REST API Design, Development & Management

raj@acloudfan.com

@acloudfan

http://ACloudFan.com

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

This deck is part of a online course on Summary of a course that covers the A to Z of RESTful API. More information.

Security

REST API Design, Development & Management

http://www.acloudfan.com

raj@acloudfan.com

Summary of a course that covers the A to Z of RESTful API. More information.

Updated: Dec 27th, 2016

API Security

raj@acloudfan.com
http://www.acloudfan.com

Authentication

Authorization

Functional attacks

raj@acloudfan.com
http://www.acloudfan.com

Basic Authentication, API Key/Secret, JWTs

http://www.acloudfan.com

raj@acloudfan.com

Summary of a course that covers the A to Z of RESTful API. More information.

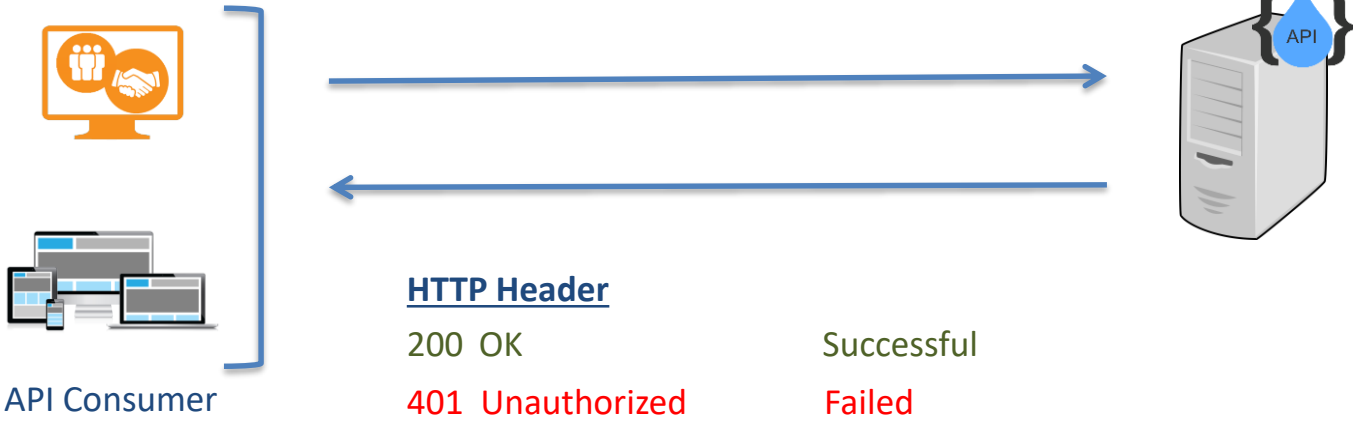
UDEMY Link With Coupon Discount

Basic Authentication

raj@acloudfan.com
http://www.acloudfan.com

- Base64 encoded
- User : Password

HTTP Header
Authorization : **Encoded-Creds**



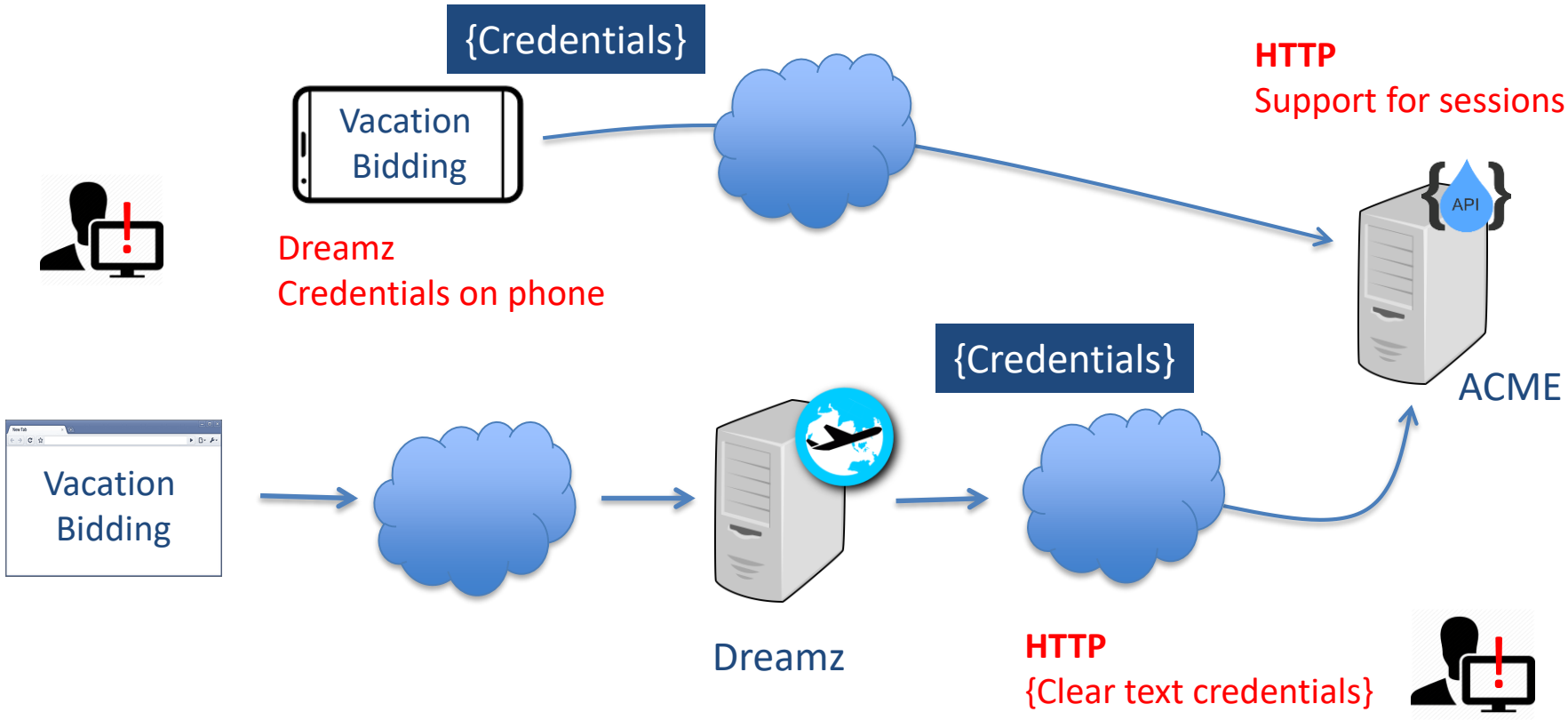
HTTP Header

200 OK	Successful
401 Unauthorized	Failed

NOT a good idea with HTTP – OK with TLS i.e., HTTPs

Basic Authentication Weaknesses

raj@acloudfan.com
http://www.acloudfan.com



Key & Secret

raj@acloudfan.com
http://www.acloudfan.com

- Sending the API Key & Secret/Signature
  - HTTP Header
  - Query parameters
  - Request body

- API key & secret management
- Security scheme
- API key/secret provisioning
- Rate limiting & analytics

API Management Platform

apigee

API Management
IBM

MASHERY

MuleSoft

API Key & Secret

Key Points

raj@acloudfan.com
http://www.acloudfan.com

- **Key** = Long strings of random characters
- API Key/Secret is issued by the API provider
  - Consumer identity
  - Security
  - Rate limiting
- Design considerations related to key/secret management

Tokens?

raj@acloudfan.com
http://www.acloudfan.com

- Encoded string

  Hashing or private key for encryption

- Eliminates the need for sessions on API

  - HTTP Header
  - Query parameters
  - Request body

- Issuer can control the validity

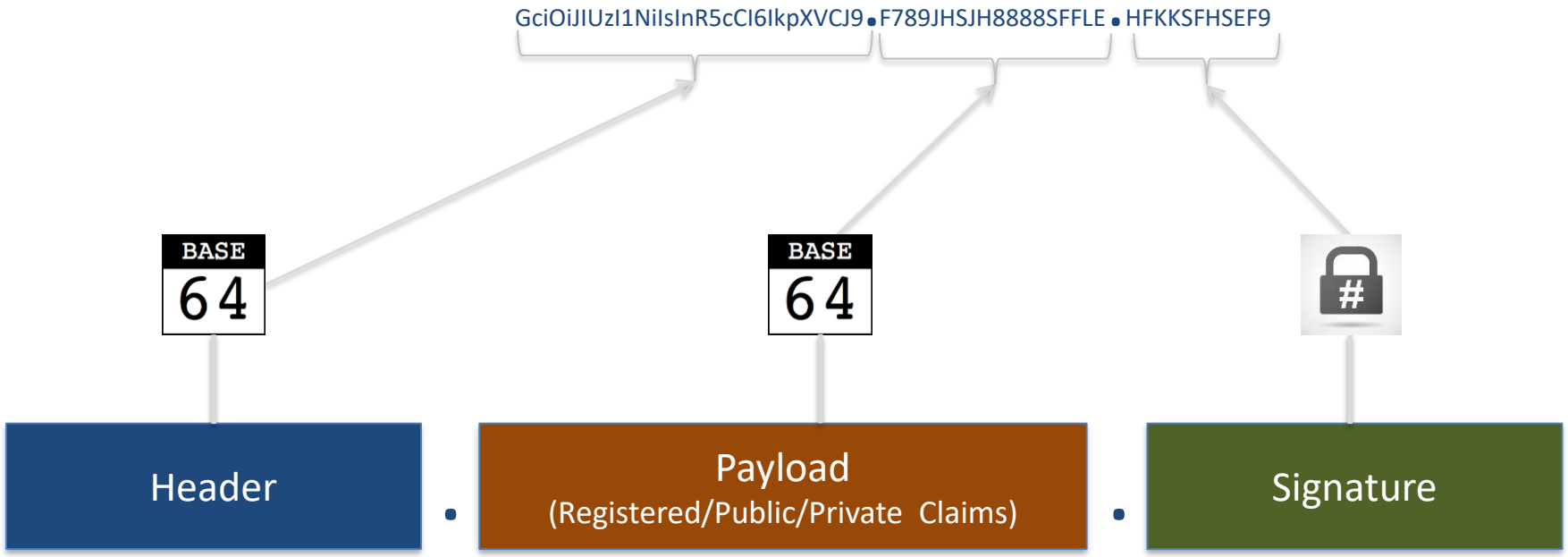
  - Expiry
  - Revocation

facebook twitter LinkedIn

raj@acloudfan.com
http://www.acloudfan.com

JSON Web Tokens

https://tools.ietf.org/html/rfc7519



Self contained | JSON based | Standard RFC 7519

raj@acloudfan.com
http://www.acloudfan.com

Authorization : OAuth2.0

http://www.acloudfan.com

raj@acloudfan.com

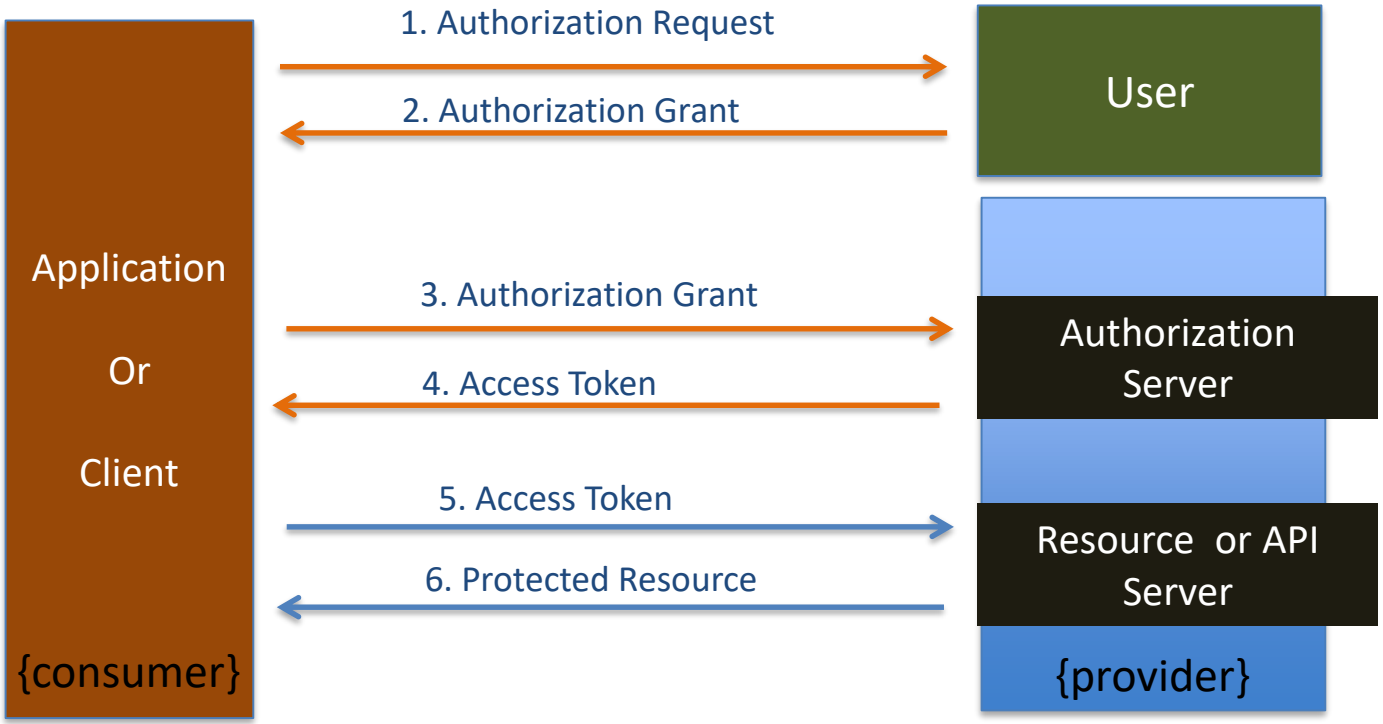
Summary of a course that covers the A to Z of RESTful API. More information.

UDEMY Link With Coupon Discount

Authorization Scope Grant

- Social login scheme

raj@acloudfan.com
http://www.acloudfan.com



OAuth2.0 Grants

raj@acloudfan.com
http://www.acloudfan.com

Authorization Scope Grant

facebook

Google Developers

Implicit Grant

For single page apps & mobile apps

Resource Owner Credentials Grant

User provides credentials to the app

Client Credentials Grant

No authorization needed from User

Refresh Token Grant

Refresh token => New access tokens

raj@acloudfan.com
http://www.acloudfan.com

https://developer.spotify.com/web-api/authorization-guide/#authorization-code-flow

FLOW	CAN FETCH A USER'S DATA BY REQUESTING ACCESS?	USES SECRET KEY? (KEY EXCHANGE MUST HAPPEN SERVER-SIDE!)	ACCESS TOKEN CAN BE REFRESHED?
Authorization Scope Grant ✓	Yes	Yes	Yes
Client Credentials Grant ✓	No	Yes	No
Implicit Grant ✓	Yes	No	No
Refresh Token Grant ✓			

~~Resource Owner Credentials Grant~~

OAuth2.0 Design Decisions

raj@acloudfan.com
http://www.acloudfan.com

- Scopes of the user data (API)
- Type of OAuth grants to be supported
  - Authorization || Implicit Grant — Private data
  - Client Credentials — Public data
  - For trusted clients would you use “Resource Credentials grant”?
- Implementing the OAuth
  - Build

API Management Platform

raj@acloudfan.com
http://www.acloudfan.com

Functional Attacks

http://www.acloudfan.com

raj@acloudfan.com

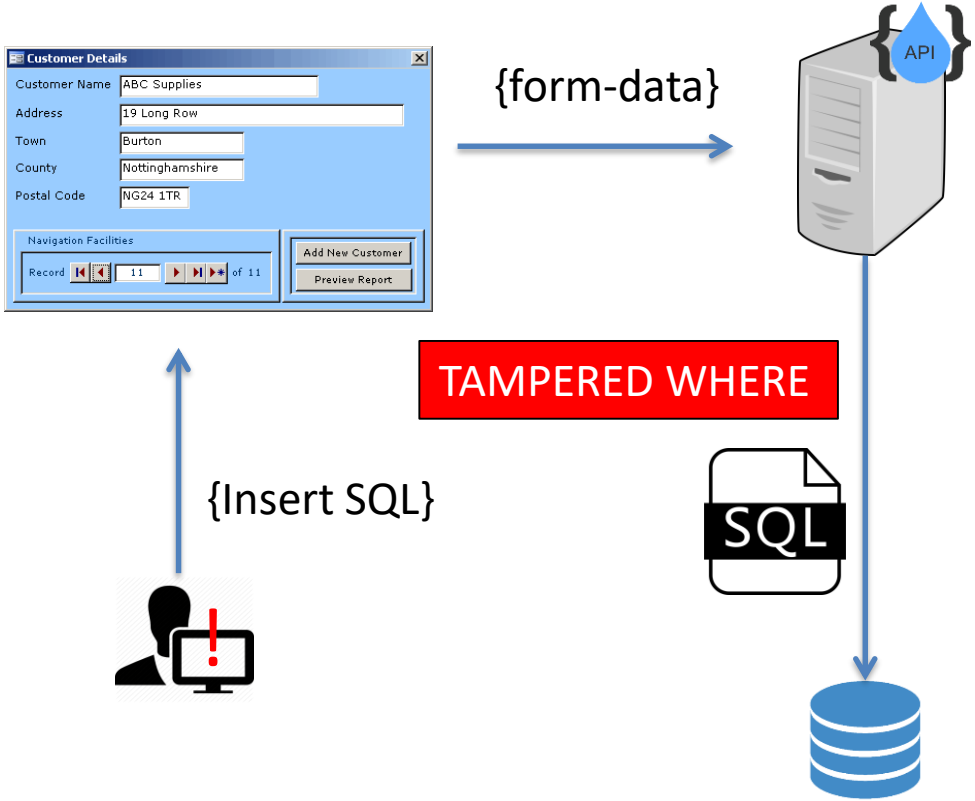
Parts of a course that covers the A to Z of RESTful API. More information.

UDEMY Link With Coupon Discount

SQL Injection

https://www.owasp.org/index.php/SQL_Injection

raj@acloudfan.com
http://www.acloudfan.com

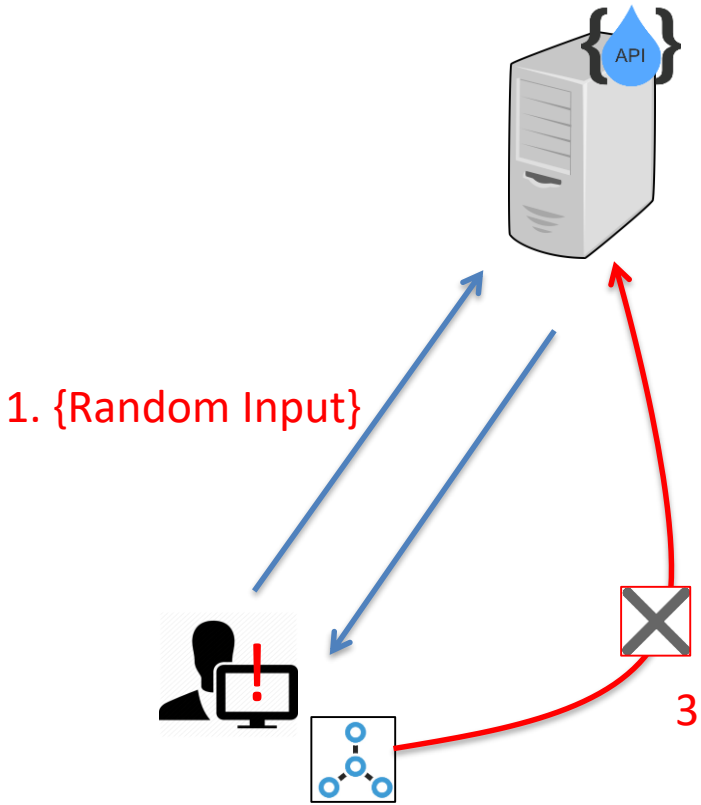


- Read sensitive data
- Modify or delete data
- Take admin action on DB
  - XPath, JSON Path, XSLT

Fuzzing

Also refers to the testing technique

raj@acloudfan.com
http://www.acloudfan.com



- Test the API with *fuzzing* in mind
- Do not send back the internal errors

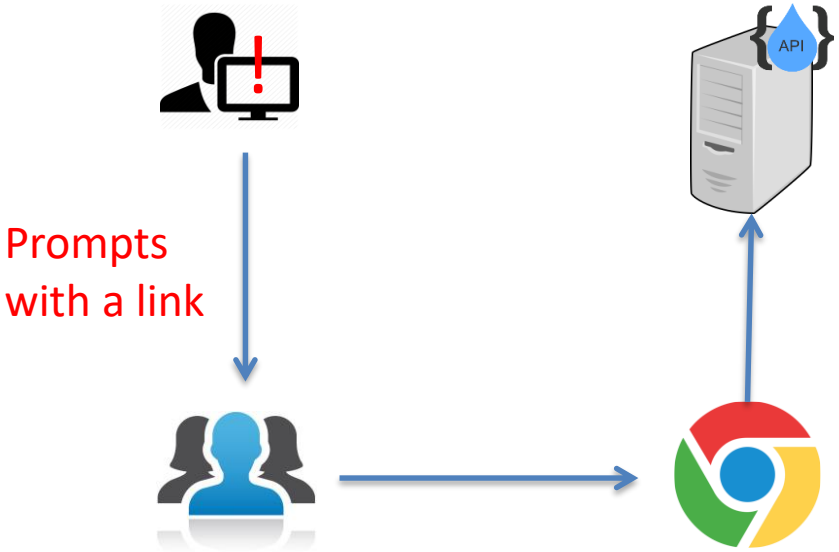
  E.g., SQL exceptions

https://www.owasp.org/index.php/Fuzzing

Cross Site Forgery

raj@acloudfan.com
http://www.acloudfan.com

Attacker forces an end user to execute script

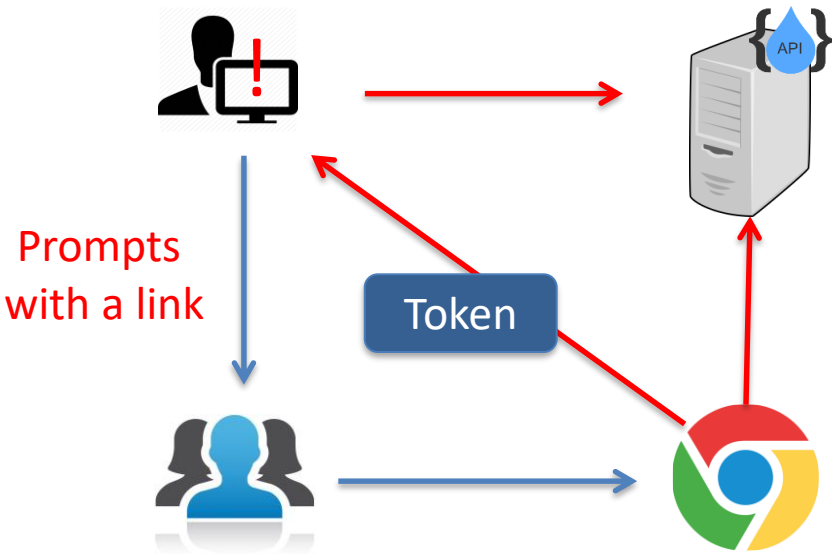


- Use POST instead of GET
- Break transaction into steps
- Add custom headers

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

Token Hijacking

raj@acloudfan.com
http://www.acloudfan.com



- Ensure expiry of token
- Un-predictable token patterns
- Additional security headers

Receives hacker's script

Script accesses access/session **Tokens**

https://www.owasp.org/index.php/Session_hijacking_attack

Solution to Functional Attacks

raj@acloudfan.com
http://www.acloudfan.com

- Follow the BEST practices for coding and REST API
- Create a process for code review (or adopt peer programming)
- Test & Monitor continuously; Invest in tools
- Select an appropriate security model for API
- Consider an API gateway or API management solution
- Set aside budget for API testing ☺

HttpMaster
API & REST Development and Test Tool

PARASOFT

SoapUI