1 Врага нужно знать в лицо

В этой главе

- ✓ Как и почему нападают хакеры
- ✓ Что вас ждет, если ваш сайт взломают
- ✓ Насколько нужно включать паранойю
- ✓ Как начать работать с угрозой взлома

Запуск веб-приложения в интернете — нетривиальная задача. Шаги, которые нужно сделать на этом тернистом пути, не назовешь простыми: создать дизайн веб-страниц, написать код, добавить интерактивность на JavaScript, реализовать сервисы бэкенда, подружить их с базой данных, выбрать хостинг и зарегистрировать доменное имя. Однако результат, несомненно, стоит этих усилий: благодаря магии интернета ваш сайт станет доступен миллиардам пользователей.

Однако не все эти пользователи придут к вам с добрыми намерениями. Интернет является прибежищем для сложной экосистемы скриптов, ботов и хакеров, которые непременно попытаются воспользоваться каждой уязвимостью вашего веб-приложения в своих гнусных целях. Пожалуй, это самый обескураживающий момент веб-разработки: после всего того труда,

который вы вложите в создание вашего веб-приложения, придет незнамо кто, проколет вам шины и поцарапает краску.

Если вы читаете эту книгу, то, скорее всего, вы разработчик, который не считает угрозы безопасности пустыми словами и хочет понять, как защититься от них. Книга представляет собой полное руководство по веб-безопасности: вы узнаете, как защитить веб-приложения в браузере, в сети, на сервере и на уровне кода. Также я познакомлю вас с основными принципами безопасности, применимыми на каждом уровне абстракции.

Перед тем как углубиться в подробности, нелишним будет разобраться, кто же они такие, эти зловредные интернет-деятели, что ими движет и какими инструментами они пользуются. Поговорим о хакерах.

Как (и почему) нападают хакеры

Хакинг (hacking) в буквальном смысле означает попытку несанкционированного доступа к программным системам. Однако за этим определением не разглядеть всего разнообразия злоумышленников, населяющих интернет, хотя оно и охватывает несколько серых зон, которые мы и не подумали бы отнести к хакингу. (Станете ли вы хакером, если поделитесь с членами своей семьи логином от Netflix? Не отвечайте на этот вопрос, Рид Хастингс[1].)

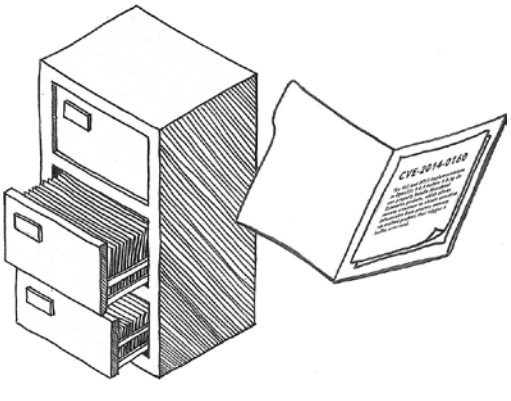
Давайте лучше обратим внимание на хакеров как таковых — на киберпреступников, мишенью которых станет ваше веб-приложение. Эти ребята используют интернет для совершения преступлений чуть ли не с тех самых пор, как он появился. Хакеров можно разделить на так называемых *черных хакеров*, или «черные шляпы» (black hat hackers), которые совершают злонамеренные (и незаконные) действия ради финансовой или политической выгоды, и *белых хакеров*, или «белые шляпы» (white hat hackers), — это те, кто пытается выявить уязвимости до того, как ими воспользуются «черные шляпы». Крупные компании частенько платят белым хакерам так называемые баг-баунти (bug bounty) в качестве вознаграждения за то, что они находят прорехи в стратегиях безопасности, опережая злоумышленников. Эта практика привела к появлению *серых хакеров*, или «серых шляп» (gray hat hackers), которые докладывают об уязвимости, но не эксплуатируют ее, если посчитают, что сообщить об этом будет более выгодно.

---

[1] Рид Хастингс (Reed Hastings) — соучредитель и директор компании Netflix. — *Примеч. пер.*

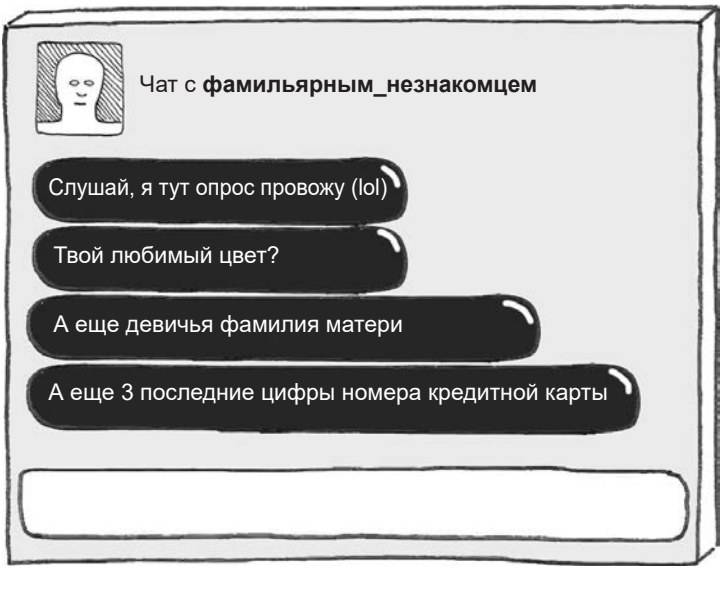
Для обнаружения уязвимостей хакеры по обе стороны баррикады применяют автоматизированные средства и скрипты. Исходный код таких средств, как правило, открыт, и достать их не составляет труда. Многие хакеры имеют на вооружении *Kali Linux*, особый дистрибутив Linux, содержащий самые популярные инструменты для цифровой криминалистики (форензики) и взлома. Белые хакеры используют Kali при проведении *пентестов* (penetration testing) — сканирования системы на предмет уязвимых точек доступа в рамках аудита безопасности. Черные хакеры прибегают к тем же инструментам для обнаружения уязвимостей, которые они могли бы использовать в своих интересах.

В мире белых хакеров существуют также *исследователи безопасности* (security researchers), которые работают над обнаружением, документированием и публикацией данных об уязвимостях в распространенном ПО. Исследователю поручается, например, обнаружить уязвимость на популярном вер-сервере, написанном на Java, таком как Apache Tomcat, и затем продемонстрировать авторам ПО, как она проявляется. Когда выпускается патч, решающий эту проблему, уязвимость вносится в каталог Critical Vulnerability and Exposure (CVE), поддержкой которого занимается MITRE Corporation, американская некоммерческая организация, специализирующаяся на кибербезопасности. Вы не раз могли видеть упоминания о подобных уязвимостях, снабженных номерами CVE.



Как только публикуется свежий CVE — а иногда и раньше, — становятся доступными эксплойты для проверки концепции (proof-of-concept exploits). *Эксплойты* — это фрагменты кода, которые демонстрируют, как можно использовать уязвимость для злонамеренных действий, например внедрения вредоносного кода в уязвимую систему. Подобные эксплойты быстро становятся частью хакерских инструментов, таких как *Metasploit*, используемых как черными, так и белыми хакерами для зондирования сайтов на предмет наличия уязвимостей. Черные хакеры держат в тайне сведения о том, что обнаружили, стараясь как можно дольше не допустить того, чтобы уязвимости были закрыты.

Эксплуатация уязвимостей ПО — не единственный прием в арсенале киберпреступников. Процесс, в ходе которого удается войти в доверие к объекту и убедить его поделиться конфиденциальной информацией (в частности, логином и паролем), называется *социальной инженерией*. Подобными действиями можно заниматься лично, по телефону или в мессенджерах. Возможно, вам приходилось сталкиваться с *фишинговыми* (phishing) электронными письмами, которые пытаются выманить у жертвы пароль к какому-нибудь ресурсу. Во многом преуспели хакеры и с технологией *целевого фишинга* (spear phishing, что можно перевести как «рыбалка с гарпуном»). В этом случае тайно наводятся справки о конкретных людях (чаще всего работающих в финансовых отделах компаний). Эта форма мошенничества расцвела пышным цветом в мессенджерах и социальных сетях.



Некоторые из самых дерзких киберпреступлений последних лет были совершены при содействии *злонамеренных инсайдеров* (malicious insider) — сотрудников или подрядчиков, решивших продать, а то и просто выложить в открытый доступ секретную информацию или интеллектуальную собственность либо навредить еще как-нибудь. Защититься от угрозы, исходящей от злонамеренного работника в организации, — одна из самых сложных задач, поэтому компании, подверженные этому риску, стремятся ограничить доступ к данным, предоставляя его только тем, кому он действительно необходим.

Почему киберпреступления настолько распространены? Ответ очевиден: потому что они весьма выгодны. Шестерни подпольной экономики вращаются в том числе в *даркнете* (dark web), где хакеры продают украденные данные, номера кредитных карт, уязвимости и даже скомпрометированные серверы. Платежи осуществляются в криптовалюте, вследствие чего их очень трудно отследить. Поскольку сайты даркнета доступны только в браузере Tor, обеспечивающем полную анонимность, эти рынки функционируют безнаказанно и остаются практически недосягаемыми для правоохранительных органов.

Помимо торговли краденым в даркнете, киберпреступники не гнушаются вымогательством денег непосредственно у своих жертв. Одной из форм вредоносного ПО являются *программы-вымогатели* (ransomware). Они зашифровывают файлы пользователя и блокируют доступ к ним до тех пор, пока злоумышленник не получит выкуп в криптовалюте. Нефтепроводы, клиники, мясокомбинаты, сети отелей — все успели побывать жертвами таких атак. Представители бизнеса в разных областях были вынуждены платить за разблокировку своих серверов. Программы-вымогатели получили столь широкое распространение, что их авторы стали действовать по модели франшизы, предоставляя группам черных хакеров свои инструменты бесплатно в обмен на долю с каждого заплаченного выкупа. Злоумышленники даже предлагают жертвам «каналы техподдержки» для помощи в расшифровке файлов после уплаты.

Стоит отметить, что хакинг не всегда обусловлен финансовыми причинами. Есть понятие *хакти-*

визм (hacktivism), обозначающее хакинг, которым по политическим соображениям занимаются некие провокаторы. Цели хактивистов порой понятны. Это может быть, например, нарушение работы сайта крайне правых путем лишения его пользователей анонимности — *доксинг* (doxing), подрыв репрессивных политических режимов или «слив» налоговых документов.

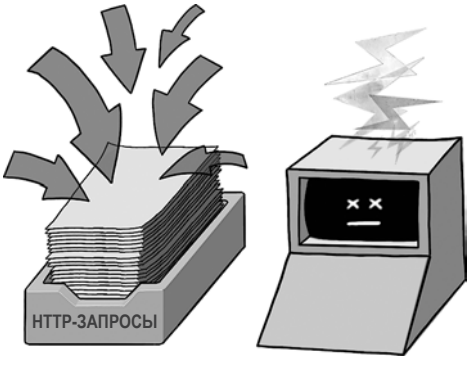
Кибершпионаж играет главную роль и в современном военном деле. Самые успешные хакерские группы финансируются государством. Хакеры, подпадающие под эту категорию, используют сложные методики наблюдения за своими объектами. Исследователи безопасности постоянно находятся в курсе таких *продолжительных атак повышенной сложности* (advanced persistent threats, APT), отслеживая используемые сигнатурные методы. Сообщество по вопросам безопасности дает угрозам забавные кодовые имена, контрастирующие с тем хаосом, который они способны посеять, например «Уютный медведь» (Cozy Bear) для русской группы хакеров или «Котенок-очаровашка» (Charming Kitten) для иранской проправительственной кибергруппы.

Преодоление последствий взлома

Теперь, когда мы познакомились с нашими противниками, давайте разберемся, что значит быть жертвой хакеров. Поскольку понятие «хакинг» охватывает широкий диапазон видов деятельности, пасть жертвой кибератаки означает столкнуться с целым букетом последствий разной степени суровости.

Прямым результатом взлома является недоступность вашего веб-приложения для других, законных пользователей. Этот вид взлома называется *атакой типа «отказ в обслуживании»*, или DoS-атакой (denial-of-service). Для этого злоумышленникам даже не нужно проникать за барьеры вашей безопасности. Нападающему достаточно бомбардировать ваши серверы таким количеством запросов, что другим посетителям просто не достанется вычислительных ресурсов.

Несмотря на кажущуюся простоту, предотвратить DoS-атаки может оказаться не так-то легко. *Распределенные DoS-атаки* (distributed denial-of-service, DDoS) вовлекают тысячи серверов для отправки запросов одновременно с разных IP-адресов, затрудняя блокировку вредоносных запросов на основании данных об их источниках. В 2006 году провайдер службы доменных имен (Domain Name System, DNS) под названием Dyn пал жертвой одной из самых крупных атак в истории. В результате самые популярные в мире сайты — от Amazon.com до Zillow.com — были недоступны бóльшую часть дня.



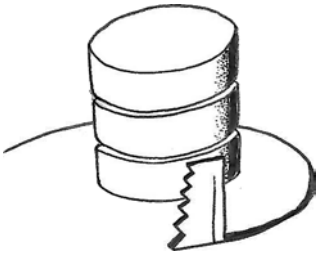
Другое возможное следствие взлома веб-приложения заключается в том, что хакер может использовать его как плацдарм для атаки на пользователей. Внедрение на сайт вредоносного кода JavaScript называется *межсайтовым скриптингом* (cross-site scripting, XSS) — это распространенная уязвимость, о которой мы поговорим в главе 6. Вредоносный код JavaScript может при-

вести к таким неприятностям, как завлечение пользователей обманом на мошеннические сайты или отслеживание активности пользователей на зараженном сайте. Скрипты-*кейлогеры* (keylogging) могут перехватывать логины и пароли, когда пользователь входит в систему. На сайтах финансовой направленности для кражи данных о кредитных картах используются *скимминговые* скрипты (web-skimming).

Данные для входа в систему часто служат целью для хакеров, потому что собранные логины и пароли можно продать в даркнете. Подобную информацию, относящуюся к популярным ресурсам типа Facebook, покупают мошенники, чтобы проворачивать свои аферы. (Да нет же, не торгует ваш дядюшка солнечными очками по суперценам. Скорее всего, его аккаунт был взломан, а данные проданы.) Украденные данные находят и косвенное применение: поскольку у людей есть привычка использовать на разных ресурсах одни и те же логины и пароли, хакер может протестировать имеющуюся у него информацию на множестве сайтов. Такая атака называется *атакой с распылением паролей* (password-spraying). Либо он может нацелиться на один сайт, перепробовав на нем целую базу данных украденных паролей в ходе атаки *подстановки учетных данных* (credential stuffing).

Самый быстрый способ украсть данные для входа «оптом» — найти способ проникнуть в базу данных и скачать ее содержимое. Для многих компаний такие *утечки данных* (data breach) являются худшим кошмаром, поскольку информация является их главным активом. В базах данных хранятся, впрочем, не только логины и пароли: из нее можно выудить токены доступа к сторонним сервисам, записи чатов, инсайдерскую информацию, личные данные, а также номера кредитных карт. Во многих странах компании, пострадавшие от утечки данных, по закону обязаны раскрыть клиентам масштабы утечки, что может нанести ущерб репутации компании.

Злоумышленник, которому удается получить доступ для записи (write access), получает возможность расширить зону поражения. Он может внедрить в базу данных вредоносный JavaScript-код, который будет выполняться на страницах веб-сайта жертвы. Также он может добавить на сайт вредоносные файлы (например, программы-вымогатели) и обманным путем заставить посетителей сайта скачать их.



Хакер, закрепившийся в вашей системе, будет *наращивать свои привилегии* до тех пор, пока у него не будет полного доступа к вашим серверам. Для этой цели обычно используют средства,

которые называются *руткитами* (rootkit). Хакер пытается завладеть учетной записью root вашего сервера с максимальными привилегиями. Хакер, получивший root-доступ, может начать использовать ваши вычислительные ресурсы в своих целях. Если сделать сервер частью *ботнета* (botnet) — централизованно управляемой сети зараженных компьютеров, называемых *ботами* (bot), то можно будет майнить криптовалюту, отправлять фишинговые письма, накручивать счетчики посещений (используя боты для искусственного раздувания числа просмотров страниц), а также осуществлять другие прибыльные операции. Доступ к скомпрометированным серверам можно продать в даркнете, то есть вашими вычислительными ресурсами будут торговать без вашего ведома.

Выявить зараженный сервер — сложная задача даже для фирм, которые занимаются этим профессионально. Как правило, для этого требуется сканирование на предмет нехарактерной активности в сети, поиск подозрительных файлов в файловой системе или выявление необъяснимого роста использования ресурсов. Современные хакерские группы идут еще дальше: они пытаются практиковать метод *living off the land*[1], имитируя существующие процессы и используя лишь те сервисы, которые доступны локально, чтобы не попасться.

Насколько нужно включать паранойю

Хакеры — это реальная угроза, и результаты их деятельности могут быть ужасающими. Компании, подвергшиеся взлому, терпят репутационный и финансовый ущерб. Кому нужен сервис, который сливает ваши данные? Кроме того, утечка данных может иметь юридические последствия, если выяснится, что жертва не позаботилась о безопасности своих систем должным образом. Кибератаки привели к банкротству многих предприятий.

Прежде чем впадать в панику, давайте оглянемся назад и реалистично оценим, насколько большую угрозу хакеры представляют для вашей организации. Оценка того, кому может понадобиться напасть на вас и что их может заинтересовать, называется *моделированием угрозы* (threat modeling).

---

[1] Living off the land в переводе с английского означает «питаться подножным кормом», то есть тем, что можно добыть на местности. По аналогии операторы LotL-атак «добывают на местности» инструменты для достижения своей цели: компоненты операционной системы и установленные самими администраторами целевой системы (https://encyclopedia.kaspersky.ru/glossary/lotl-living-off-the-land/). — *Примеч. ред.*