ASP.NET Security

Dominik Pinter, dominikp@kentico.com, @DominikPinter

Kentico

About me

- 6 years experience with ASP.NET development
- MCPD for .NET 4.0
- Certified Ethical Hacker
- Working at Kentico software
- Development -> Product management
- Likes: beer, scotch whiskey, cloud, security
- @DominikPinter

Kentico

Agenda

- Introduction
- Development
  - Authentication
  - Writing secure code
- Deployment

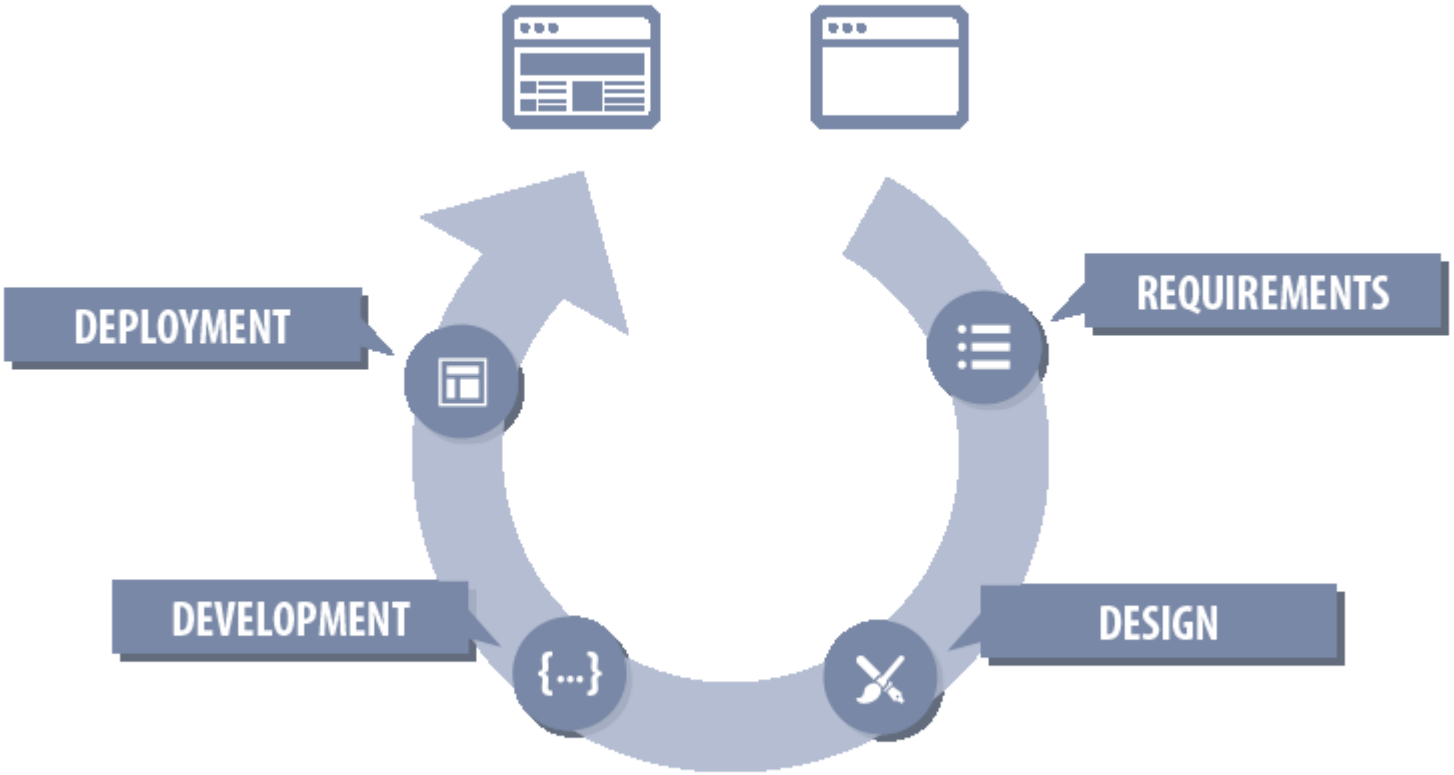
Resistance is futile

A.K.A

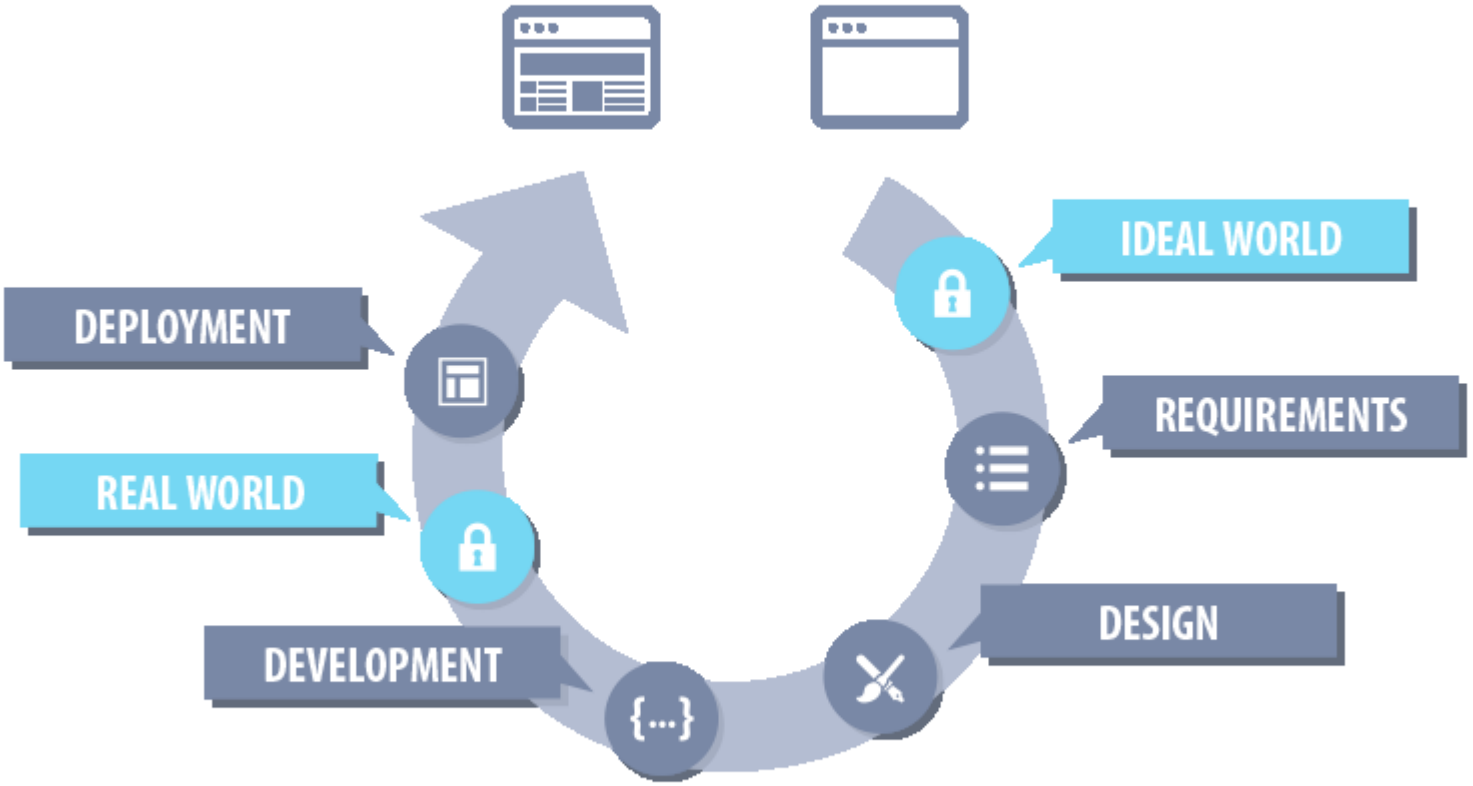
No website is 100% Secure

Kentico

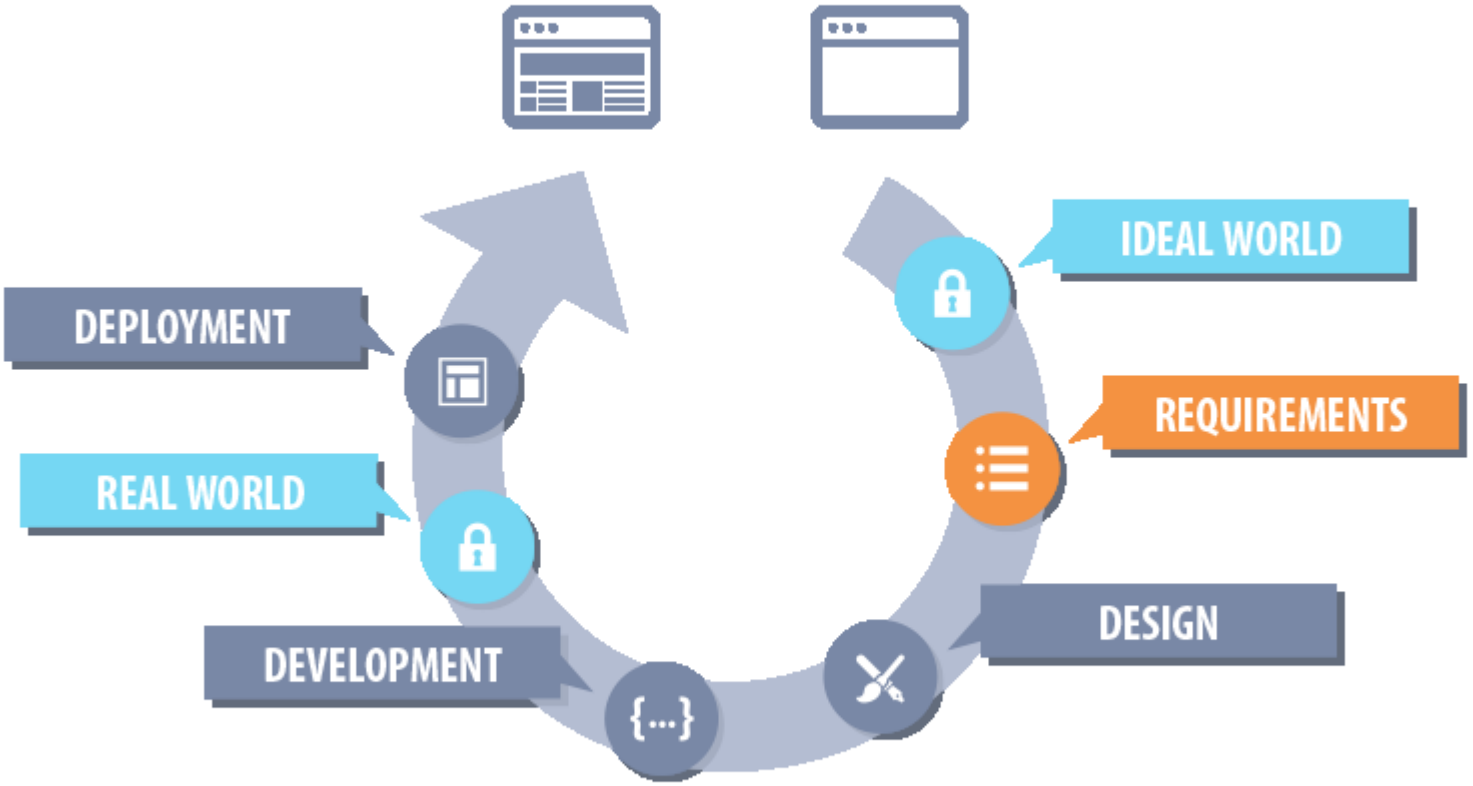
Development process



Security process



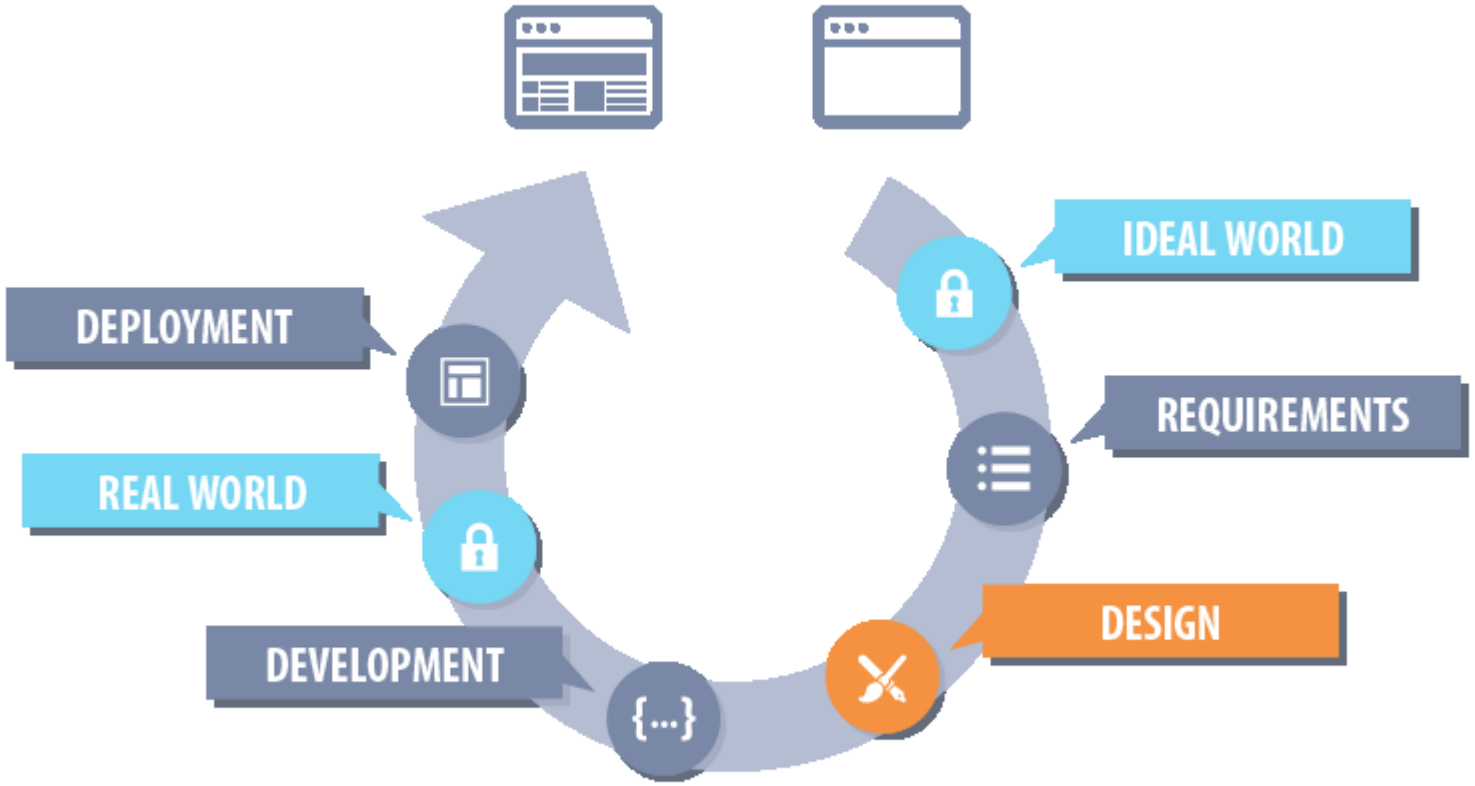
Requirements



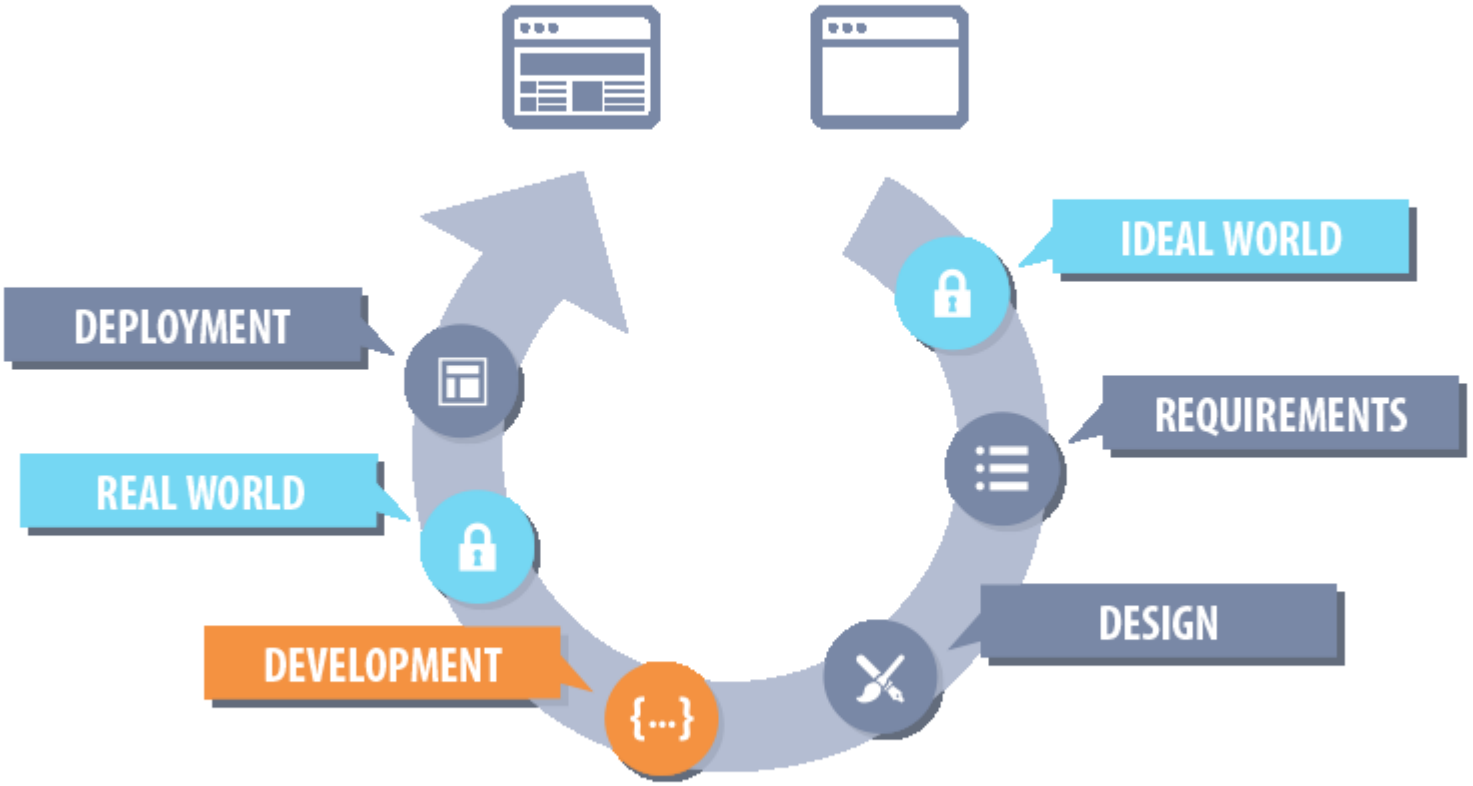
Security related certifications

- PCI (Payment Card Industry) = Credit cards
  - PA = Vendor cerfitication
- Safe Harbor = Trasferring data between EU and US
- HIPAA = Private medical information

Design


IDEAL WORLD
REQUIREMENTS
DESIGN
DEVELOPMENT
REAL WORLD
DEPLOYMENT

Development



Authentication

HTTP Basic Authentication

```
GET http://localhost/page HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 …
Accept: text/html,application/xhtml+xml,…
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Connection: keep-alive
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

ASP.NET Forms Authentication

- Built in ASP.NET
- Uses forms and HTTP POST
- Cookie based
- Prepared components
- Web.config settings
- Integrated with ASP.NET membership providers

ASP.NET Membership Providers

- .NET way how to work with Users, Roles, …
- SQL Tables + Standard classes
- Providers model

DEMO

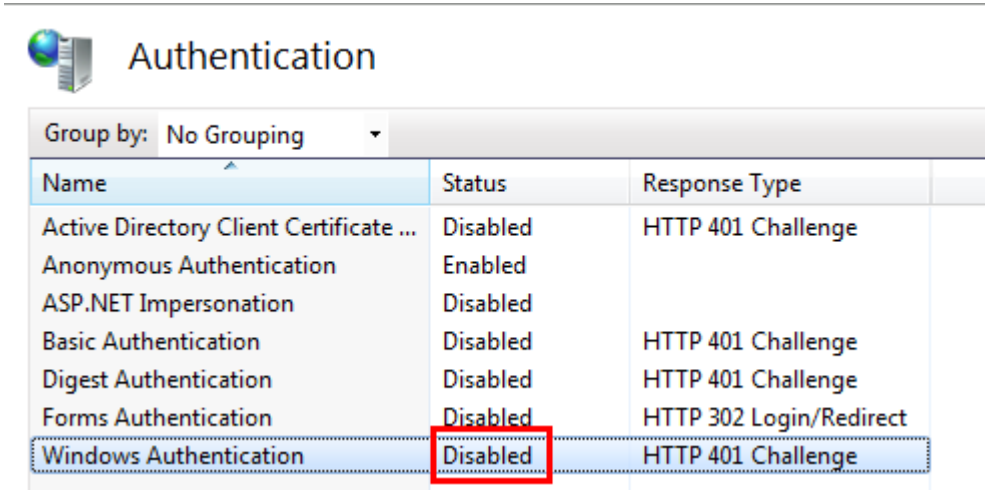
ASP.NET Forms + Membership providers

ASP.NET Windows Authentication

- Web.config:

```
<authentication mode="Windows">
</authentication>
```

- IIS



DEMO

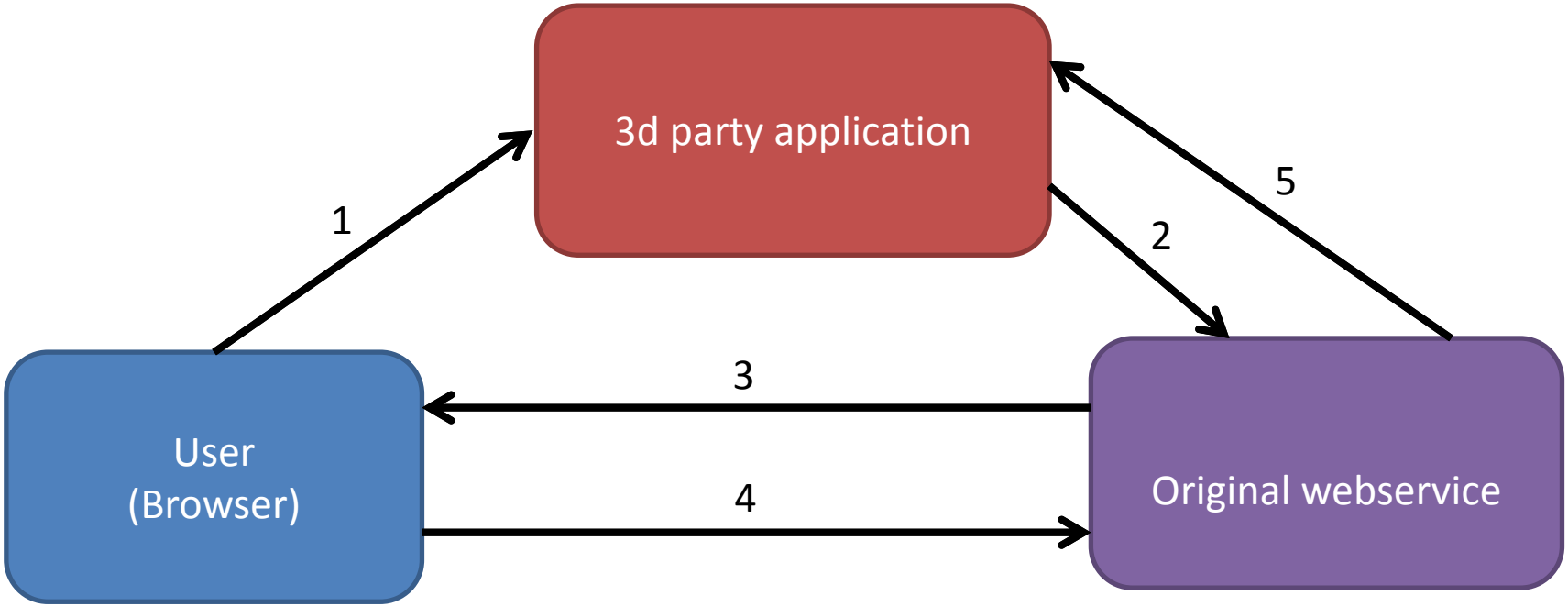
ASP.NET Windows auhentication

OAuth Basics

- An authentication mechanism for web applications/web services

- OAuth 1.0 - RFC 5849 http://tools.ietf.org/html/rfc5849
- OAuth 2.0 – draft http://tools.ietf.org/html/draft-ietf-oauth-v2-31

OAuth – How It Works



1. User sends request to 3rd party application
2. 3rd party application requests access token
3. User is redirected to original web service
4. User authenticates by user name and password to original web service
5. 3rd party application gets the access token

Kentico

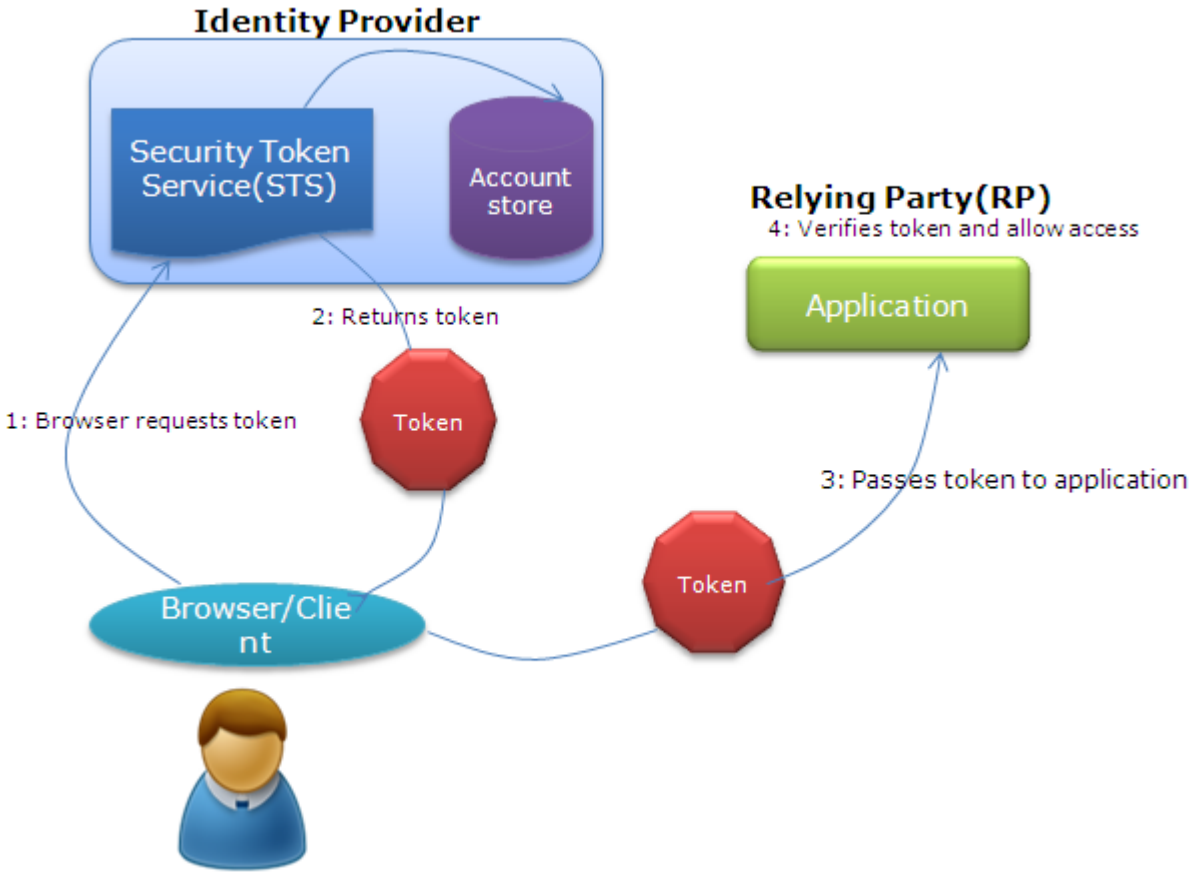
DEMO

DEMO

OAuth

Kentico

Claim Based Authentication



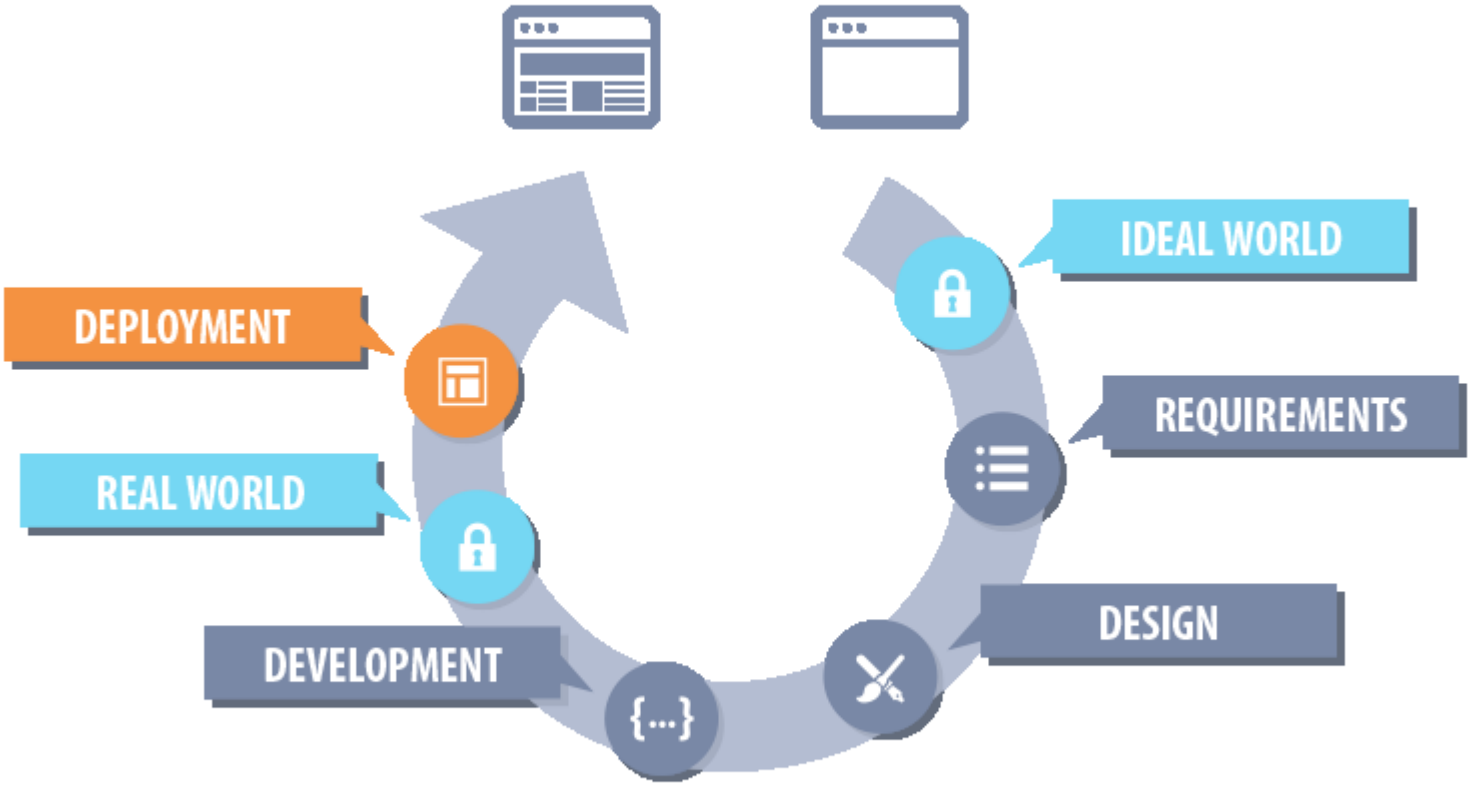
Kentico

DEMO

Claim based authentication

Writing Secure Code

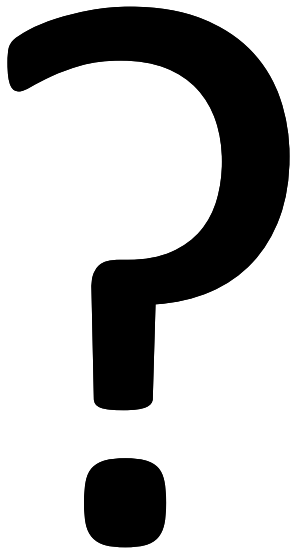
- SQLi => LinqToSQL, ASP.NET Entity Framework
- XSS => Request validation, AntiXSS library, Output encoding
- CSRF => ViewState validation (WebForms)
- Clickjacking => X-Frame-Option:SAMEORIGIN
- Session attacks => Session ID regeneration
- OWASP project


IDEAL WORLD
REQUIREMENTS
DESIGN
DEVELOPMENT
REAL WORLD
DEPLOYMENT

Deployment

- Create Checklist and use it!
- Delete all the testing data!
- Turn off all debugging features!
- Deploy to well secured environment!
- Configure SSL!
- Limit access to private data!
- Consider external security audit

Q&A



Kentico

Thank you

dominikp@kentico.com
@DominikPinter