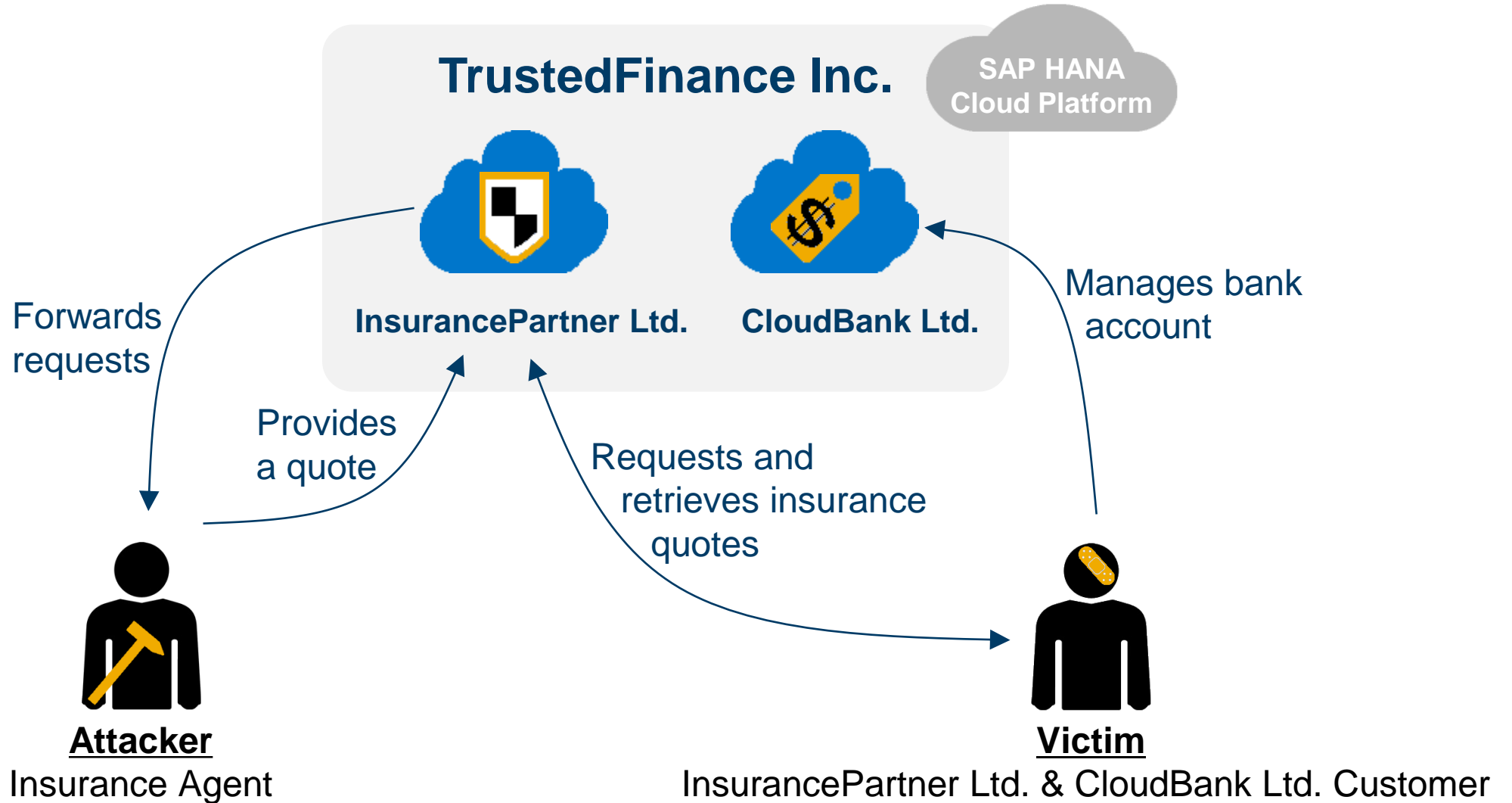


# Week 3 Unit 2: Protecting Against CSRF Attacks

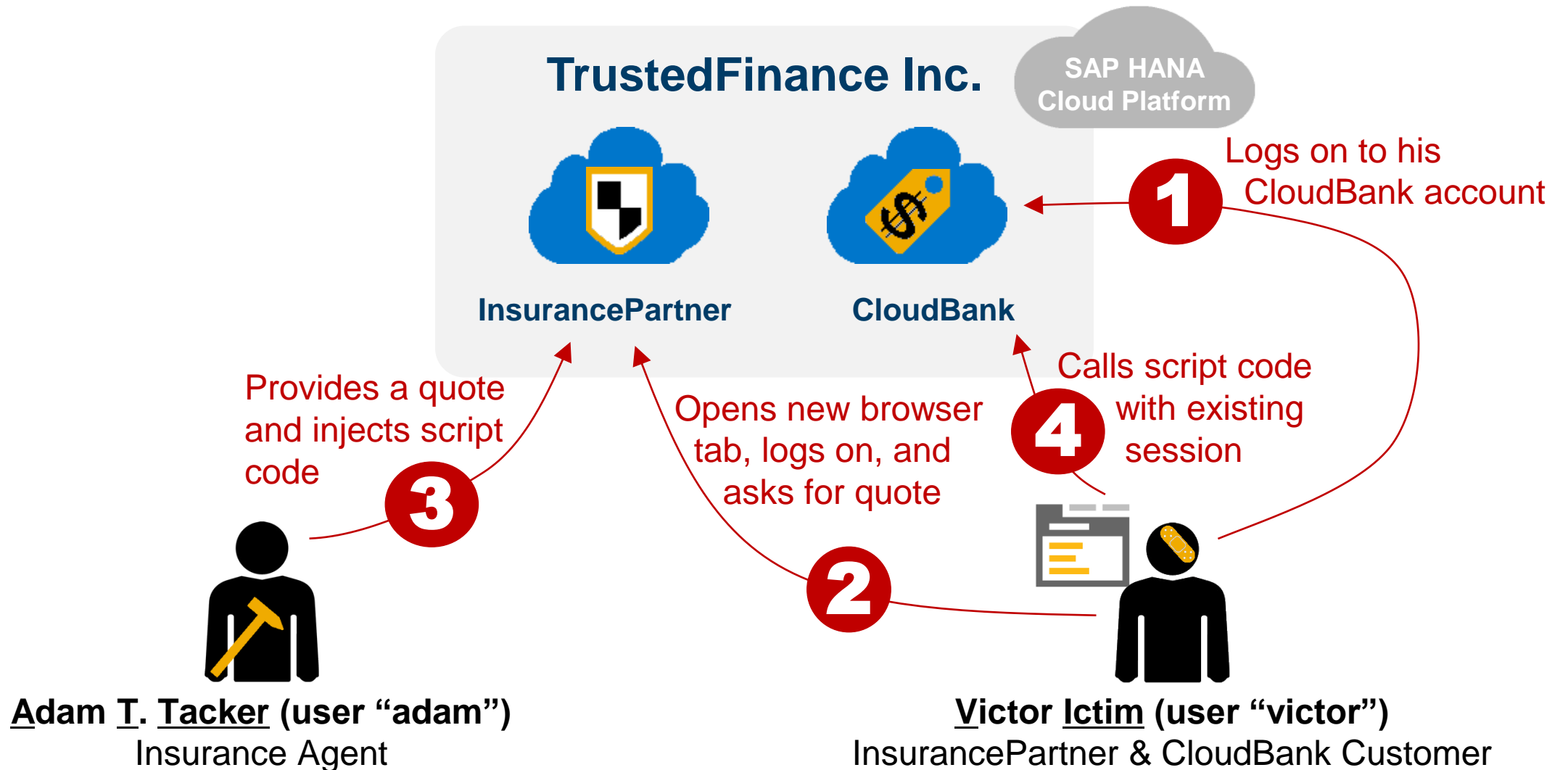
# Protecting Against CSRF Attacks

A business scenario (1/2)



# Protecting Against CSRF Attacks

A business scenario (2/2)



# Protecting Against CSRF Attacks

## Strategies to protect against CSRF attacks

---

- CSRF = cross-site request forgery
- Make your application's URLs unpredictable!
- Use randomly generated tokens with each request that are associated with the user's current session
- Use a CSRF filter provided by the HCP runtimes
  - Java: `org.apache.catalina.filters.RestCsrfPreventionFilter`
  - SAP HANA XS: `prevent_xsrf` keyword in `.xsaccess` file
  - HTML5: CSRF must be taken care of by the consumed (REST) services



# Protecting Against CSRF Attacks

## What you've learned in this unit

---

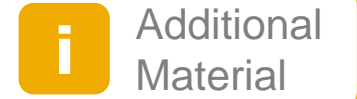
- CSRF is (still) a serious Web attack.
- Protection against it is YOUR responsibility.
- HCP offers a protection mechanism based on a token (a nonce value) generated on each request and stored in the session.



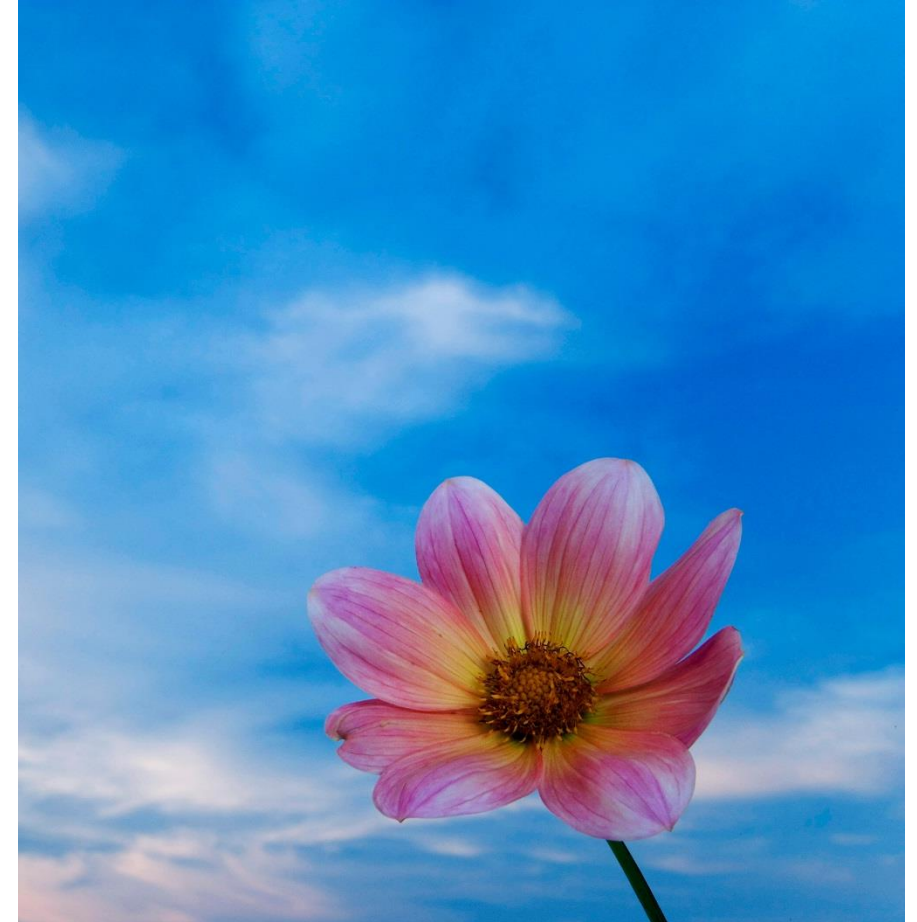


# Protecting Against CSRF Attacks

## Further reading



- Using the Apache Tomcat CSRF Prevention Filter:  
<https://help.hana.ondemand.com/help/frameset.htm?e5be9994bb571014b575a785961062db.html>





# Thank you

Contact information:

[open@sap.com](mailto:open@sap.com)

open**SAP**

# © 2016 SAP SE or an SAP affiliate company. All rights reserved.

---

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.