Skillbox

Security

Виды информационных угроз
OWASP TOP 10

Чернухин Максим
Software Architect АО Альфа-Банк

В прошлом модуле

- Познакомились с автоматическим добавлением и удалением сервисов в системе
- Узнали о способах конфигурации для большего числа сервисов

В этом модуле

- Узнаем о векторах атак
- Познакомимся с OWASP TOP 10
- Разберёмся с шифрованием данных
- Поговорим про аутентификацию и авторизацию

Skillbox

На этом уроке мы

- Узнаем виды информационных угроз
- Познакомимся с OWASP TOP 10

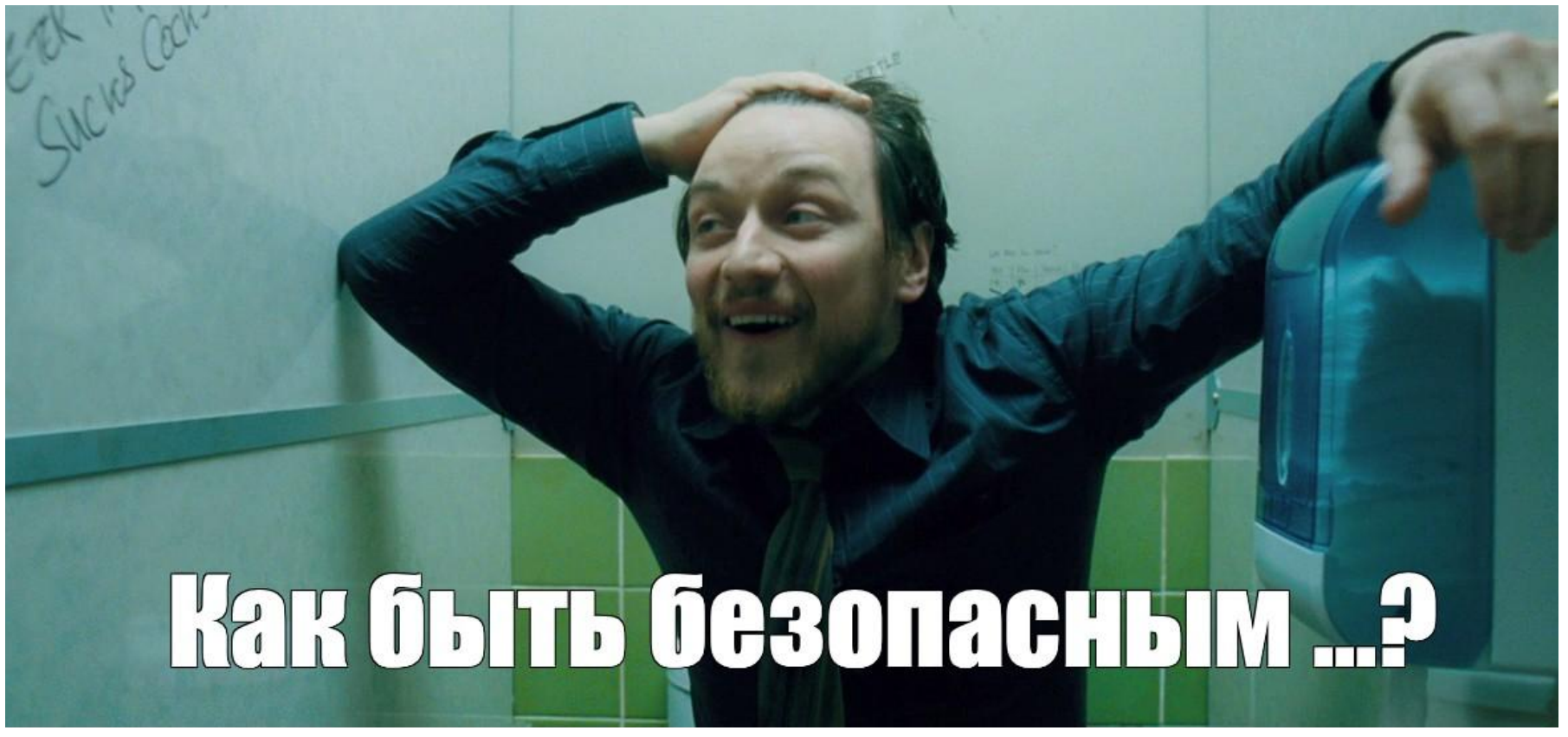
Виды информационных угроз

- Преднамеренные
  - Физическое воздействие
  - Социальный инжиниринг
  - Хищение информации
  - Malware, вирусы и т. д.
- Случайные
  - Ошибки пользователей
  - Ошибки разработки, администрирования
  - Отказ аппаратуры, сети, ЦОДов
  - Форс-мажоры

Виды информационных угроз

- Преднамеренные
  - Физическое воздействие
  - Социальный инжиниринг
  - Хищение информации
  - Malware, вирусы и т. д.
- Случайные
  - Ошибки пользователей
  - Ошибки разработки, администрирования
  - Отказ аппаратуры, сети, ЦОДов
  - Форс-мажоры

С чего же начать?



Skillbox

OWASP TOP 10

- OWASP — Open Web Application Security Project
- Обновление раз в 3–4 года
- Последнее обновление в 2017 г.
- Уже есть предварительный вариант OWASP 2021

Skillbox

OWASP TOP 10 2021

Draft

- Инъекции
- Недостатки аутентификации
- Межсайтовый скриптинг (XSS)
- Незащищённость конфиденциальных данных
- Небезопасная десериализация, внешние сущности XML

Skillbox

OWASP TOP 10 2021

Draft

- Нарушение контроля доступа
- Неэффективный мониторинг
- Подделка запросов со стороны сервера (SSRF)
- Использование компонентов с известными уязвимостями
- Некорректная настройка параметров безопасности

Injections

Инъекции

- https://example.com/?param=123 **AND 1=2--**
- https://example.com/?param=123 **AND 1'/***
- https://example.com/?param=123' **AND '1'='1**

Skillbox

Injections

Инъекции

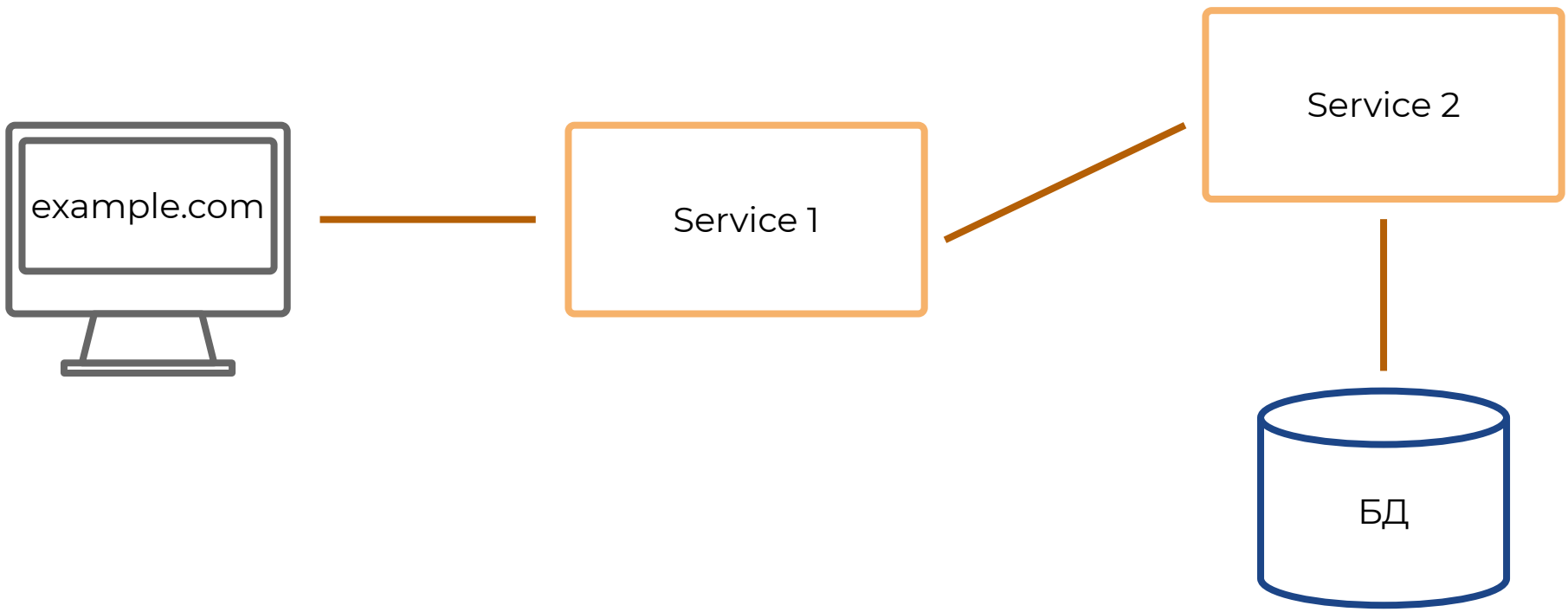
Информация

- **Аутентификация** — процедура проверки подлинности, например, проверка подлинности пользователя с помощью логина и пароля
- **Авторизация** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий

Skillbox

Broken Authentication

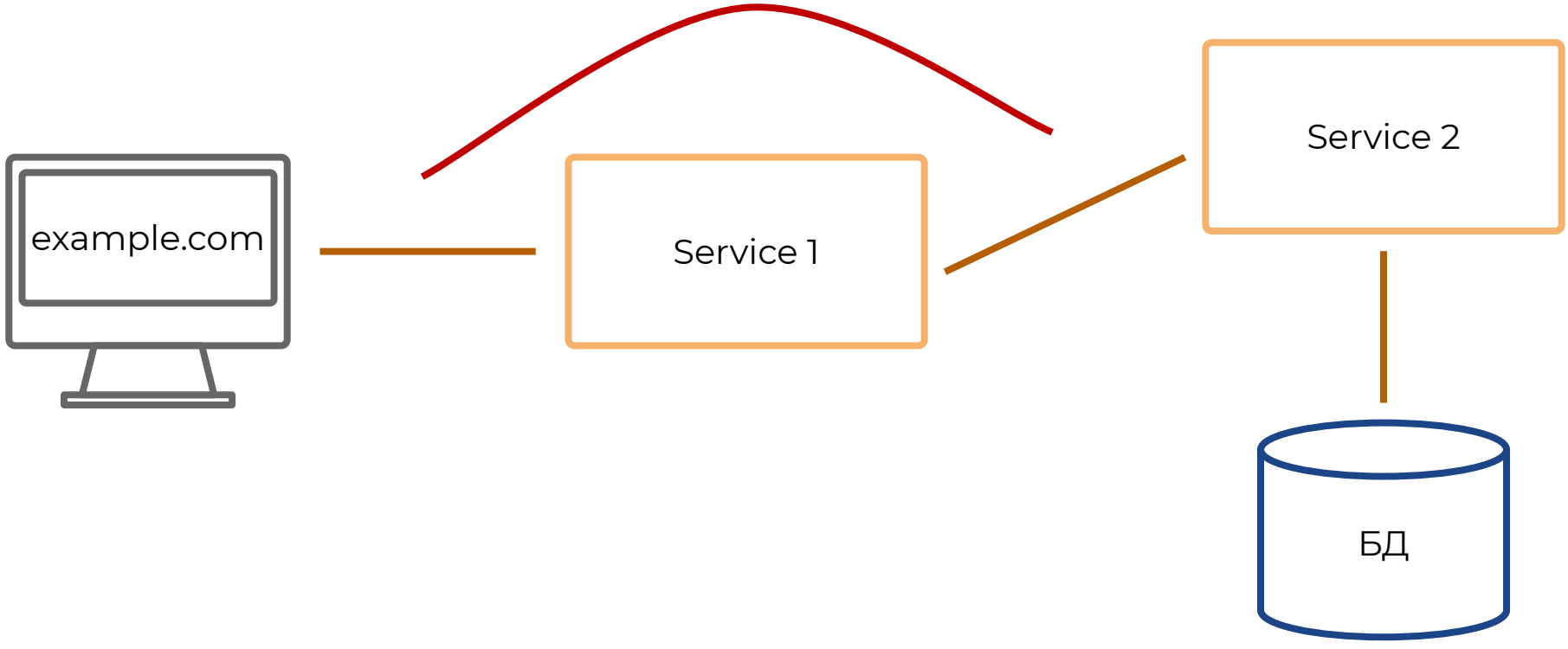
Нарушенная аутентификация



Skillbox

Broken Authentication

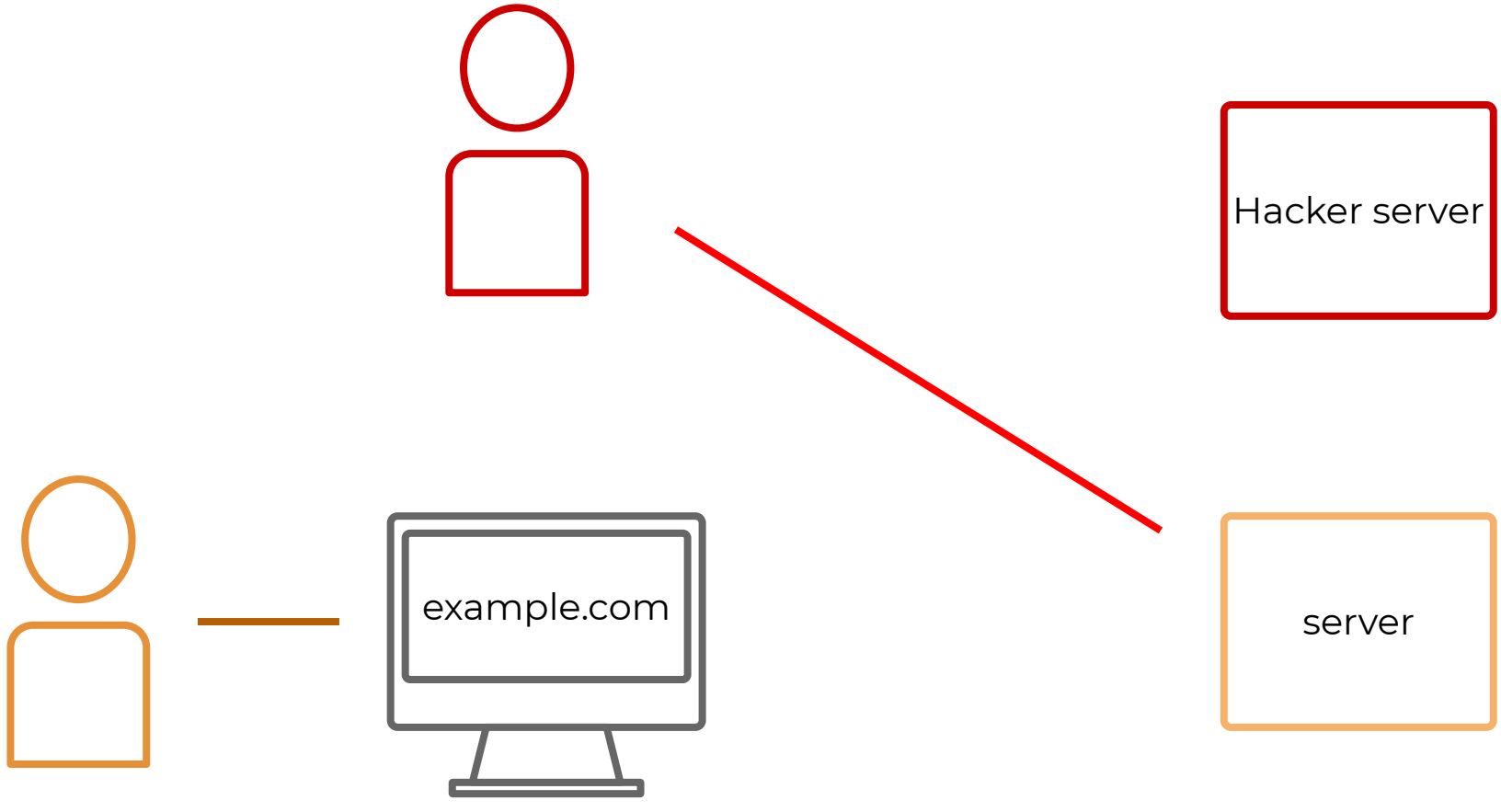
Нарушенная аутентификация



Skillbox

Cross-Site Scripting (XSS)

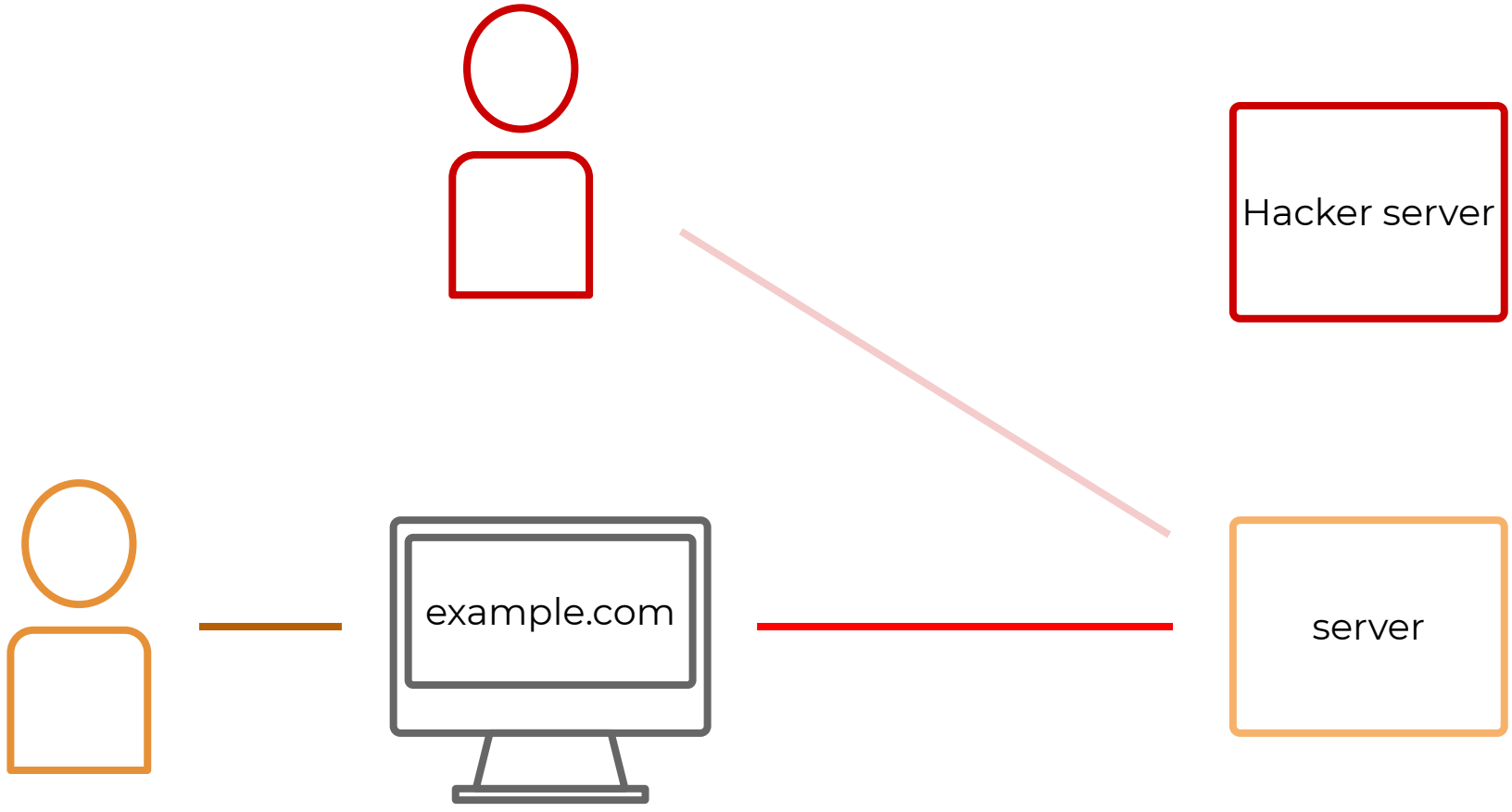
Межсайтовый скриптинг



Skillbox

Cross-Site Scripting (XSS)

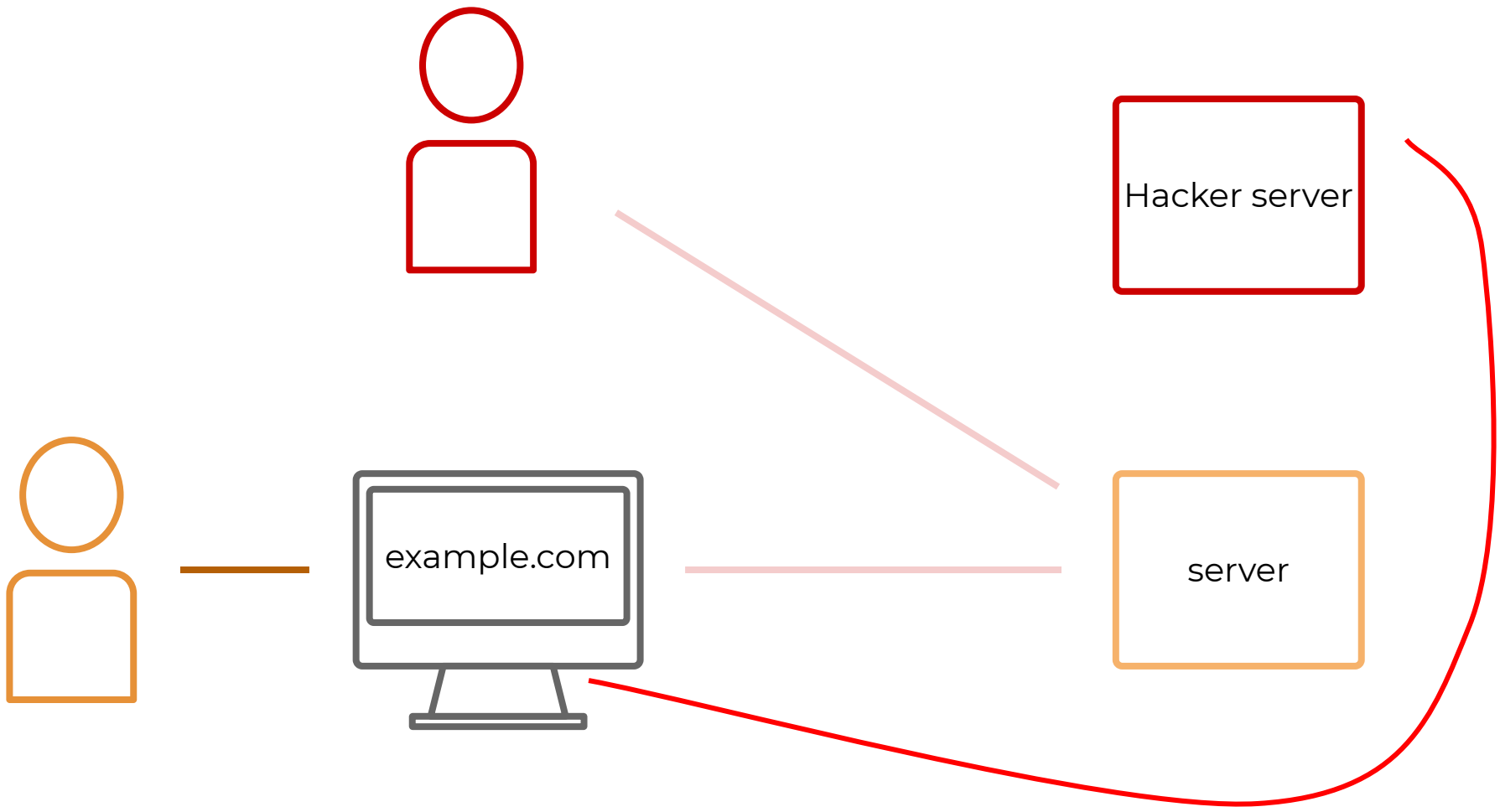
Межсайтовый скриптинг



Skillbox

Cross-Site Scripting (XSS)

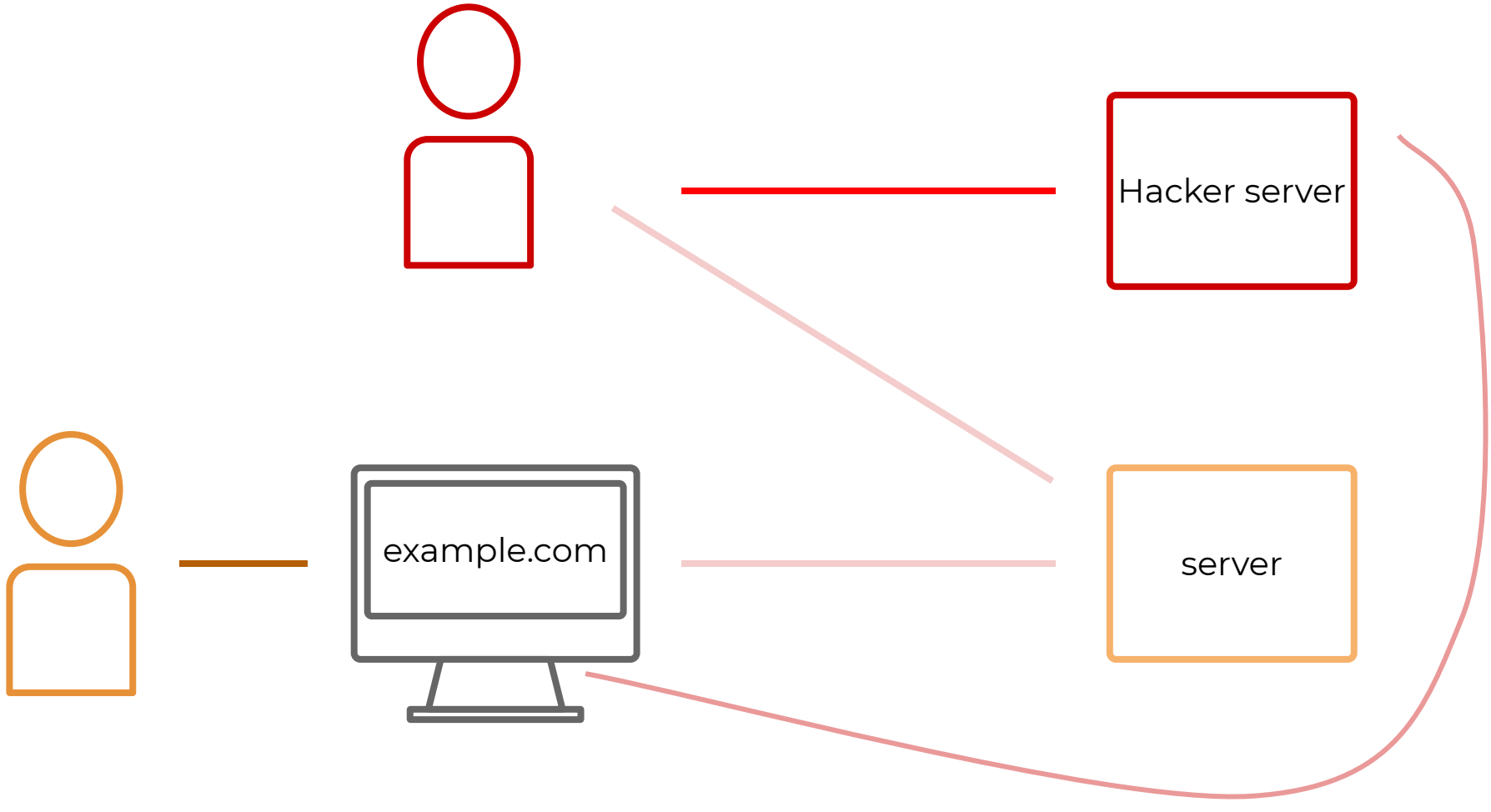
Межсайтовый скриптинг



Skillbox

Cross-Site Scripting (XSS)

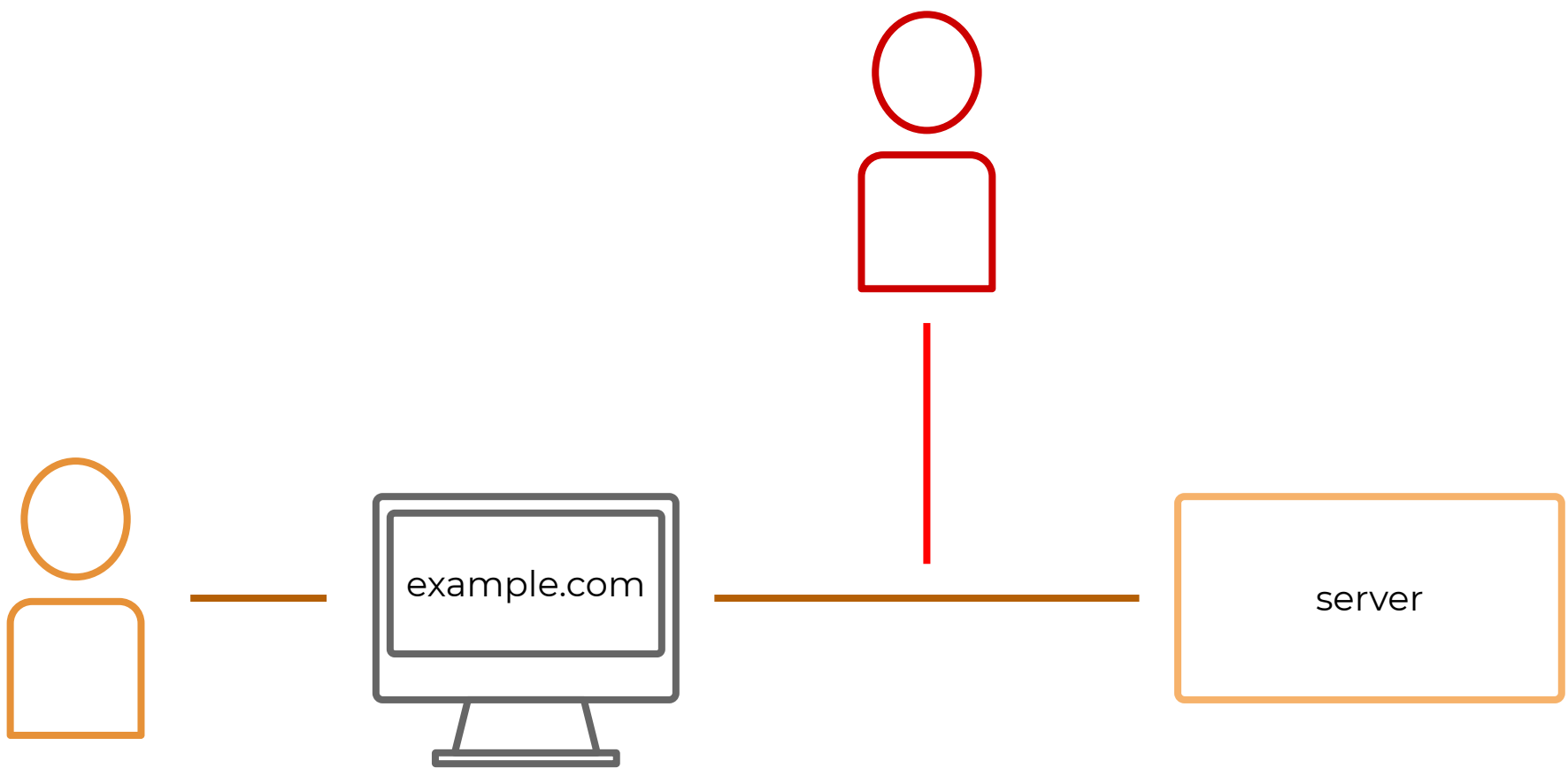
Межсайтовый скриптинг



Skillbox

Sensitive Data Exposure

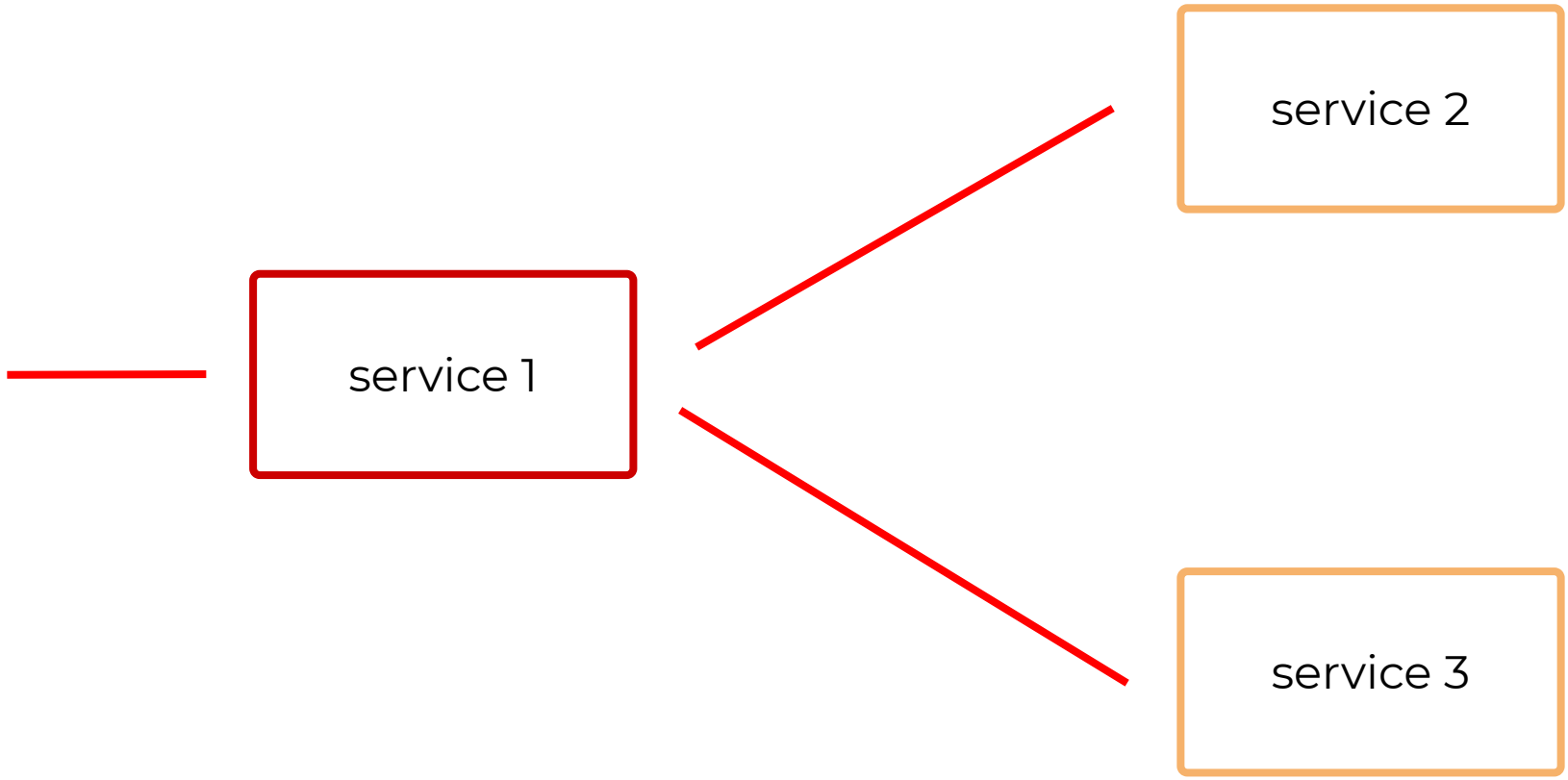
Незащищённость конфиденциальных данных



Skillbox

XML External Entities (XXE), Insecure Deserialization

Внешние сущности XML, Небезопасная десериализация



Skillbox

XML External Entities (XXE), Insecure Deserialization

Внешние сущности XML, небезопасная десериализация

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<foo>&xxe;</foo>

<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
<foo>&xxe;</foo>
```

Skillbox

XML External Entities (XXE), Insecure Deserialization

Внешние сущности XML, небезопасная десериализация

- Включать только необходимую функциональность библиотек для парсинга и десериализации
- Настроить один раз и использовать везде
- Использовать простые объекты JSON
- **DMZ** (англ. «Demilitarized Zone» — демилитаризованная зона, ДМЗ)

Skillbox

Broken Access Control

Нарушение контроля доступа

- Возможность прочитать файлы по FTP, SFTP, SSH
- Доступ к данным другого пользователя БД
- Доступ к системным приложениям
- Доступ к административным панелям
- Доступ к панелям управления хостинга и др.

Skillbox

Insufficient Logging and Monitoring

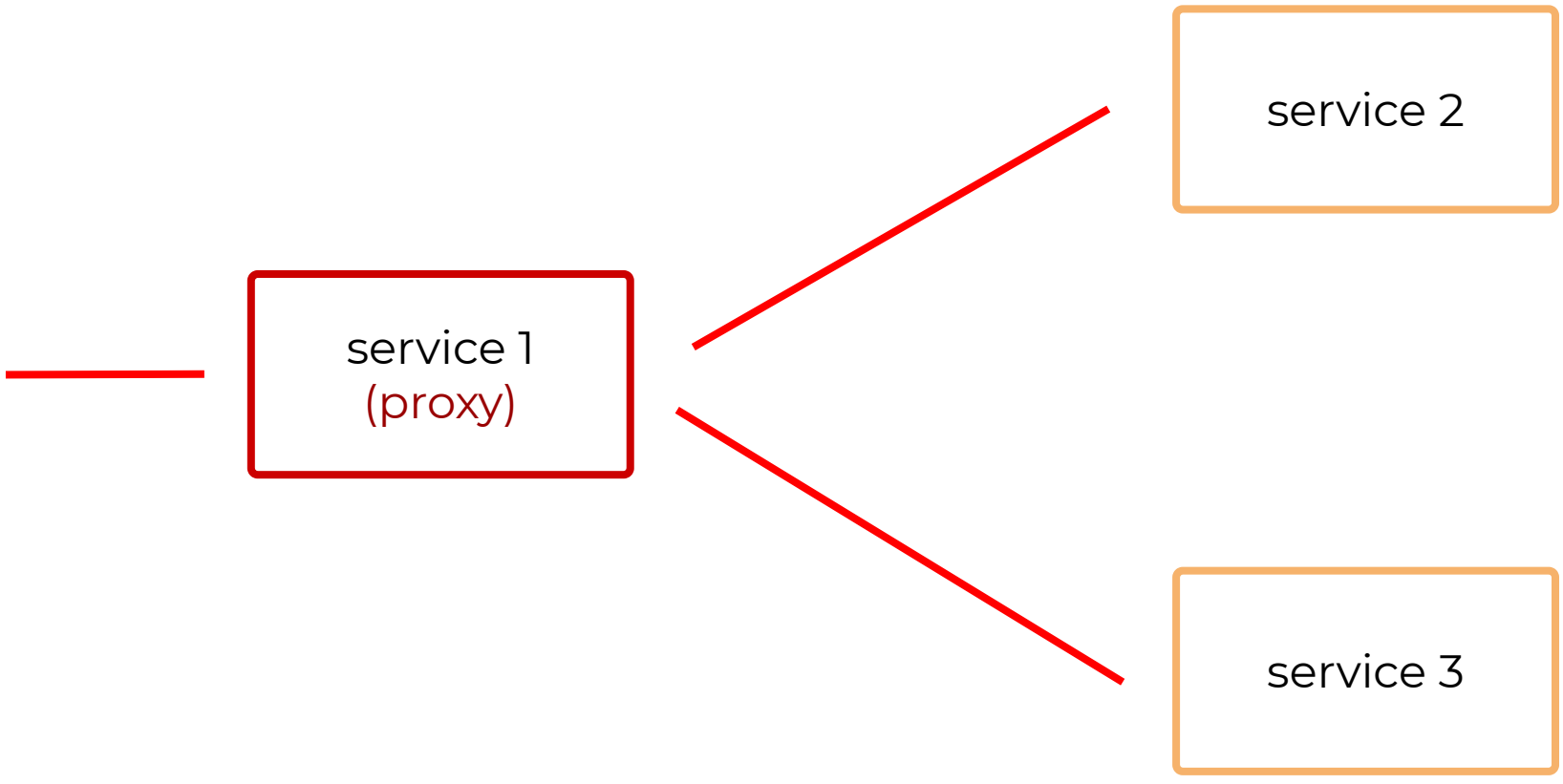
Неэффективный мониторинг

- Отсутствие аудита
- Отсутствие фиксации действий пользователей
- Отсутствие мониторинга показателей
- Отсутствие уведомлений при достижении пороговых значений

Skillbox

Server-Side Request Forgery SSRF

Подделка запросов со стороны сервера



Skillbox

Using Components with known vulnerabilities

Использование компонентов с известными уязвимостями

- Применение неиспользуемых зависимостей
- Устаревшие версии библиотек
- Устаревшие версии патчей
- Библиотеки со встроенным зловредным ПО

Skillbox

Using Components with known vulnerabilities

Некорректная настройка параметров безопасности

- Неисправленные недостатки
- Конфигурации по умолчанию
- Наличие неиспользуемых страниц
- Незащищённые файлы и каталоги
- Ненужные службы

Итоги

- Мы узнали, что векторов атак очень много
- Есть OWASP с приоритезацией угроз
- Наиболее эффективно векторы атак работают в комбинации
- «Zero Trust» — никому не доверять

Что дальше?

- Что такое SSL?
- Чем он отличается от TLS?
- Какими способами шифруются данные?

Skillbox

Спасибо за внимание!