса будет присутствовать видимость того, что клиент подключается с локальной системы.

Данная ситуация, например, воспроизводима с одним из популярных средств администрирования phpMyAdmin для СУБД MySQL. Несмотря на то, что изначально при конфигурировании MySQL был запрещён доступ к БД и к средству администрирования БД со всех адресов, кроме 127.0.0.1, при доступе по предложенной схеме, административная панель становится доступна. При этом выявить источник проблемы может быть затруднительно, поскольку на уровне веб-сервера в журналы доступа в качестве клиента будет записан адрес, который фигурирует как значение переменной REMOTE_ADDR, т.е. 127.0.0.1.

Таким образом, проблема вполне может возникнуть из-за разности в конфигурации между приложением и сервером.

В качестве решения проблемы можно использовать подход, когда правила доступа к административным частям веб-ресурса регулируются не исключительно по адресам подключающихся клиентов, но с использованием данного функционала вкупе с другими.

Другим решением, которое поможет сократить вероятность коллизий, когда адрес из чужой частной подсети воспринимается как адрес из своей частной подсети, может быть переход на IPv6. В силу особенностей IPv6 (сильная ограниченность адресного пространства IPv4 по сравнению с IPv6) пропадает практическая необходимость таких механизмов, как NAT. Однако это снижает возможности лишь случайных ситуаций получения доступа к

ресурсам не уполномоченными на это лицами. При этом не исключается возможность целенаправленного воздействия злоумышленником, поскольку в стандарте IPv6 по-прежнему присутствуют такие понятия как:

- Loopback - представлен в IPv4 как 127.0.0.1/8, т.е. localhost. В IPv6-адресации данный адрес представлен в виде ::1/128.

- Unique Local Unicast – стандарт RFC[3], пришедший на смену стандарту site-local[4] (аналог сетей 10.0.0.0/8, 172.16.0.0/16 и 192.168.0.0./24).

Таким образом, в качестве общих рекомендаций к решению проблемы, можно предложить следующее:

- не строить систему безопасности на основе одного элемента/ При необходимости использования рассмотренного заголовка XFF в целях безопасности следует совмещать несколько средств безопасности, например с использованием пары «логин-пароль»;

- не доверять непроверенным данным, приходящим в приложение из других (в т.ч. смежных) систем.

ЛИТЕРАТУРА

1. Стандарт «Forwarded HTTP Extension» // [Электронный ресурс] The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc7239.

2. Исследование веб-серверов «June 2014 Web Server Survey» // [Электронный ресурс] The Internet Engineering Task Force (IETF). URL: http://news.netcraft.com/archives/2014/06/06/june-2014-web-server-survey.html.

3. Стандарт «Unique Local IPv6 Unicast Addresses» // [Электронный ресурс] The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc4193.

4. Стандарт «Deprecating Site Local Addresses» // [Электронный ресурс] The Internet Engineering Task Force (IETF). URL: http://tools.ietf.org/html/rfc3879.

XFF HTTP-HEADER AS ELEMENT OF UNAUTHORIZED ACCESS TO WEB RESOURCES.

A.M. MAXIMOV

Rostov State University of Economics
69, B. Sadovaya st., Rostov-on-Don, Russian Federation, 344002

Review includes short analysis of documents, which describe standards and functioning of HTTP-headers. Also there was reviewed importance of the proper use of headers due to wide presence of platforms with X-Forwarded-For HTTP-header support.
The presence of risk in case of the X-Forwarded-For de facto standard header use was determined. Threat realization allows unauthorized access with elevated privileges to the target system. Beside this, case when X-Forwarded-For header represents the unauthorized entry point. In conclusion, some affirmations, based on obtained result, were formulated to reduce chances of system penetration.
Key words: XFF, HTTP-header, REMOTE_ADDR.