Simpler Approach to Threat Modeling (RTMP Step by Step Tutorial)

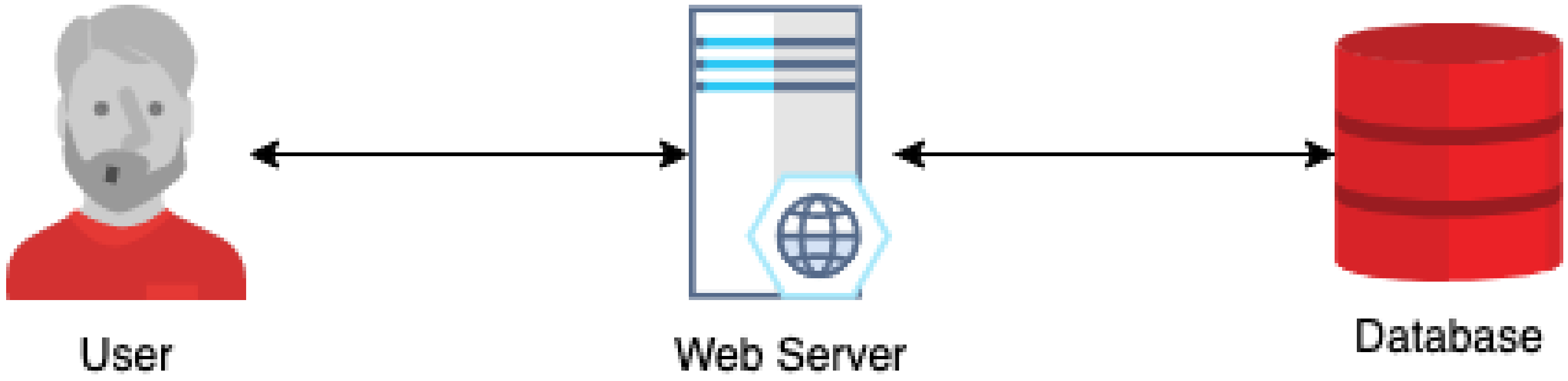
Apr. 23rd, 2025

Adlizan Ibrahim｜Nobu

Rakuten Group, Inc.

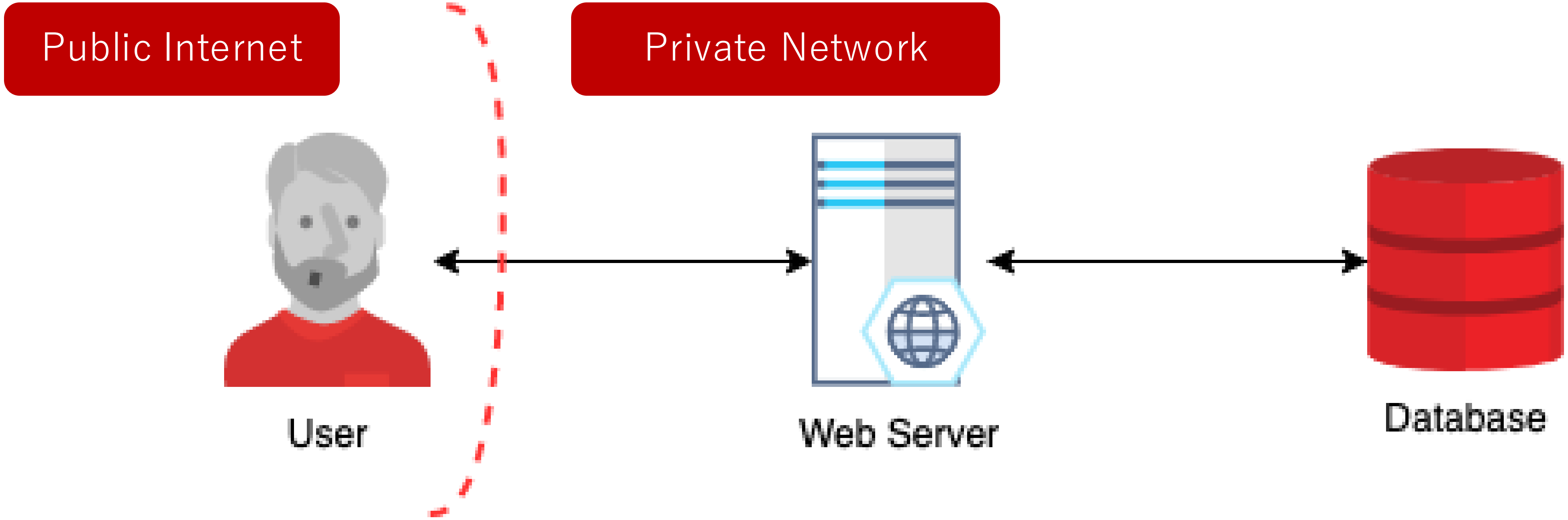
Rakuten

RTMP HowTo: STEP 0 (Preparation)



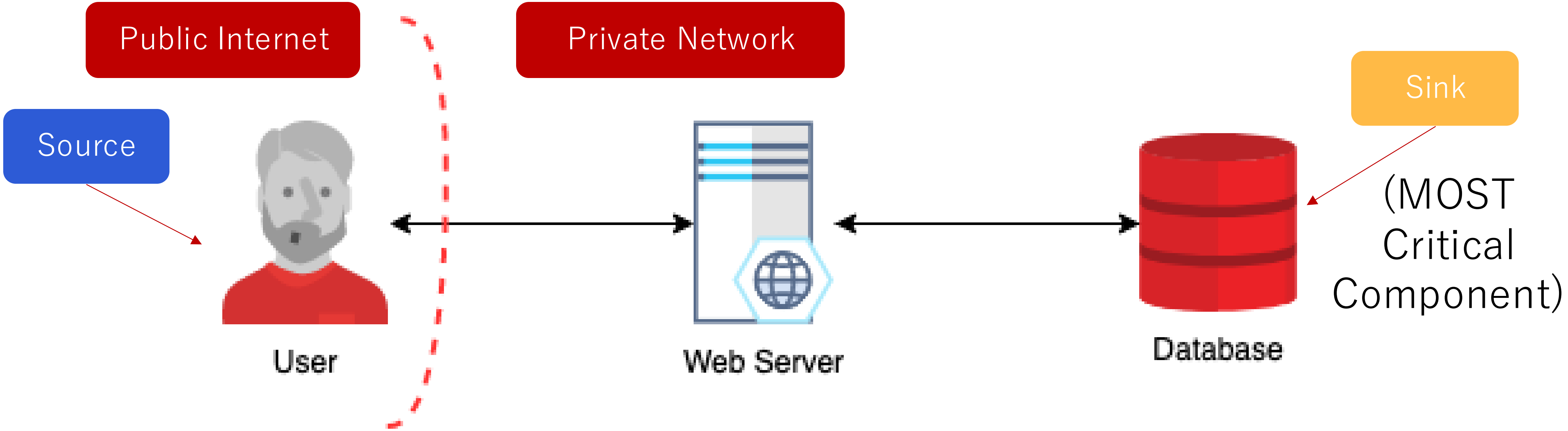
- Use whatever architecture diagram you already have in hand.
- RTMP is intended to start a conversation - to get the ball rolling.
  - To identify baseline requirements based on the STRIDE threats, not complete in-depth.
  - It should be simple and fast ☺

RTMP HowTo: STEP 1 (Mark Your Boundary)



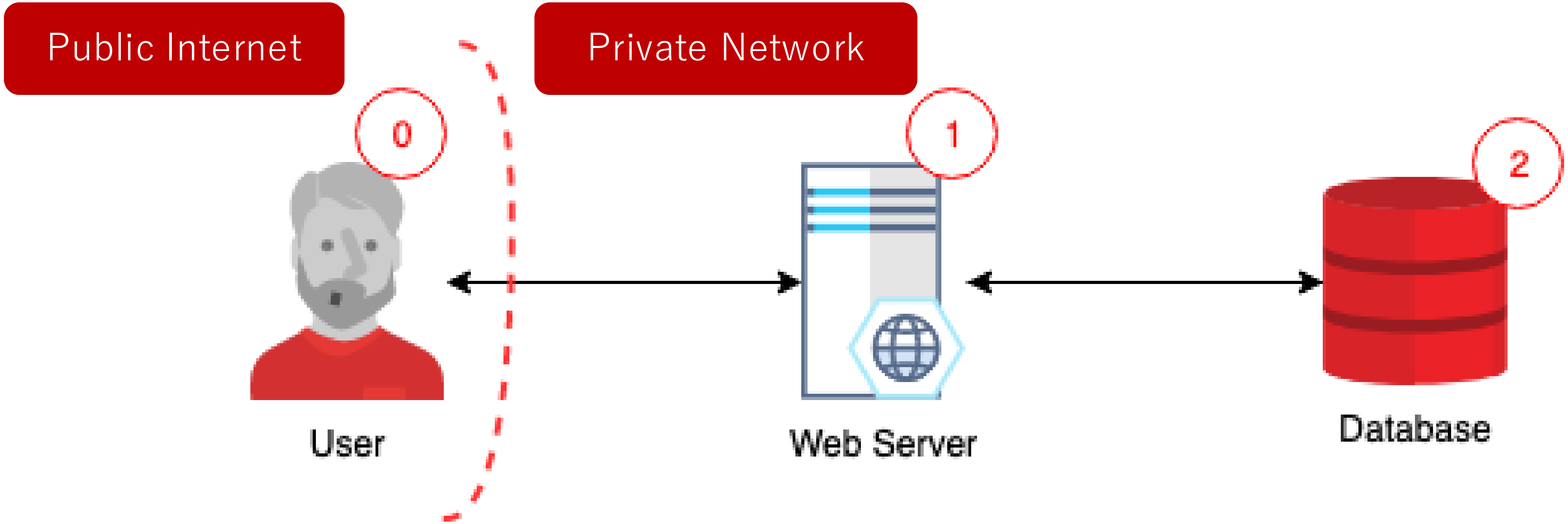
- Define your trust boundaries.
- Represent change of trust level as data flows through your system.
- Trust level defines what kind of security controls you need to implement.
- Also includes integration with external system (what you cannot control, you cannot trust)

RTMP HowTo: STEP 2 (Model Your System)



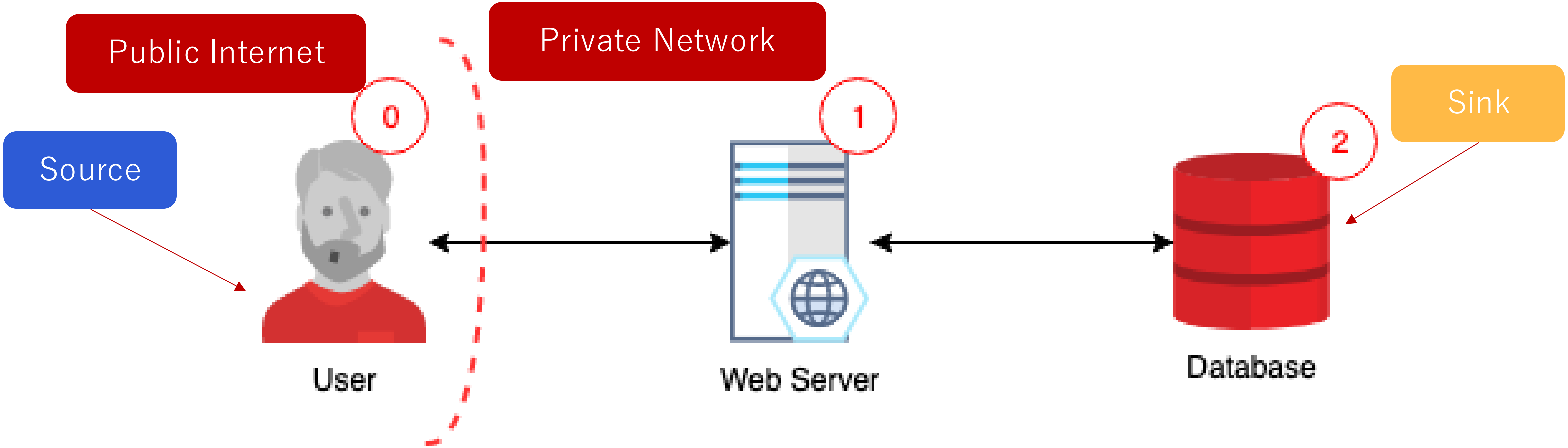
- Define the sources (where flow starts) and sink (where data is stored)
- Example of source e.g human user, admin, external system
- Example of sink e.g database (final data destination)
- [Tips] There should be only one sink for each threat model.

RTMP HowTo: STEP 3 (Assign Zone of Trust)



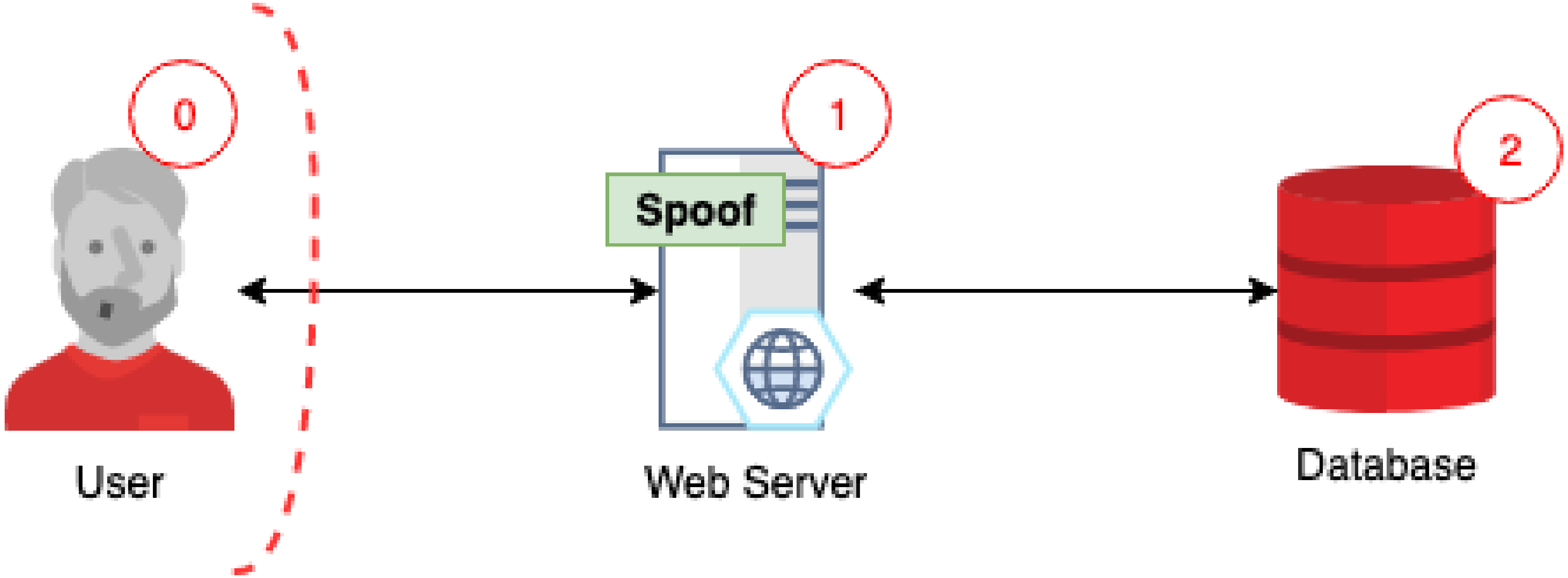
- Zone 0 = anything NOT under your control e.g user, admin, other internal system
- Zone 1 = any component that receive data directly from Zone 0.
- Zone > 1 = different logical zone, based on higher level of criticality.
- [Tips!] Sink e.g database should be assigned with the highest zone.

RTMP HowTo: STEP 4 (Finding Threats)



- RTMP methodology already defines specific rules to identify threats based on the STRIDE framework.
- From this point, follow the predefined rules based on the simple zone math.

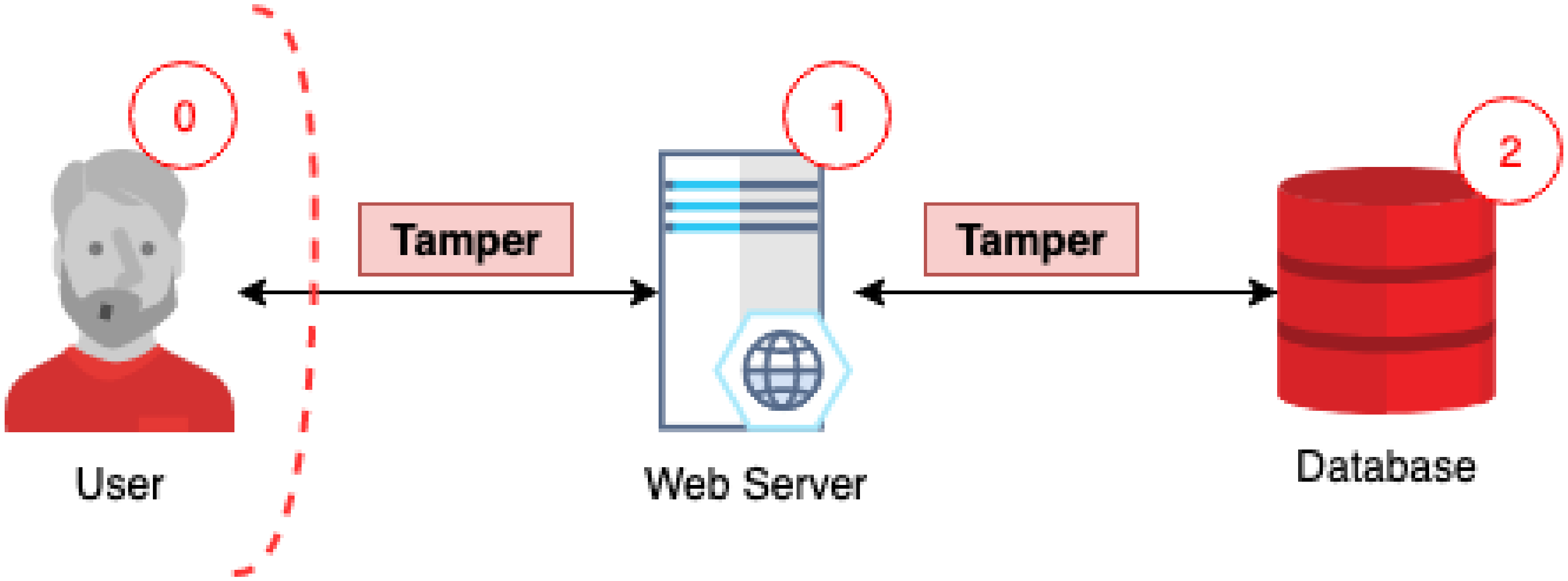
RTMP HowTo: STEP 4.2 Finding Threats (Spoofing threats)



- Spoofing Rule:
    - Place these on the destination component where its Zone of Origin is Zone 0.

S →

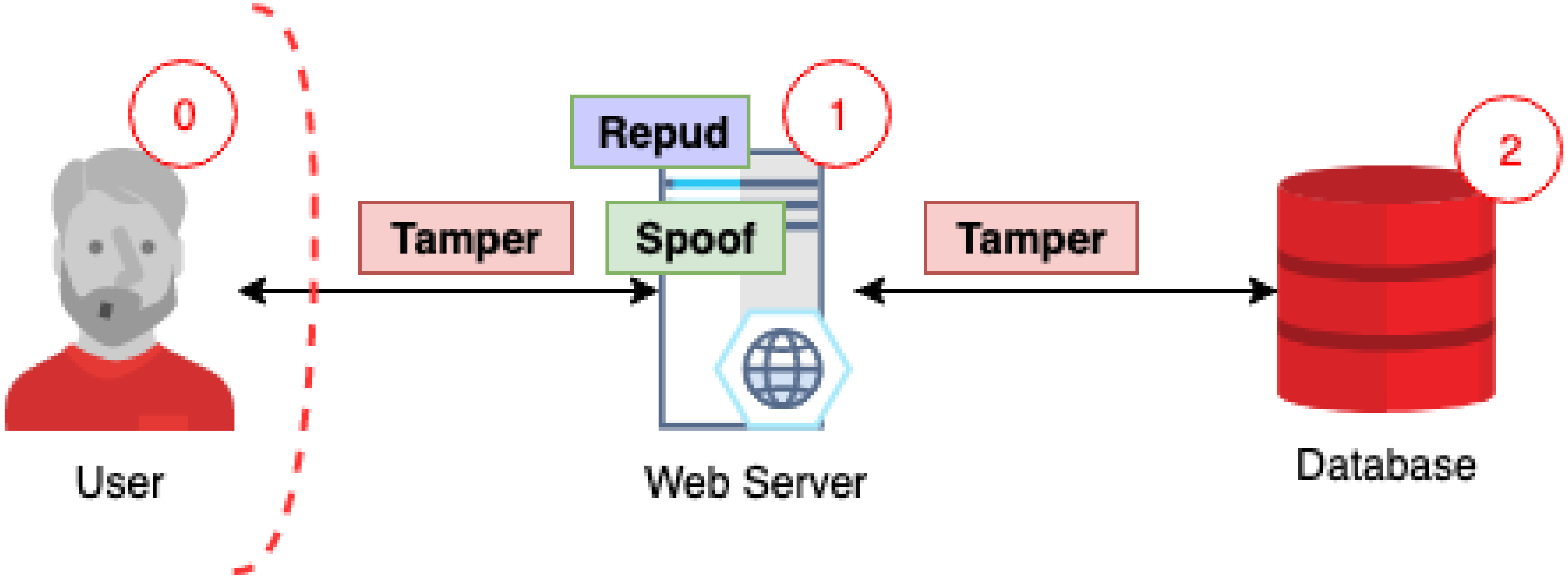
RTMP HowTo: STEP 4.3 Finding Threats (Tampering threats)



- Tampering Rule:
  - Place these on connecting flows where the Zone of Destination is higher than the Zone of Origin
  - Example: Zone 0 → Zone 1 | Zone 1 → Zone 2 | Zone 0 → Zone 3

S → T →

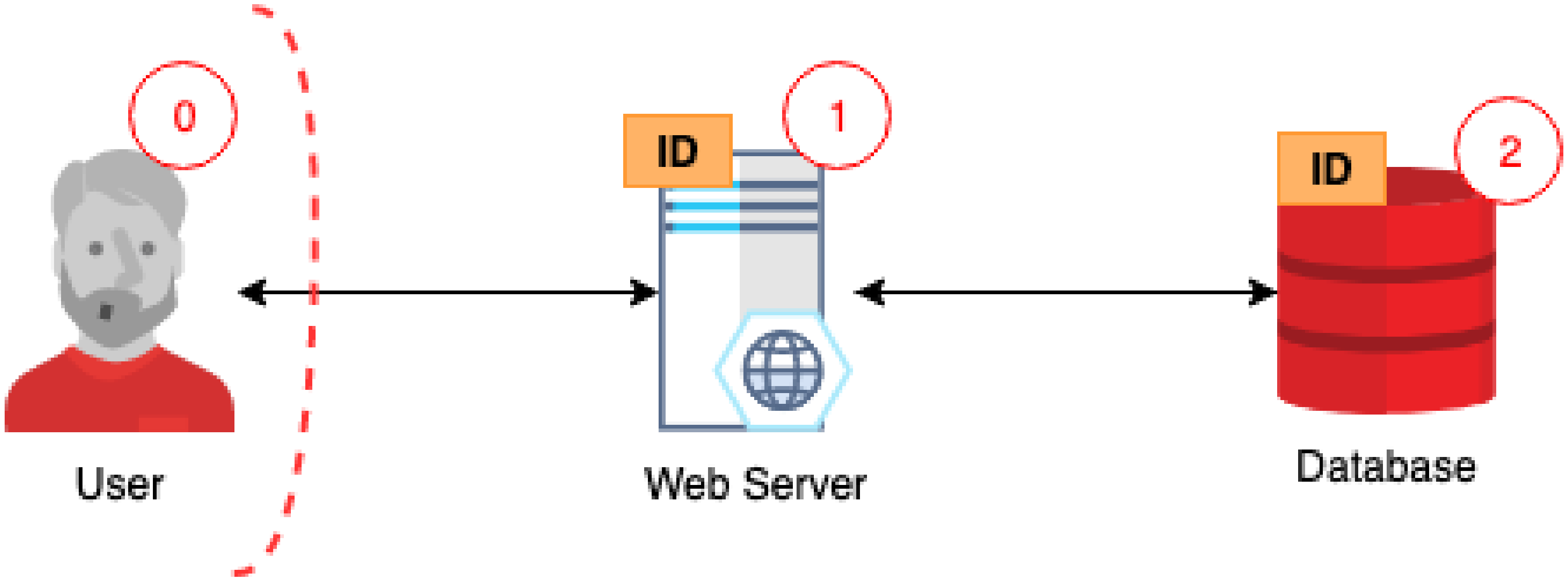
RTMP HowTo: STEP 4.4 Finding Threats (Repudiation threats)



- Repudiation Rule:
  - Place these on the destination component where there is Tampering on the connecting flow and Spoofing on the component.

S → T → R →

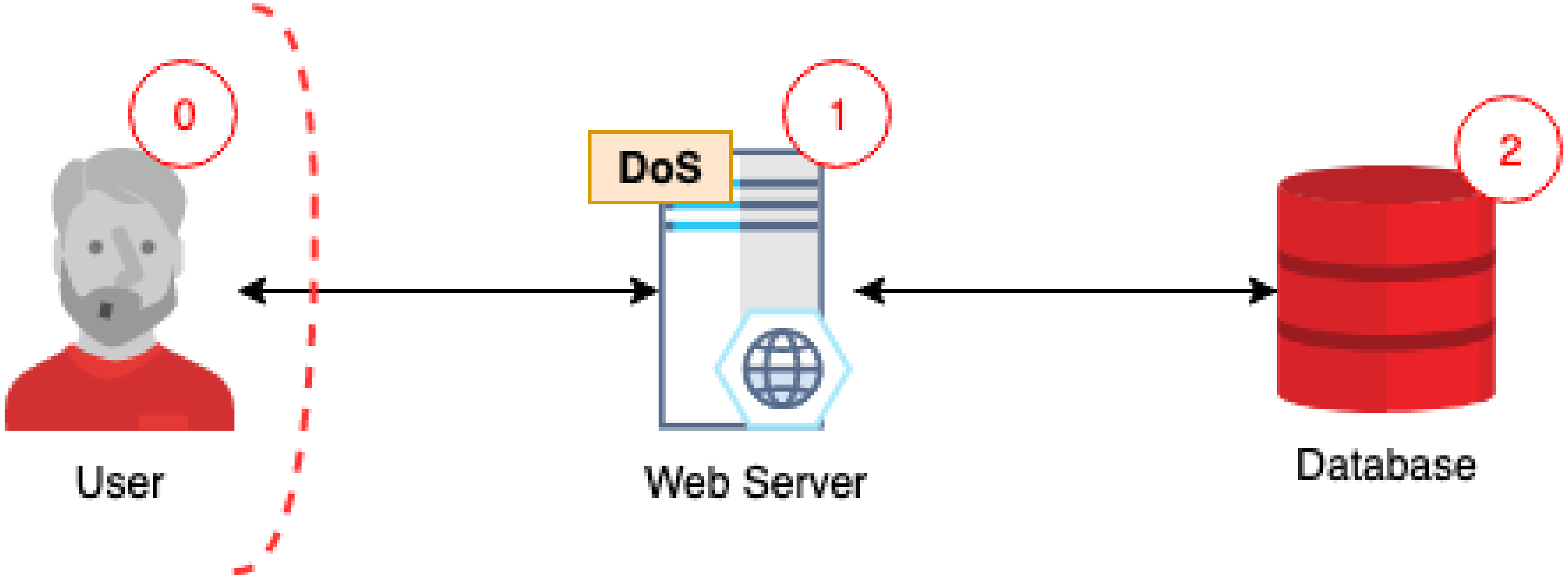
RTMP HowTo: STEP 4.5 Finding Threats (Info Disclosure threats)



- Info Disclosure Rule:
  - Place these on origin (NOT ~~destination~~) component where Zone of Destination is lower than Zone of Origin.
  - Example: Zone 2 → Zone 1 | Zone 3 → Zone 2 | Zone 1 → Zone 0

S → T → R → I →

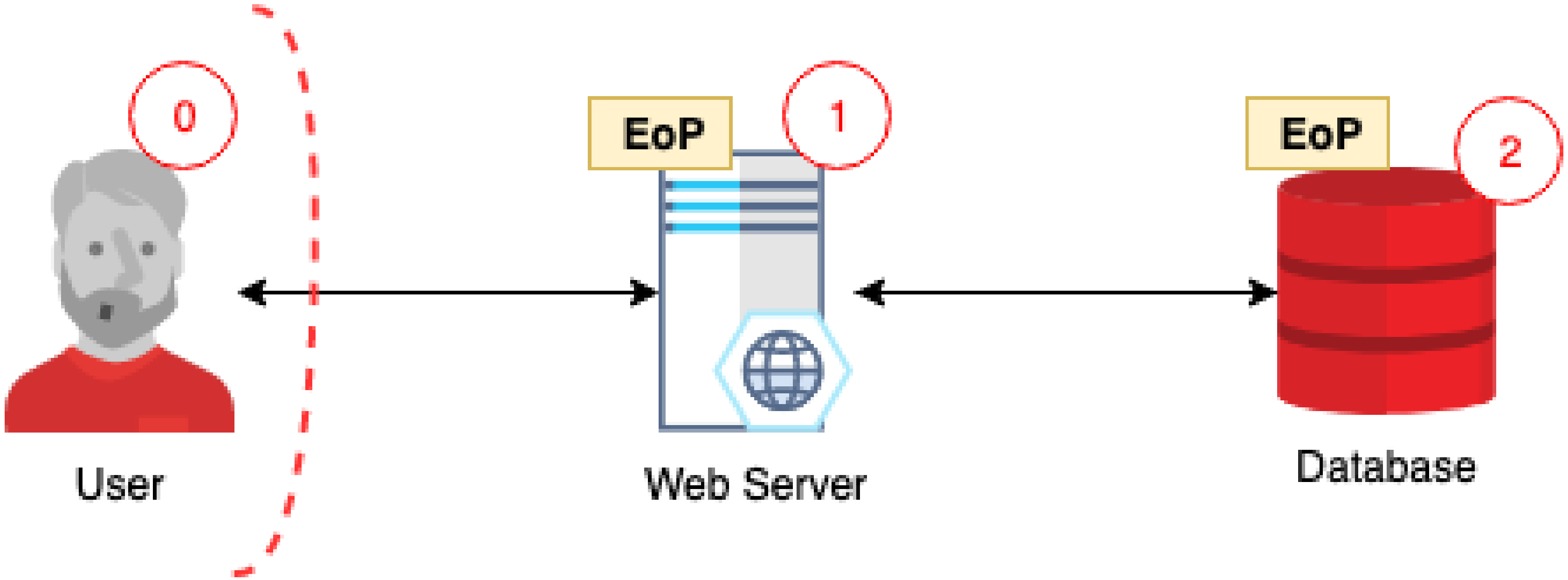
RTMP HowTo: STEP 4.6 Finding Threats (DoS threats)



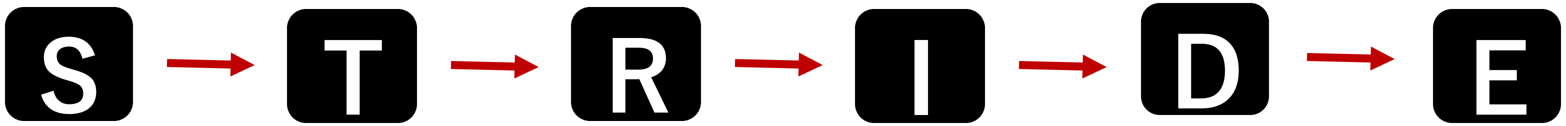
- Denial of Service, DoS Rule:
  - Place these on the destination component where its Zone of Origin is Zone 0.

S → T → R → I → D

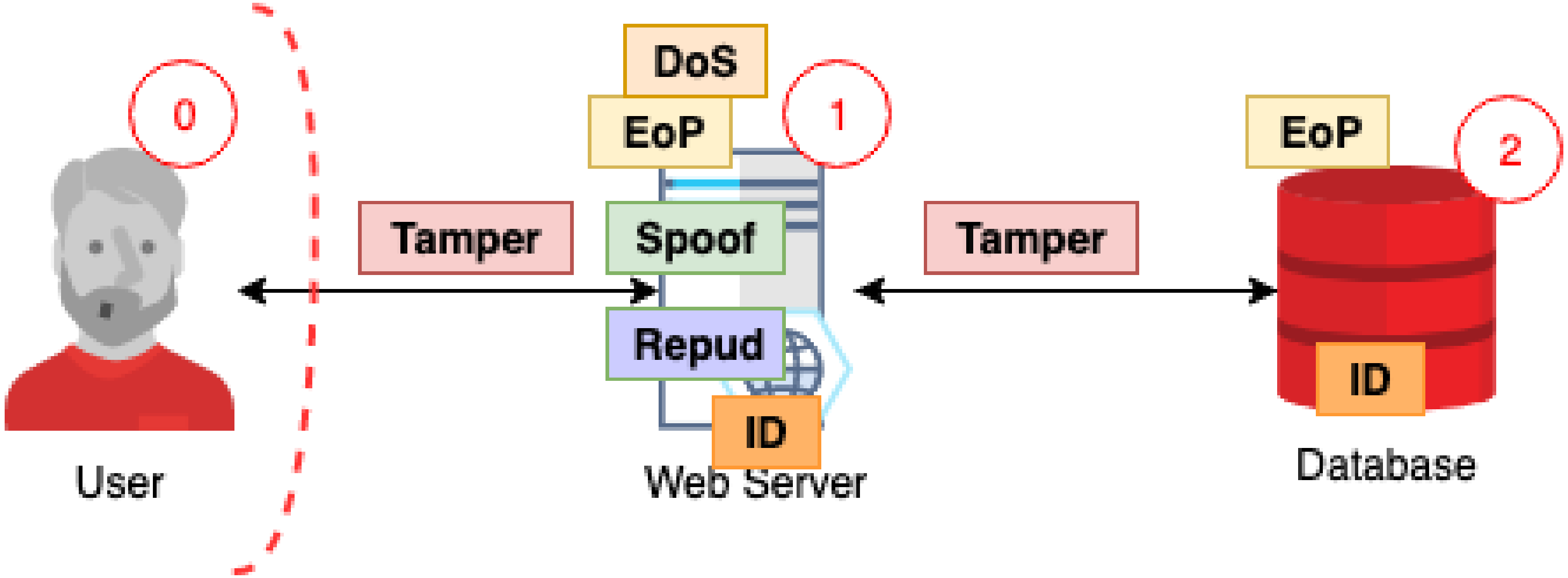
RTMP HowTo: STEP 4.1 Finding Threats (EoP threats)



- Elevation of Privileges, EoP Rule:
  - Place these on the destination component where the Zone of Destination is higher than the Zone of Origin.
  - Example: Zone 0 → Zone 1 | Zone 1 → Zone 2 | Zone 0 → Zone 3



RTMP HowTo: STEP 5 You’re (Almost) Done!



- By now, your diagram should already have a number of STRIDE threat categories mapped to each component/flows ☺
- The next step is to identify the most suitable security control(s) to mitigate each STRIDE threat.

S → T → R → I → D → E

RTMP HowTo: STEP 6 Finished!

STRIDE threats		Most Common Security Requirements/Controls
S	Spoofing	If possible – MFA, change default credential, enforce strong password, limit failed login attempts.
T	Tampering	Encrypted-in-transit (TLS v.1.2 or higher), input validation.
R	Repudiation	Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious/malicious accounts, ensure high-value transactions have an audit trail with integrity controls.
I	Information Disclosure	Encrypted-at-rest (code level or database level), encrypted-in-transit, strong up-to-date crypto algorithm.
D	Denial of Service	Rate-limit API, proper patch management.
E	Elevation of Priviliges	If not public facing - deny by default (whitelisting), disable directory listing, log access control failure, proper patch management, server hardening.

Rakuten