MODULE 03

WEB API SECURITY

MODULE TOPICS

Authentication
Cross-Site Scripting (XSS)
SQL Injection (SQLi)
Cross-Site Request Forgery (CSRF)
Over-Posting

AUTHENTICATION

3 COMMON AUTHENTICATION METHODS

HTTP Basic Authentication

- Username and password is sent via HTTP user agent and the HTTP header
- Credentials are sent as plain text, so must be secured with SSL

AUTHENTICATION

3 COMMON AUTHENTICATION METHODS

API Keys

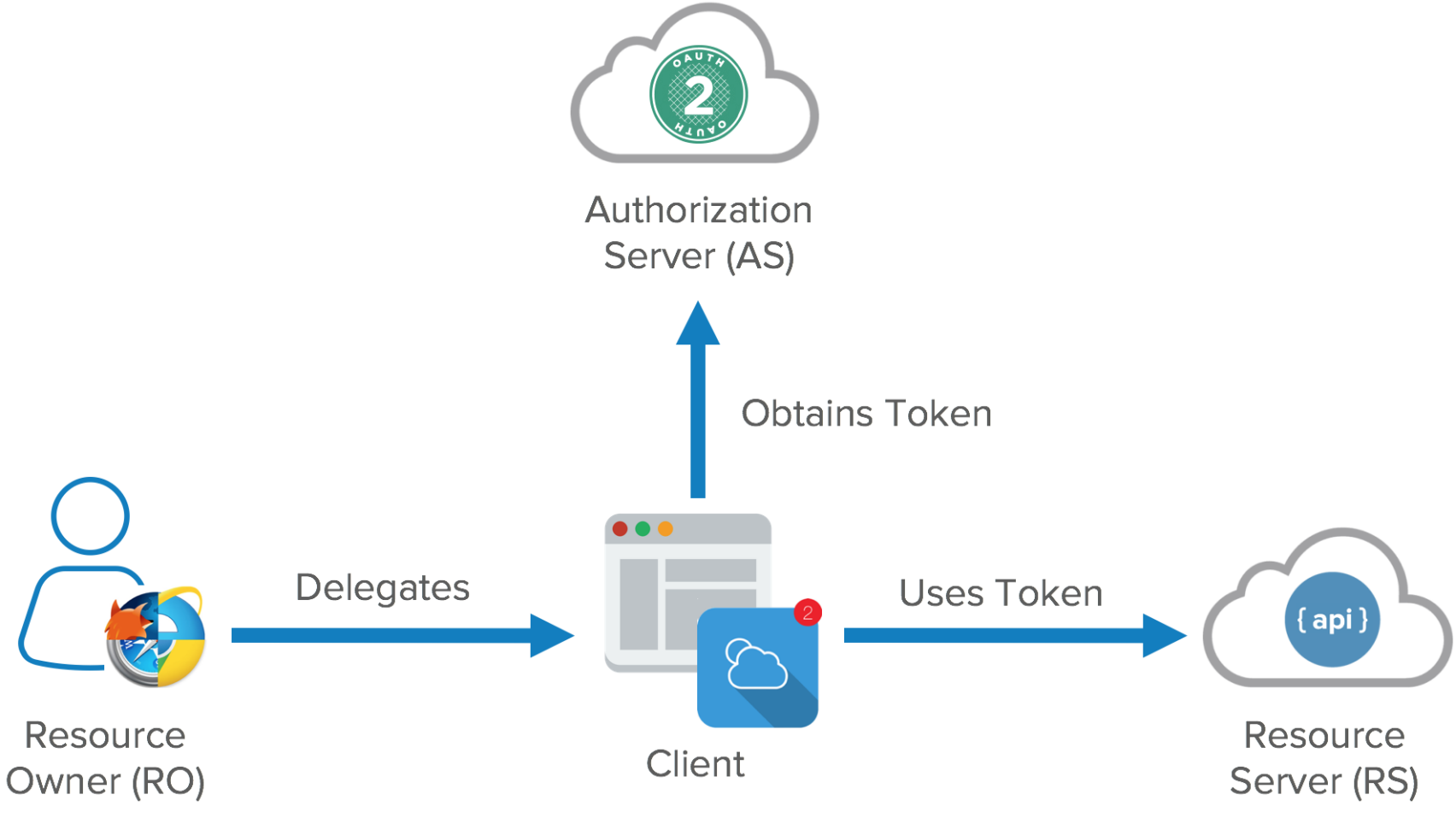
- Server generated key is sent to client which uses it to authenticate going forward
- If key is intercepted, system is compromised
- Often used for authorization as well, which it is not designed for

AUTHENTICATION

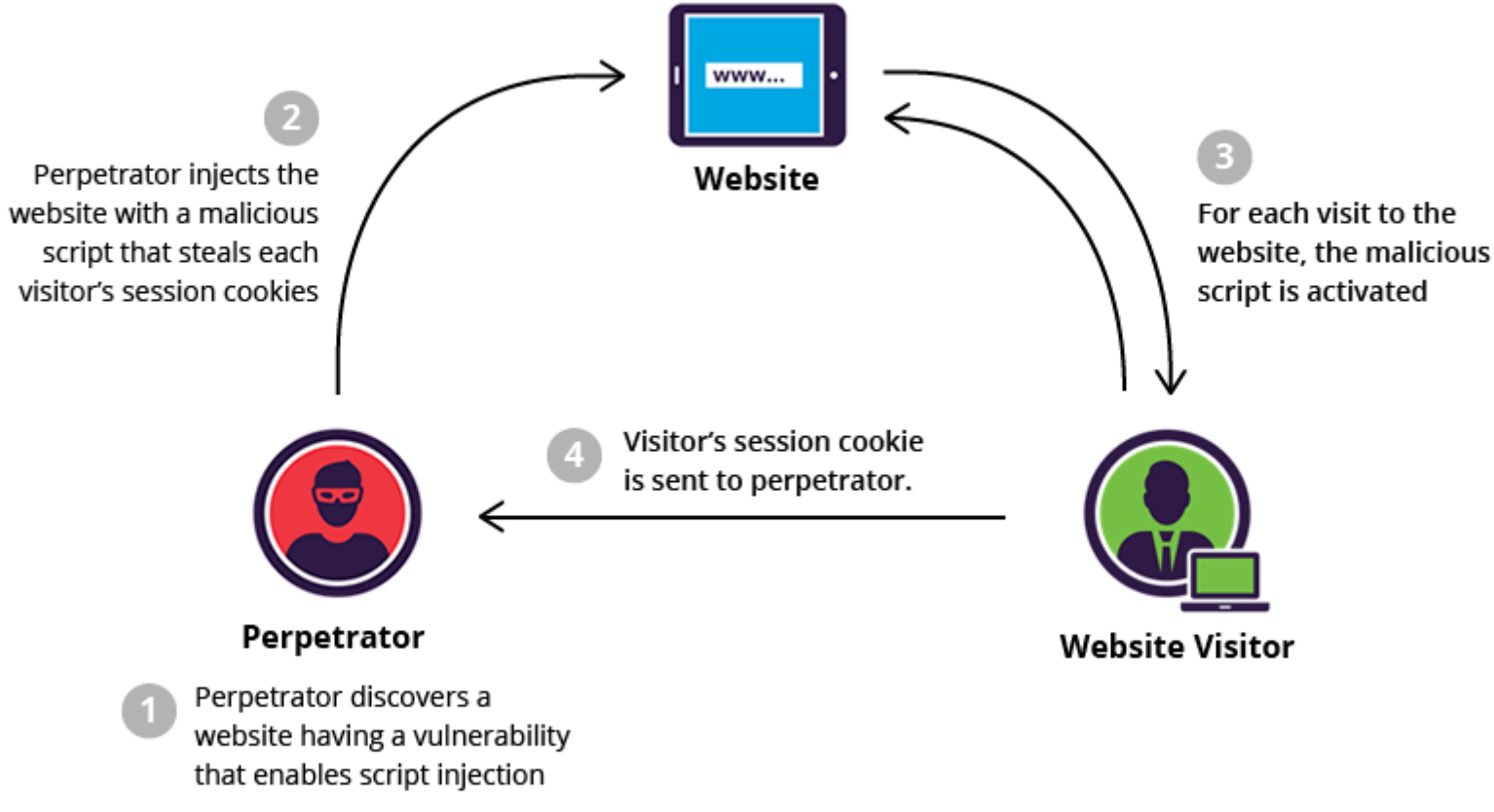
3 COMMON AUTHENTICATION METHODS

OAuth2

OAUTH


Authorization
Server (AS)
Obtains Token
Delegates
Uses Token
{ api }
Resource
Owner (RO)
Client
Resource
Server (RS)

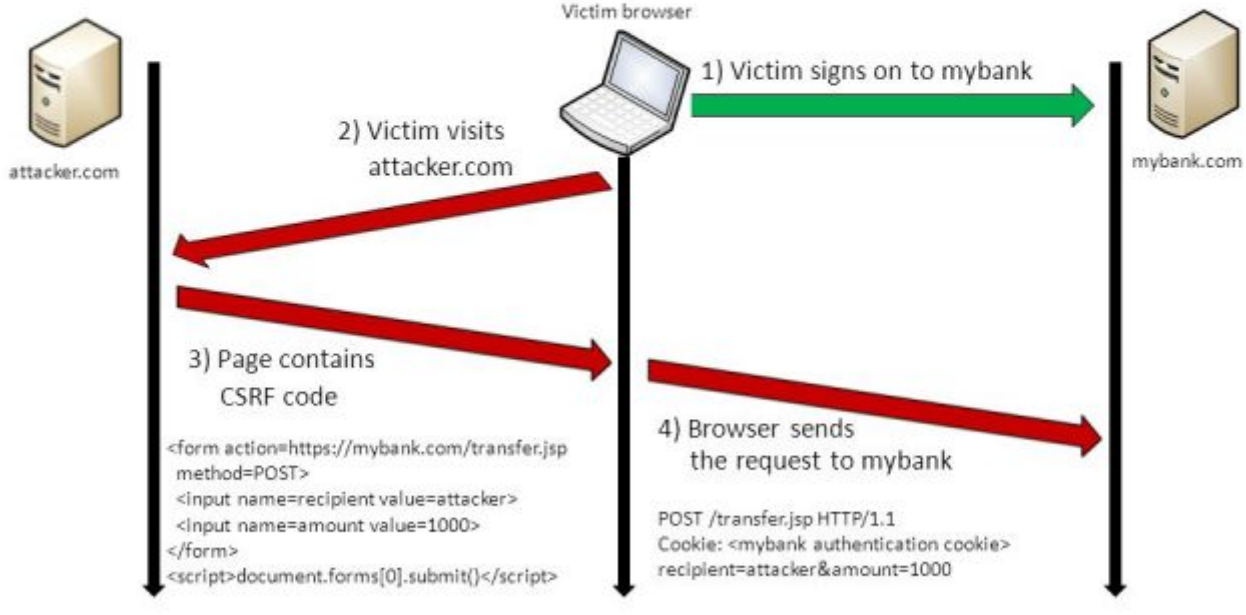
CROSS-SITE SCRIPTING (XSS) AND SQL INJECTION (SQLI)



CROSS-SITE SCRIPTING (XSS) AND SQL INJECTION (SQLI)

- With Post and Put, Web API accepts in data that will be stored usually in a SQL database
- This means XSS (HTML / JavaScript code) or SQLi (SQL code) and be injected for dubious reasons
- **Defense:** Sanitize data being received from users, best to use a Security Encoding Library like Microsoft's AntiXSS

CROSS-SITE REQUEST FORGERY (CSRF)



CROSS-SITE REQUEST FORGERY (CSRF)

- Malicious site uses authentication token from another site to access data
  - Takes advantage of tokens being passed via all requests
- Also known as one-click attack or session riding
- **Defense:** CSRF Anti-Forgery Token to verify source of request

OVER-POSTING

- Model data that should be private is public, so can be bound to
- Malicious web site can send data to the Web API and model binding will set the "private" data since it is marked public
- **Defense:** MVVM, Base Class, or [BindNever]

ANY QUESTIONS?