

# Salesforce Snafus: Unveiling and Exploiting Security Misconfigurations Using Commonly Used Widgets

# whoami

- Red Teamer in Healthcare
- Badge Life Enthusiast
- Yoga Instructor and Runner
- Dog Parent

LinkedIn: [Jessa Gegax](#)



# Agenda

- **Background**
  - What is Salesforce: Point-and-Click vs. Manual Coding
    - Flow Builder
    - Page Layout
    - Widgets and Chatter
    - Digital Experience
- **Security Concerns**
  - Misconfigurations
    - Unproper Access to Objects
    - Elevated User Privilege/Roles
- **Attacks in Salesforce**
  - Widgets reveal insecurities
    - Broken Access Control
    - Insecure Direct Object References (IDORs)
- **Remediation, Detection, and Prevention**
  - How to detect proper access for objects/users
  - How to test/detect
- **Closing**
  - Q/A
  - Future Work

# Advisory!

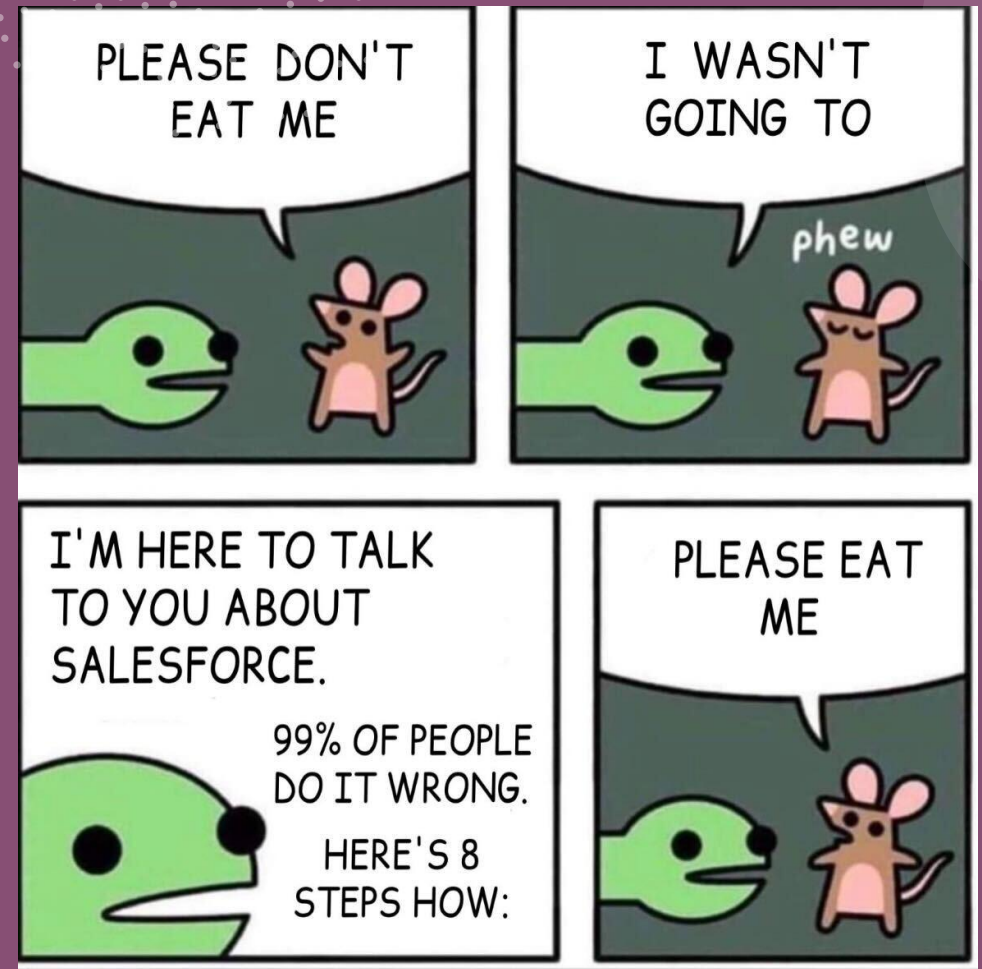


# What is Salesforce?

TLDR; Companies tend to have a lot of data, Salesforce (and other CRMs) help support teams to manage that data.

This talk focuses on:

- Flow Builder (modifies salesforce objects)
- Page Layouts (determines visibility)
- Chatter widget (displays information)
- Digital Experience Site (renders widgets)



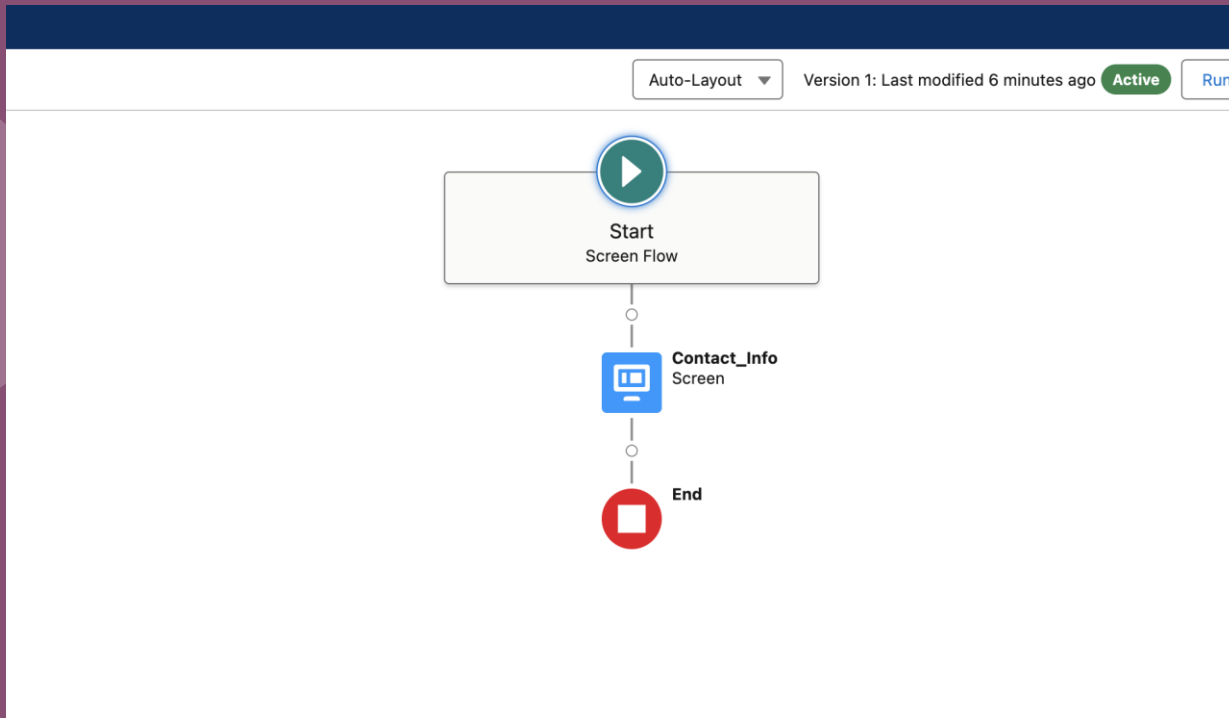


**DEFAULT CONFIGURATIONS...**



**DEFAULT CONFIGURATIONS EVERYWHERE**

# Flow Builder



### Edit Screen

#### New Contact

**Name**

First Name

Last Name

**Account**

If this contact already exists, update the existing record.  Create other contact

# Page Layout

Desktop   Shrink To View   ↻

Account **Biotech Company**   + Follow   New Contact   New Case   New Note

Type	Phone (666) 666-6666	Website	Account Owner Jessa G...	Account Site	Industry Biotechnology
------	-------------------------	---------	-----------------------------	--------------	---------------------------

**Related**   Details

Insufficient permissions  
You don't have user access to view this component.

**We found no potential duplicates of this Account.**

**Contacts (1)**   [New](#)

**John Smith**   [▼](#)

Title: CEO  
Email:  
Phone: (666) 666-6666

[View All](#)

**Opportunities (0)**   [New](#)

**Cases (0)**   [New](#)

**Notes & Attachments (0)**   [Upload Files](#)

[Upload Files](#)

Or drop files

**Partners (0)**   [New](#)

**Activity**   Chatter

[📅](#)   [💬](#)   [📅](#)   [✉️](#)

Filters: All time · All activities · All types   [⚙️](#)

[Refresh](#) · [Expand All](#) · [View All](#)

**Upcoming & Overdue**

No activities to show.  
Get started by sending an email, scheduling a task, and more.

No past activity. Past meetings and tasks marked as done show up here.



Save Quick Save Preview As... Cancel Undo Redo Layout Properties

Quick Find

Add Contacts To C...	Change Record Type	Create Summary	Edit	Generate Document	Link a Slack Channel	Prospecting Insights	Submit for Approval	View Partner Scor...
Add to an Actiona...	Check for New Data	Delete	Edit Labels	Get Contacts	New Gift Entry	Send Survey	View Account Hier...	View Relationship...
Add to Call List	Company Hierarchy	Disable Customer ...	Enable As Partner	Get Survey Invita...	New Partner Channel	Sharing	View Catalogs	
Change Owner	Create Donor Brief	Disable Partner A...	Evaluate Candidate	Include Offline	Printable View	Sharing Hierarchy	View Licensing De...	

Account Sample

Highlights Panel

Customize the highlights panel for this page layout...

Quick Actions in the Salesforce Classic Publisher i

Salesforce Mobile and Lightning Experience Actions i

←

Account Detail

Standard Buttons

Custom Buttons



**New Contact**

Name

First Name

Last Name

Account

Chatter

Create New...

Recent Items

- jessagegax
- Biotech Company
- Josh Ortiz
- Grand Hotels & Resorts Ltd
- Fashion Shop
- Dickenson plc
- Research\_Site
- 23\_0127\_eed\_ps-...
- cyber-security-...

Unable to Access Page

The value of the "file" parameter contains a character that is not allowed or the value exceeds the maximum allowed length. Remove the character from the parameter value or reduce the value length and resubmit. If the error still persists, report it to our Customer Support team. Provide the URL of the page you were requesting as well as any other related information.

[Back](#)

 Recycle Bin

Chatter

- Create New...
- Recent Items
  - jessagegax
  - Biotech Company
  - Josh Ortiz
  - Grand Hotels & Resorts Ltd
  - Fashion Shop
  - Dickenson plc
  - Research\_Site
  - 23\_0127\_ecd\_ps-...
  - cyber-security-...

## Recycle Bin

Help for this Page ?

View: My recycle bin  Search

Undelete Empty your recycle bin Empty your organization's recycle bin

Name	Type	Deleted By	Deletion Date
No records to display.			

Undelete Empty your recycle bin Empty your organization's recycle bin

Empty your organization's recycle bin

# Chatter/Widgets

The screenshot shows the Salesforce Chatter interface for the 'Biotech Company' account. The top navigation bar includes 'Salesforce Chatter', 'Home', 'Chatter', 'People', 'Groups', 'Files', and tabs for '\* All Accounts' and '\* Biotech Company | Account'. The account header displays 'Account Biotech Company' with buttons for '+ Follow', 'New Contact', 'New Case', and 'New Note'. Below this is a table with columns: Type, Phone ((666) 666-6666), Website, Account Owner (Jessa Gegax), Account Site, and Industry (Biotechnology). The main content area is split into two panels. The left panel, titled 'Related', has a 'Details' sub-tab and shows a message: 'We found no potential duplicates of this Account.' followed by a 'Contacts (1)' section containing a card for 'John Smith', CEO, with contact details and a 'View All' link. The right panel, titled 'Activity', has a 'Chatter' sub-tab and features a filter bar with icons for list, chat, calendar, and email. It includes filter settings ('All time', 'All activities', 'All types'), 'Refresh', 'Expand All', and 'View All' options. The activity feed shows 'Upcoming & Overdue' with the message 'No activities to show. Get started by sending an email, scheduling a task, and more.' and a note at the bottom: 'No past activity. Past meetings and tasks marked as done show up here.'

Salesforce Chatter Home Chatter People Groups Files \* All Accounts \* Biotech Company | Account

Account **Biotech Company** + Follow New Contact New Case New Note

Type	Phone	Website	Account Owner	Account Site	Industry
	(666) 666-6666		Jessa Gegax		Biotechnology

**Related** Details

We found no potential duplicates of this Account.

**Contacts (1)** [New](#)

[John Smith](#)

Title: CEO  
Email:  
Phone: (666) 666-6666

[View All](#)

**Activity** Chatter

Filters: All time · All activities · All types


[Refresh](#) · [Expand All](#) · [View All](#)

▼ **Upcoming & Overdue**

No activities to show.  
Get started by sending an email, scheduling a task, and more.

No past activity. Past meetings and tasks marked as done show up here.

 New Task   Log a Call   New Event   Email 

Filters: All time • All activities • All types 

[Refresh](#) • [Expand All](#) • [View All](#)

▼ **Upcoming & Overdue**

No activities to show.  
Get started by sending an email, scheduling a task, and more.

No past activity. Past meetings and tasks marked as done show up here.



# Digital Experience Sites



Login

Research Site

# Finding and Exploiting Vulnerabilities for Your Company



Accounts  
All Accounts ▾

New

17 items • Sorted by Account Name • Filtered by All accounts • Updated a few seconds ago

Search this list.



	Account Name ▾	Account Site ▾	Billing State/Province ▾	Phone ▾	Type ▾	Account Owner Alias ▾
1	University of Arizona		AZ	(520) 773-9050	Customer - Direct	▾
2	United Oil & Gas, UK		UK	+44 191 4956203	Customer - Direct	▾
3	United Oil & Gas, Singapore		Singapore	(650) 450-8810	Customer - Direct	▾
4	United Oil & Gas Corp.		NY	(212) 842-5500	Customer - Direct	▾
5	Test User Account			(999) 999-9999		▾
6	tForce		CA	(415) 901-7000		▾
7	Pyramid Construction Inc.			(014) 427-4427	Customer - Channel	▾
8	Nonprofit for Veterans			(511) 111-1111	Prospect	▾

# General

View and edit the main properties of your site.

## Site Details

Template

Build Your Own

Public Access ⓘ

Guest users can see and interact with the site without logging in



SETUP

## Profiles

### Standard Object Permissions

The permissions defined here control access at the object level. Access to individual records within that object type is controlled by the sharing model. Set access level permissions for individual contributors, managers, and administrators. [How do I choose?](#) ⓘ

	Basic Access		Edit	Delete	Data Administration	
	Read	Create			View All ⓘ	Modify All ⓘ
Accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Account Brands	<input type="checkbox"/>					
Addresses	<input type="checkbox"/>	<input type="checkbox"/>				



SETUP

## Sharing Settings

You can use sharing rules only to grant wider access to data, not to restrict access.

### Step 1: Rule Name

Label

Rule Name  [i](#)

Description

### Step 2: Select your rule type

Rule Type  Based on record owner  Based on criteria  Guest user access, based on criteria

### Step 3: Select which records to be shared



This sharing rule grants access to guest users without login credentials. By modifying the default settings in accordance with these criteria, you're allowing anyone matching these criteria to anyone accessing the site, even without logging in. To secure your site and its data from guest users, consider all the use cases and scenarios that you think are appropriate for the sensitivity of your data. Salesforce isn't responsible for any exposure of your data to guest users related to this change from the default settings.

Criteria **Error: No criteria specified**

Field	Operator	Value	
<input type="text" value="Account Name"/>	<input type="text" value="does not contain"/>	<input type="text" value="&lt;"/>	AND <b>Error: You must enter a value</b>
<input type="text" value="--None--"/>	<input type="text" value="--None--"/>	<input type="text" value=""/>	AND
<input type="text" value="--None--"/>	<input type="text" value="--None--"/>	<input type="text" value=""/>	AND
<input type="text" value="--None--"/>	<input type="text" value="--None--"/>	<input type="text" value=""/>	AND
<input type="text" value="--None--"/>	<input type="text" value="--None--"/>	<input type="text" value=""/>	

[Add Filter Logic...](#)

Additional Options  Include records owned by high-volume users [i](#)

### Step 4: Select the users to share with

Share with

### Step 5: Select the level of access for the users

Default Account and Contract Access



Salesforce URL

/detail/001aj00000WPiLBAA1



CYPRESS



Account  
**Fashion Shop**

Type

Phone

(888) 888-8888

Website

Account Owner



Jessa Gegax



Account Site

Industry

Apparel

```
Sniper attack Start attack
Target   Update Host header to match target
Positions   
1 GET /researchsite/s/detail/$001aj00000WPiLBAA1$ HTTP/2
2 Host: privateresearch-dev-ed.develop.my.site.com
3 Cookie: renderCtx=
  %7B%22pageId%22%3A%22c78c985e-3920-4ce1-af74-6c513e672a18%22%2C%22schema%22%3A%22Published%22%2C%22viewType%22%3A%22Published%22%2C%22brandi
  ngSetId%22%3A%2265234b5b-5e23-4ca3-a5d2-d782a8d6c2c2%22%2C%22audienceIds%22%3A%22%22%7D; CookieConsentPolicy=0:1;
  LSKey-c$CookieConsentPolicy=0:1; BrowserId=UnMqc80eEe-Mazmyi3U-uw; pctrk=d392ebf5-be02-4903-b9c8-f059d708bd09
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
1 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-Mode: navigate
4 Sec-Fetch-User: ?1
5 Sec-Fetch-Dest: document
6 Accept-Encoding: gzip, deflate, br
7 Priority: u=0, i
8
```



### 3. Intruder attack of https://privateresearch-dev-ed.develop.my.site.com

Results Positions

Intruder attack results filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length
0		200	296			115175
1	0000000000f390135	200	146		2294	
2	00000000004a9a491	200	138		2294	
3	00000000003fe2194	200	167		2294	
4	00000000005d2191e	200	166		2294	
5	00000000004fc8d3b	200	139		2294	
6	0000000000102d705	200	166		2294	
7	000000000012d0424	200	175		2294	
8	00000000004f80d08	200	169		2294	
9	00000000007cae89a	200	163		2294	
...	...	...	...	...	...	...
22214	0000000000ff37c2c	200	74		2294	
22215	0000000000e8fb304	200	107		2294	
22216	0000000000b3a7c7f	200	102		2294	
22217	0000000000057e3a3	200	104		2294	
22218	0000000000823556a	200	125		2294	
22219	00000000003495ea2	200	103		2294	
22220	00000000004b1b6e8	200	103		2294	
22221	000000000016b4514	200	119		2294	
22222	0000000000241d78f	200	86		2294	
22223	0000000000c25a8a4	200	79		2294	
22224	00000000004746ea6	200	71		2294	
22225	0000000000486fc1	200	81		2294	
22226	0000000000323a742	200	101		2294	
22227	00000000001f890bc	200	102		2294	
22228	00000000004b74523	200	96		2294	
22229	000000000071d9f0d	200	102		2294	
22230	00000000001d0892e	200	81		2294	
22231	00000000003c61a05	200	102		2294	

#### 4. Intruder attack of https://privateresearch-dev-ed.develop.my.site.com

Results Positions

Intruder attack results filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length
0		200	201			118235
1	003aj000004pYIHAA2	200	345			115175

Salesforce URL: `l/003aj000004pYIHAA2`

## CYPRESS

Contact **Josh Ortiz**

Title: Owner    Account Name: [Fashion Shop](#)    Phone (2): (888) 888-8888    Email:    Contact Owner: [Jessa Gegax](#)

[New Task](#)    [Log a Call](#)    [New Event](#)    [Email](#)

# Remediation, Prevention, and Detection



# Future Work and QA

- Where can default configurations show up in Flows?
- Digital Experience shenanigans...
- Can we automate finding these security misconfigurations?



**What is Salesforce**



**What Does Salesforce Do?**