Разработка web-приложений

Безопасность web-приложений

Цыгулин Алексей Александрович к.т.н.

Безопасность

Разрабатывая своё приложение, стоит задумываться о его безопасности. Веб-безопасности. Не хотелось бы, чтобы в одно прекрасное утро на сайте появилась надпись «Hacked by %hackername%» на белом фоне или же чтобы все содержимое сайта, включая персональные данные пользователей ушли в чужие руки.

Общесетевые атаки (legacy)

- **Фишинг (phishing)** - вид атаки, который начинается с рассылки почтовых сообщений, содержащих ссылку на известный ресурс (или имитирующий такую ссылку). Дизайн веб-страницы обычно копируется с воспроизводимого ресурса.
- **Спуфинг (spoofing)** - одна из разновидностей фишинга. Ее суть заключается в атаке через DNS (или каким-то иным способом), когда страница с известным URL подменяется страницей злоумышленника.
- **Социальная инженерия** - это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.
- **Троянский конь (Spyware)** - программа, записывающая все нажатия клавиш на терминале или мышке, способна записывать screenshot'ы и передавать эти данные удаленному хозяину.

Аутентификация (Authentication)

- Подбор (Brute Force)

автоматизированный процесс проб и ошибок, использующийся для того, чтобы угадать имя пользователя, пароль, номер кредитной карточки, ключ шифрования и т.д.

- Недостаточная аутентификация (Insufficient Authentication)

эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации

- Небезопасное восстановление паролей (Weak Password Recovery Validation)

эта уязвимость возникает, когда Web-сервер позволяет атакующему несанкционированно получать, модифицировать или восстанавливать пароли других пользователей

Авторизация (Authorization)

- Предсказуемое значение идентификатора сессии (Credential/Session Prediction)

предсказуемое значение идентификатора сессии позволяет перехватывать сессии других пользователей

- Недостаточная авторизация (Insufficient Authorization)

недостаточная авторизация возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен

- Отсутствие таймаута сессии (Insufficient Session Expiration)

в случае если для идентификатора сессии или учетных данных не предусмотрен таймаут или его значение слишком велико, злоумышленник может воспользоваться старыми данными для авторизации

- Фиксация сессии (Session Fixation)

используя данный класс атак, злоумышленник присваивает идентификатору сессии пользователя заданное значение

Атаки на клиентов (Client-side Attacks)

- Подмена содержимого (Content Spoofing)

используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированны Web-сервером, а не переданы из внешнего источника

- Межсайтовое выполнение сценариев (Cross-site Scripting, XSS)

наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя

- Расщепление HTTP-запроса (HTTP Response Splitting)

при использовании данной уязвимости злоумышленник посылает серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа

Выполнение кода (Command Execution)

- Переполнение буфера (Buffer Overflow)

эксплуатация переполнения буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы

- Атака на функции форматирования строк (Format String Attack)

при использовании этих атак путь исполнения программы модифицируется методои перезаписи областей памяти с помощью функций форматирования символьных переменных

- Выполнение команд ОС (OS Commanding)

атаки этого класса направлены на выполнение команд операционной системы на Web-сервере путем манипуляции входными данными

- Внедрение операторов SQL (SQL Injection)

эти атаки направлены на Web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем

- Внедрение серверных сценариев (SSI Injection)

атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на Web-сервере

Разглашение информации (Information Disclosure)

- Индексирование директорий (Directory Indexing)

атаки данного класса позволяют атакующему получить информацию о наличии файлов в Web каталоге, которые недоступны при обычной навигации по Web сайту

- Идентификация приложений (Web Server/Application Fingerprinting)

определение версий приложений используется злоумышленником для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах

- Утечка информации (Information Leakage)

эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы

- Обратный путь в директориях (Path Traversal)

данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера.

- Предсказуемое расположение ресурсов (Predictable Resource Location)

позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностям

Логические атаки (Logical Attacks)

- Злоупотребление функциональными возможностями (Abuse of Functionality)

данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничение доступа

- Отказ в обслуживании (Denial of Service)

данный класс атак направлен на нарушение доступности Web-сервера

- Недостаточное противодействие автоматизации (Insufficient Anti-automation)

эти уязвимости возникаеют, в случае, если сервер позволяет автоматически выполнять операции, которые должны проводиться вручную

- Недостаточная проверка процесса (Insufficient Process Validation)

уязвимости этого класса возникают, когда сервер недостаточно проверяет последовательность выполнения операций приложения

SQL-инъекции

SQL-injection (инъекция, инжект) — рзновидность уязвимости, позволяющая подменить и дополнить оригинальный sql-запрос своими данными, что может привести к выводу любой информации, или, что хуже — полному доступу к серверу.

Пример уязвимого кода:

```
...
$id=$_GET['id'];
$query="SELECT * FROM articles WHERE id='".$id."';
$ret=mysql_query($query);
...
```

Красным и выделена уязвимая строчка. Если злоумышленник гетом передаст, например, знаечние $id = 13', то кавычка вставится в запрос, что приведет к ошибке и позволит вывести любые данные из базы данных. (Способы рассматривать не буду из определенных побуждений).

Также при некотоырх обстоятельствах у злоумышленника есть возможность аже выполнять php код, что может привести к очень трагичным последствиям.

Способы устранения уязвимости:

1) Самое-самое главное — фильтровать кавычки. Везде — в $_GET, $_POST и даже $_COOKIES Например, заменять "'" на "\'"

2) Не использоать в запросе такие конструкции: ...where id = $id..., но использовать ...where id = '$id' с отфильтрованными заранее кавычками.

XSS-атаки

XSS означает Cross Site Scripting (межсайтовый скриптинг). Так как аббревиатура CSS занята под Каскадные Таблицы Стилей, то используют аббревиатуру именно XSS, а не CSS. Эта уязвимость позволяет выполнять вредоносный JavaScript код «без спроса» пользователя путем вставки его в html код сайта.

XSS делятся на пассивные и активные.

- Активные XSS — вредоносный код сохраняется в базе\файле и напрямую выводится на уязвимой сайте в браузере. Например, в заголовках сообщений, теле постов и т.д.
- Пассивные XSS — вредоносный код передается GET\POST параметром и выводится на страницу, сохранение на сервер не происходит.

Например:

site.ru/page.php?var=

Если переменная var никак не фильтруется и напрямую выводится на страницу, то при заходе по данной ссылке пользователь увидит всплывающее сообщение. Или же злоумышленник получит его cookies, составив определенный запрос.

Все XSS-уязвимости позволяют сформировать определенную ссылку, подбросить администратору\пользователю сайта и заполучить себе его cookies. Такие уязвимости были даже на многих крупных сайтах — таких, как Вконтакте.

Способы устранения: делать htmlspecialchars полей, где это необходимо, жестоко фильтровать все html теги.

Что делать…

- Никому не доверять
- Не полагаться на сокрытие (чтоб никто не догадался)
- Знать что вместо человека может прийти робот
- Не публиковать служебную информацию
- Не использовать устаревшие инструменты
- Никому не доверять