Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Р Е Ф Е Р А Т

Компьютерные сети

Тема: Безопасность протоколов передачи данных. HTTPS.

Студенты: Зыкин Д.А.
Бабаджанян Р.В.

Группа: ИУ7-73 - ИУ7-76

Преподаватель: Рогозин Н. О.

Москва, 2019

Статистика, представленная Google, свидетельствует: за 2016 год в интернете зафиксировано на 32% больше взломов сайтов, чем годом раньше[1], и в будущем прогнозируется рост этого показателя. Казалось бы, с увеличением количества и качества средств защиты угроз сайтам должно стать меньше. Но цифры — вещь упрямая, и очевидно, что хакеры также успешно совершенствуют свое мастерство.

В нашем обзоре мы расскажем о протоколе безопасного соединения HTTPS, сертификатах безопасности и видах уязвимости сайтов. Целями злоумышленников чаще всего становятся сайты банков, мобильных операторов, известные медиапорталы, правительственные учреждения. Объясняется это тем, что взлом таких сайтов, во-первых, может помочь заработать немалые деньги, а во-вторых, дать доступ к важной информации. Подвергаются взлому и те сайты, аудитория которых ежедневно составляет несколько тысяч посетителей.

Но владельцам небольших сайтов не стоит заблуждаться и чувствовать себя в безопасности. Мелкие сайты нередко используются как плацдарм для тренировок перед взломом больших или для нецелевых атак, когда атакуются сразу сотни или тысячи ресурсов, выбранных по определенному критерию. Есть мнение, что каждый третий сайт находится под наблюдением посторонних людей, которые изучают его уязвимости и в любой момент могут совершить взлом. А значит, главная задача владельца — максимально защитить сайт от всех возможных угроз, чтобы не потерять важную информацию и собственные деньги.

Виды уязвимостей сайта

Так что же представляют собой эти таинственные уязвимости, через которые и совершается большинство взломов? Сам термин «уязвимость» — это перевод английского слова vulnerability, он означает недостаток в коде сайта или программном обеспечении, используя который можно нарушить работу системы. Часто появление уязвимости бывает вызвано ошибками программирования, недостатками при проектировании сайта или ненадежными паролями. Уязвимости позволяют атакующему заставить интернет-приложение совершить действия, на которые у того нет прав.

К основным типам уязвимостей относятся следующие:
- недочеты системы аутентификации и управления сессией;
- небезопасные прямые ссылки на объекты;
- небезопасная конфигурация;
- утечка чувствительных данных;
- отсутствие контроля доступа к функциональному уровню;
- использование устаревших компонентов;
- невалидированные редиректы (несанкционированные перенаправления);

- кликджекинг (использование невидимых элементов).

Это далеко не полный перечень, к тому же постоянно появляются все новые и новые уязвимости. Мы сегодня расскажем только об одном типе уязвимости — небезопасной передаче данных и о ключевых видах атак, ей вызванных. Доля взломов сайтов, вызванных небезопасной передачей, например, в мобильных банковских системах, составляет 73%.

Поскольку каждое действие в интернете — это обмен данными, то каждый раз, когда пользователь открывает нужный сайт или отправляет сообщение в соцсети, компьютер посылает запрос серверу и получает ответ. Обычно обмен идет по протоколу HTTP. Он устанавливает правила обмена данными, и именно с его помощью содержание сайта загружается на устройство.

Несмотря на популярность и удобство использования, данные протокола абсолютно ничем не защищены, они передаются в открытом виде. На пути от компьютера или смартфона пользователя до сервера информация проходит через огромное количество неких промежуточных пунктов. Если хоть один из них взят под контроль посторонними людьми, имеющими злой умысел, данные с легкостью могут быть перехвачены. Вот только несколько видов атак, причиной которых может стать небезопасная передача данных:

Кража паролей

Первая причина взлома — кража пароля к аккаунту или административной части сайта. Это может случиться из-за вируса, устаревшей версии браузера, с которого введен пароль или даже из-за того, что пароль был слишком простым — хакеры без труда его подобрали.

Несмотря на вполне реальную опасность хакерского вмешательства, многие владельцы сайтов для аутентификации до сих пор используют открытый канал. В результате этого пароли без проблем перехватываются мошенниками, имеющими доступ к сети, в которой работают несознательные пользователи.

В результате кражи пароля злоумышленники получают доступ к сайту и большой простор для мошеннических манипуляций. Например, с сайта может рассылаться спам, но это еще не самое страшное. Другая причина кражи клиентских аккаунтов — это именно взлом сторонних сайтов. Получив доступ к сайту через украденный пароль, хакеры непременно воспользуются и конфиденциальной информацией о клиентах. Следующим их шагом будет использование этой информации с выгодой для себя, например, снятие денег с банковских карт. Крупные сервисы, например, банки, постоянно работают над защитой своих паролей, тогда как мелкие интернет-магазины, форумы, торрент-трекеры нередко этим пренебрегают. Хакеры, конечно, знают об этом, и нередко атакуют именно их.

В августе 2014 года появилась информация о том, что хакерская группировка из России CyberVor похитила 4,5 млрд учетных записей. Логины и пароли были украдены с 420 000 веб-сайтов. Хакеры взломали множество ресурсов крупных компаний, но не упустили из виду и мелкие, и даже личные сайты. По оценке представителей американской компании, HoldSecurity, занимающейся информационной безопасностью, в руки к преступникам попала самая большая база учетных данных.

Взлом через хостинг-провайдера

Нередко взломы сайтов происходят по вине хостинг-провайдера. Во-первых, это может происходить по причине того, что на сервере установлено устаревшее программное обеспечение, которое взломать проще, чем новое ПО.

Во-вторых, взлом происходит через соседей по аккаунту. Сайты редко размещаются изолированно, по одному на каждом аккаунте. В большинстве случаев они соседствуют друг с другом, а ненужный или забытый веб-проект, которому не уделяется внимание в сфере защиты, легко может быть взломан. И это потянет за собой и взлом всего аккаунта.

В-третьих, взлом может произойти из-за того, что сайт размещен не у профессионального провайдера, а, например, у знакомого программиста для экономии денег. Если у него нет нужных компетенций или опыта безопасного администрирования защиты, сервер будет взломан через уязвимые компоненты и настройки.

В начале этого года хакерская группировка взломала серверы подпольного хостинга Freedom Hosting II. Было скомпрометировано более 10 000 сайтов сети Tor и похищена база данных хостинга, включающая адреса электронной почты 381 000 пользователей.

Взлом CMS

Для управления контентом, структурой и дизайном сайта используются системы управления сайтом (Content Management System — CMS). Программирование, дизайн и поддержка сайта с использованием таких систем доступно даже для людей, имеющих очень смутное представление о программировании и вообще о web-архитектуре.

Но, как и все виды ПО, CMS содержит уязвимости, через которые ее можно взломать. Особенно эта угроза актуальна для популярных систем, поскольку их взлом дает возможность взломать сразу десятки тысяч сайтов по всему миру.

Используя уязвимости системы, хакеры могут размещать на сайте код, заражающий компьютеры посетителей вредоносными программами, публиковать контент сомнительного содержания или перенаправлять пользователя на другие сайты с таким контентом. Репутация сайта в этом случае серьезно страдает, из-за чего существенно уменьшается количество посетителей.

Взлом сайта через модули и компоненты вне CMS

Справедливости ради нужно заметить, что любую из указанных CMS в «чистом виде» взломать сложно даже хакерам очень высокого уровня. Опасность кроется во всевозможных расширениях — компонентах, плагинах, модулях, создаваемых сторонними разработчиками. Например, при установке компонента комментариев, в котором есть «дырка», хакер получит возможность вместо комментария залить на сайт специальный скрипт и совершить взлом.

SQL-инъекции

SQL-инъекция — это уязвимость, возникающая при недостаточной проверке и обработке передаваемых от пользователя данных. Она дает возможность хакерам модифицировать и даже выполнять не предусмотренные кодом программы запросы путем внедрения вредоносного кода в запрос к базе данных. Результатом является получение доступа к данным, к которым в обычных условиях доступ запрещен.

Использование этой уязвимости позволяет осуществлять кражу данных, их подмену или уничтожение и провоцировать отказ в обслуживании (DDoS). Есть подозрение, что именно с помощью SQL-инъекций осуществлялись громкие взломы последних лет, такие как утечка паролей с сайтов Yahoo, LinkedIn и eHarmony.

Отчет компании Akamai Technologies, Inc. показывает, что в 1 квартале 2016 года увеличение нападений, связанных с SQL-инъекциями, выросло на 87% по сравнению с предыдущим периодом. Около 60% атак приходится на сайты с медиа и развлекательным контентом, 30% — на сайты онлайн-услуг и 10% — на правительственные сайты.

Способов защиты от уязвимостей существует множество, в том числе и от каждого конкретного их вида. Это, прежде всего, использование лицензионного ПО, регулярное обновление CMS, отказ от простых паролей и небезопасных браузеров, установка межсетевого экрана. Одним из надежных средств защиты можно считать протокол https. О нем мы подробно поговорим ниже.

Как обеспечить безопасность веб-сайта, или Протокол HTTPS нас бережет

HTTPS — это некая защитная оболочка для обычного HTTP, позволяющая надежно шифровать передаваемую от пользователя к серверу и обратно информацию. Такое шифрование не допускает утечки данных, а значит, защищает сайт от взлома.

https: необходимость или рекомендация?

Переход на https вовсе не является жестким требованием для всех без исключения сайтов. Конечно, если сайт работает с платежными данными клиентов или любой другой персональной информацией, такой протокол должен быть установлен в обязательном порядке. Во всех остальных случаях переходить или не переходить на https решает только владелец сайта. Однако неприятности в случае взлома грозят любому сайту — рассылка спама, автоматический переход на сайты сомнительного содержания или даже полное уничтожение.

Кстати, использование https, как показывает практика, это серьезный плюс сайту со стороны клиентов и пользователей. Надежность соединения вызывает с их стороны больше доверия к самой компании. К тому же сайты с защищенным соединением лучше ранжируются поисковыми системами.

Как работает https

Как уже говорилось, протокол http, по которому осуществляется передача данных, практически ничем не защищен, и информация может стать легкой добычей хакеров. Для исключения возможности утечки в 1994 году был создан протокол https, использующий криптографическую систему SSL/TLS, которая шифрует все передаваемые данные и дает возможность установки защищенного соединения через незащищенный канал.

При установке соединения по протоколу https компьютер пользователя и сервер сначала генерируют некий секретный ключ, а затем уже обмениваются информацией, при этом шифруя ее с помощью данного ключа. Ключ создается заново при каждом сеансе связи, так что перехватить и подобрать его практически невозможно — он представляет собой число с количеством знаков более ста. Для полной надежности используется еще и цифровой сертификат для идентификации сервера. Первое, что делает браузер при установке соединения по https, — проверяет подлинность сертификата. Только после ее подтверждения начинается обмен данными.

Как перевести сайт на https

Перевести сайт на протокол https не так сложно, как может показаться. Процесс перехода состоит всего из нескольких шагов.

- Шаг 1. Получение и настройка сертификата. Получить сертификат можно в центрах сертификации за отдельную плату, но существуют и бесплатные варианты. Для небольших фирм они могут быть вполне приемлемы, но крупные компании обычно отдают предпочтения платным сертификатам, которые отличаются расширенной аутентификацией, возможностью включения субдоменов и т.д. Кроме того, бесплатные сертификаты иногда увеличивают время передачи данных в несколько раз из-за особенностей их обслуживания удостоверяющими центрами. И что очень важно, бесплатный сертификат не подойдет для сайтов с приемом онлайн-платежей, поскольку неизвестно, кто является владельцем такого сайта. Кстати, за услугу перевыпуска некоторых бесплатных сертификатов или внесения в них каких-либо изменений все равно придется заплатить. Затем сертификат нужно настроить. Цель настройки — переадресация всех запросов с http на https.

- Шаг 2. Работа с внутренними ссылками. Полные ссылки внутри сайта придется заменить на относительные с помощью скриптов. Поскольку после перехода прокол http не заменится на https автоматически, может возникнуть ситуация с загрузкой смешанного контента. Одновременное действие обоих протоколов не обеспечивает полноценной защиты и может привести даже к тому, что сайт совсем перестанет работать.

- Шаг 3. Переадресация. После установки сертификатов сайт станет доступен по двум адресам, из которых оставить нужно только тот, который начинается с https. Для этого нужно настроить прямой редирект «301» с http на https. Делается это на сервере, но можно и в htaccess, хотя последний вариант хуже. После этого даже http-запросы пользователей будут переадресовываться на сайт с новым протоколом.

- Шаг 4. Внесение изменений в файл robots.txt. Для того чтобы поисковые роботы могли обнаружить сайт с измененным протоколом, нужно указать этот протокол в файле robots.txt.

- Шаг 5. Включение HTTPS Strict-Transport-Security. Этот процесс индивидуален для каждого сервера, так что универсальных рекомендаций не существует. Для облегчения задачи можно обратиться к специалистам, которые разрабатывали сайт. И в заключение необходимо включить Secure Cookies — с этого момента информация на ресурсе надежно защищена.

Как выбрать сертификат безопасности для сайта (TLS/SSL)

При выборе сертификата можно пойти двумя путями. Если у вас небольшой офлайн-бизнес или личный блог, и вы просто хотите донести информацию о своей компании до потенциальных клиентов, используйте Domain Validation SSL. Этот вид верификации не позволит защищать субдомены и вести

финансовые операции через сайт. Зато сертификат делается быстро, и заработает он сразу после того, как вы подтвердите владение доменом. Это можно сделать несколькими способами: через e-mail, через запись в DNS и через хэш-файл. Стоимость таких сертификатов бывает относительно невелика, например, всего 610 рублей в год.

Для владельцев сайтов, на которых предполагаются финансовые онлайн-операции необходима установка сертификатов типа Business Validation. Такой вид сертификата надежнее, поскольку подтверждает не только владение доменом, но и связь компании с сайтом. Для верификации нужно отправить в верификационный центр пакет документов и принять звонок на корпоративный номер. Все сертификаты Business Validation делятся на несколько видов:

- Extended Validation SSL — сертификаты с расширенной проверкой, обычно используются банками, платежными системами, крупными интернет-магазинами — теми, кто работает с большими объемами денег.

- Wildcard SSL — защищает сам сайт и его поддомены. Используется в том случае, если предполагается несколько поддоменов с разной региональной привязкой.

- SAN SSL — поддерживает внешние и внутренние альтернативные доменные имена.

- CodeSigning SSL — подтверждает безопасность кодов и программных продуктов с сайта, пригодится разработчикам приложений.

Но какой бы сертификат не был выбран, сначала необходимо сгенерировать запрос на его получение, содержащий всю информацию о хозяине домена и открытый ключ. Запрос направляется в центр верификации. В результате выдается сертификат и файл с ключом, который ни в коем случае не должен попадать в открытый доступ. Сертификаты такого типа могут стоить несколько сотен тысяч рублей, например, приблизительная стоимость Symantec Secure Site Wildcard — от 281 967 рублей в год.

Даже стремление к экономии не должно приводить к отказу от обеспечения безопасности данных на сайте. Намного проще потратить средства и время на ее обеспечение, чем после взлома приводить сайт в порядок и бороться с негативной репутацией, которую спровоцировал этот взлом. А если сайт имеет отношение к онлайн-торговле, то его безопасность должна быть основной задачей владельца.