

#JDF17

Publishing your app on Appexchange

Sagar Pareek
Sr. Salesforce Engineer
Kayako

@sagarjaipareek

Jaipur Dev Fest



www.jaipurdevfest.com



[@jaipurdevfest](https://twitter.com/jaipurdevfest)





Hello!

I am Sagar Pareek

Sr. Salesforce Engineer @Kayako

Author of two SFDC books

Leader @ India Students DUG

You can find me on twitter @sagarjaipareek

#JDF17

| 2

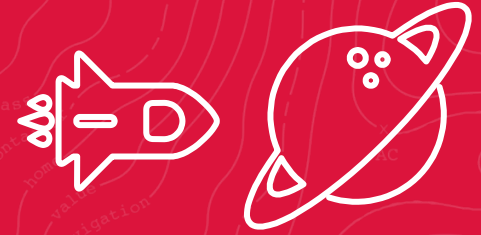
 www.jaipurdevfest.com

 [@jaipurdevfest](https://twitter.com/jaipurdevfest)

 jaipurdevfest@googlegroups.com



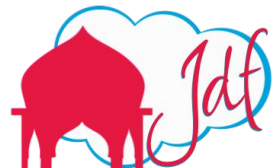
Agenda



- Evaluating your idea and competition.
- Every developer is product manager.
- Securing your app and passing the security review.
- After product launch.



1. Evaluating your Idea and Competition.



“ Usage is like oxygen for Ideas. That means every moment you are working on something without being in public, it's actually dying.
– Matt Mullenweg

Founding Developer Wordpress



Evaluating your Idea

Questions to ask -

- What problem you are trying to solve?
- Who is your target audience?
- What value it will bring into the business?



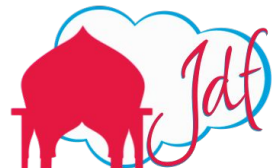
Competition

Questions to ask -

- Who are your competitors?
- How are you different from them?
- What feature set makes you ahead than others?



2. Every developer is a product manager.



“ *Writing code? That's the easy part.
Getting your app in hands of users
and creating apps that people
really want to use - now that's the
hard stuff.*

– *Jeff Atwood*

Stack Exchange Co-Founder



Vision

You need to have a vision of where the product is heading.

Communication

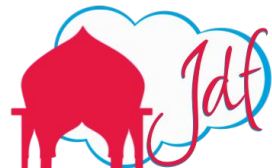
Communicate clearly where the product should be going and let the team execute efficiently.

Execution

Making sure product is being shipped on time.



3. Securing your app and passing the security review



Steps Involved



“ *Nothing is more important to our company than the security of our customer's data.*

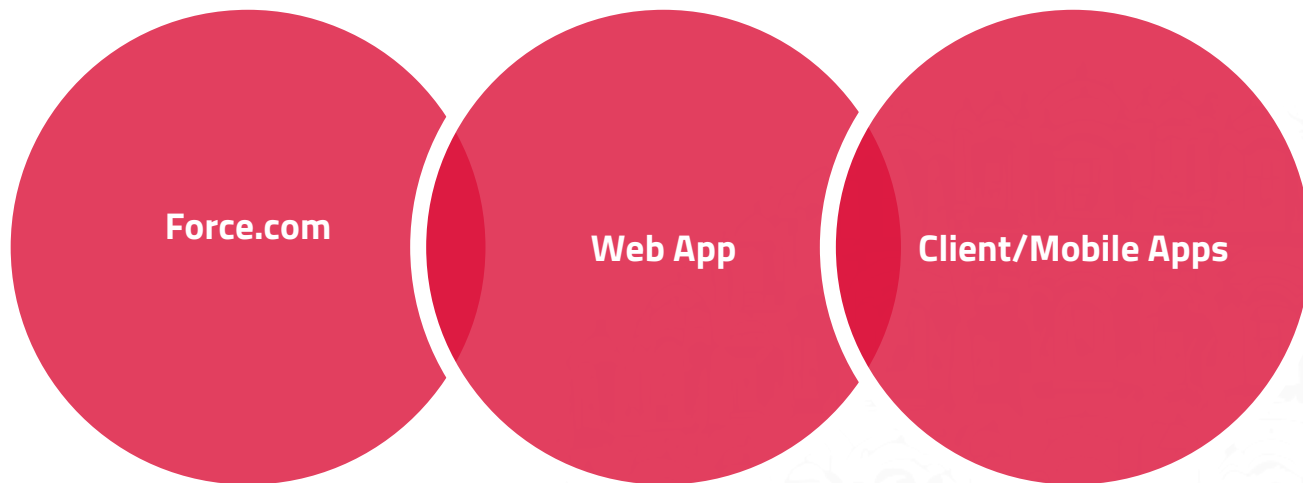
– *Parker Harris*

Salesforce.com Co-Founder



Scope

App Security



Some Major Concepts

Sharing Violations

XSS/ Cross Site Scripting

Storing Secrets

CRUD & FLS

Parameter Tampering

SOQL/SOSL Injection



Sharing Violations

- What is it? : Controller does not respect sharing rules.
- Remedy: Declare classes with sharing.

☹️ public class ClassName {

☹️ public without sharing class ClassName{

😊 public with sharing class ClassName {



CRUD/FLS Violations

- What is it? : Apex does not respect CRUD or FLS.
- Remedy: Use appropriate checks.



```
Account a = new Account (id='0011000001CEFKL');  
a.customField1__c = 'some value';  
update a;
```



```
if(Schema.sObjectType.Account..customField1__c.isUpdateable()){  
    Update a;  
}
```



Cross-site scripting (XSS)

- What is it? : User data is interpreted as active content in a page.
- Remedy: Understand context of merged value and encode in visualforce using `JSENCODE()`
`JSINHTMLENCODE()`



Var scriptvar = '{!myval}';



Var scriptvar = '{!JSENCODE(myvar)}';



Storing Secrets

- What is it? : Sensitive data is exposed to user.
- Remedy: Use protected custom settings.

Demo Involved



SOQL/SOSL Injection

- What is it? : SOQL injection involves taking user-supplied input and using those values in a dynamic SOQL query. If the input is not validated, it may include SOQL commands that effectively modify the SOQL statement and trick the application into performing unintended commands.
- Remedy: Avoid using dynamic SOQL queries. Instead, use static queries and binding variables.



SOQL/SOSL Injection

☹ Folio__cfo=[select id,name from Folio__c where
Transaction__r.Id=:sr.Transaction__r.Id AND id!=null LIMIT 1];

😊 Folio__cfo=[select id,name from Folio__c where
Transaction__r.Id=:String.escapeSingleQuotes(sr.Transaction__r.Id) AND id!=null
LIMIT 1];



Parameter Tampering

- What is it? : While trying to send some value from visualforce page and the value is being used throughout the controller. When this being used with any query it may result into database tampering.
- Remedy: Directly access the parameter while binding with query.



```
String vid = ApexPages.currentPage().getParameters().get('id');  
account acc =[select id,name from account where id=:vid limit 1];
```



```
account acc =[select id,name from account where id=:ApexPages.currentPage().getParameters().get('id') limit 1];
```



Tools for scanning App Security

- Force.com Security Scanner: used for force.com (native) apps. <https://security.secure.force.com/security/tools/forcecom/scanner>
- ZAP tool : used for scanning web apps.

Demo Involved



Initiating Security Review

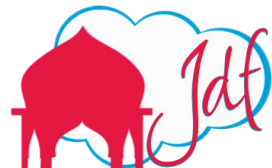
Publishing your app

- Upload and attach managed package with your listing
- Provide a fully functional demo org
- Provide all credentials involved in listing
- Make sure you have false positive justification document if some vulnerabilities are found in web app.
- Don't forget to provide all guides/documentation involved for operation of app.
- Price \$2,700 for paid apps (\$150 thereafter) and free for free apps

Demo Involved



4. After product launch.



After product launch

Publishing your app

- Use right platforms such as producthunt community or online group to get in touch of right audience.
- Use publishing console to get more into analytics related to your app.
- Ask reviews from the customers.
- Make necessary changes using VOC.



Resources

- Secure Codeing Guideline
https://developer.salesforce.com/page/Secure_Coding_Guideline
- Publishing app on appexchange
https://developer.salesforce.com/docs/atlas.en-us.packagingGuide.meta/packagingGuide/appexchange_publish.htm
- Resources used in demo -
<http://sagarpareek.com/meetup/jdf-17/>



#JDF17



Thanks!!



Any questions?

You can find me at @sagarjaipareek



Jaipur Dev Fest



www.jaipurdevfest.com



[@jaipurdevfest](https://twitter.com/jaipurdevfest)

