

#SafeSAPUI5

Keeping SAP customers safe

José Sequeira
June 16th, 2021

UI5con^{ON AIR}

Agenda

What is #SafeSAPUI5

- Definition and Background

#SafeSAPUI5 Objectives

- What's the GOAL of the movement + the “needed” security upskill

Cybersecurity

- Bringing the subject more to the “SAP World”, for developers and everyone involved. Demystifying the “Hacker” role.

The Blog Series

- 10 episodes of real vulnerable customers and attack simulations.

Dos and Don'ts

- Discussing what to do and not to do on custom UI5/Gateway applications (from real life examples).

UI5 Hacker

- The “final” output

What is #SafeSAPUI5

Definition and Background

Overall

- How it all started;
- Definition;
- The current “scenario”;
- The “upskill challenge” for regular ABAP developers.

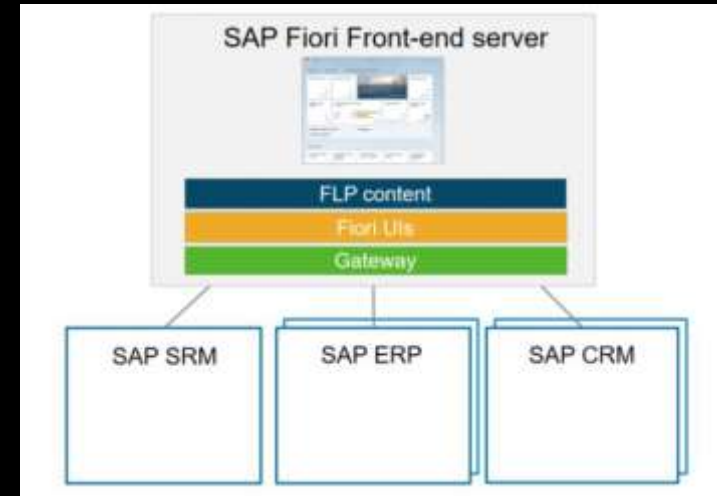
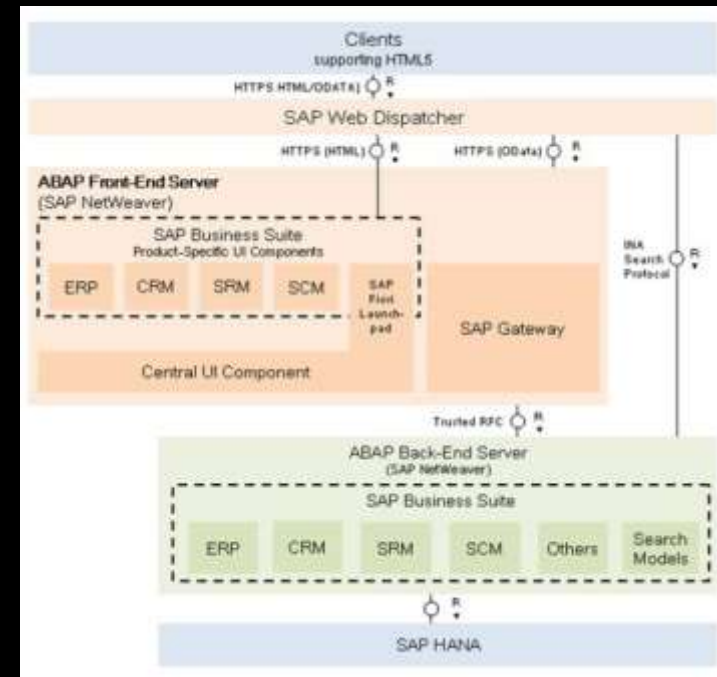
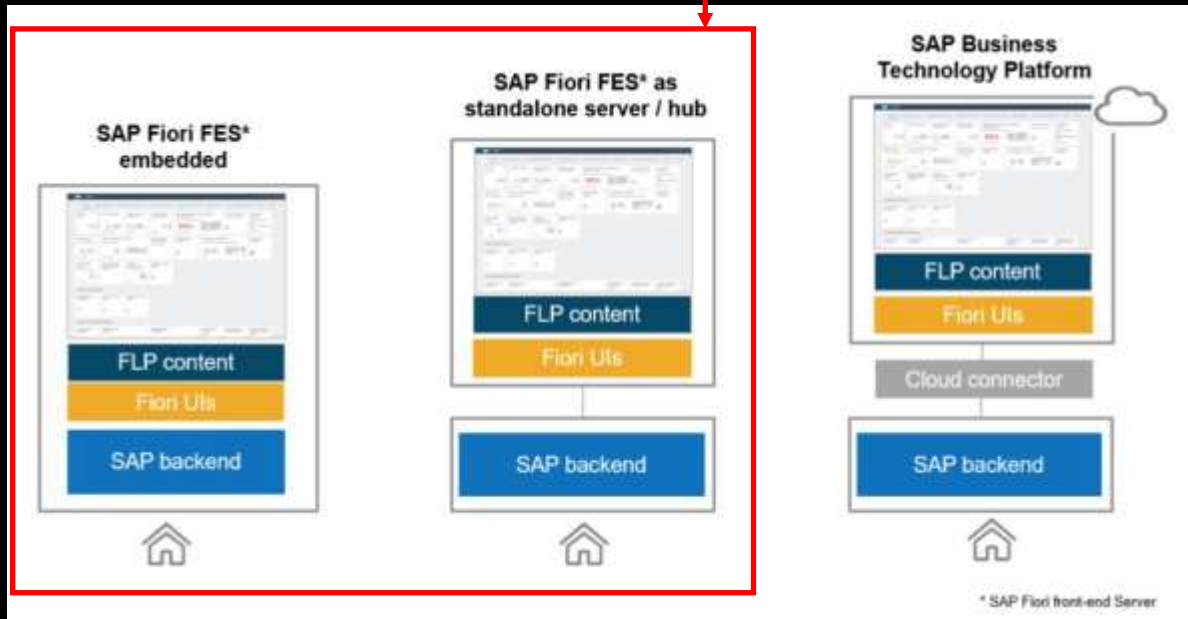


What is #SafeSAPUI5

Definition and Background

Landscapes

- Most common vulnerable Implementations;
- Internet facing applications



#SafeSAPUI5 Objectives

The Goals

Overall

- Upskill for SAP developers (with real examples);
- **Security** Perspective on all SAP “roles” (analysts, QA, Managers, etc);
- Security and QA steps on internet facing developments (Web Apps, Mobile Aps, etc) and interfaces;
- If it's too complex, get external help (security researches, etc).

Keep in mind...

- Remember, your code/solution will probably be “scanned” for vulnerabilities!
- Hackers “love” developers mistakes...

Cybersecurity

in the “SAP World”

Overall

- SAP **Product** Security Response Team (secure@sap.com);
- Security Notes and Patch Days;
- Acknowledgment's;
- “Product” Vulnerability X “Customer Implementation” Vulnerability (**the challenge**);
- Demystifying the “Hacker”;
- Ethical Hacker;
- Bug Bounties.

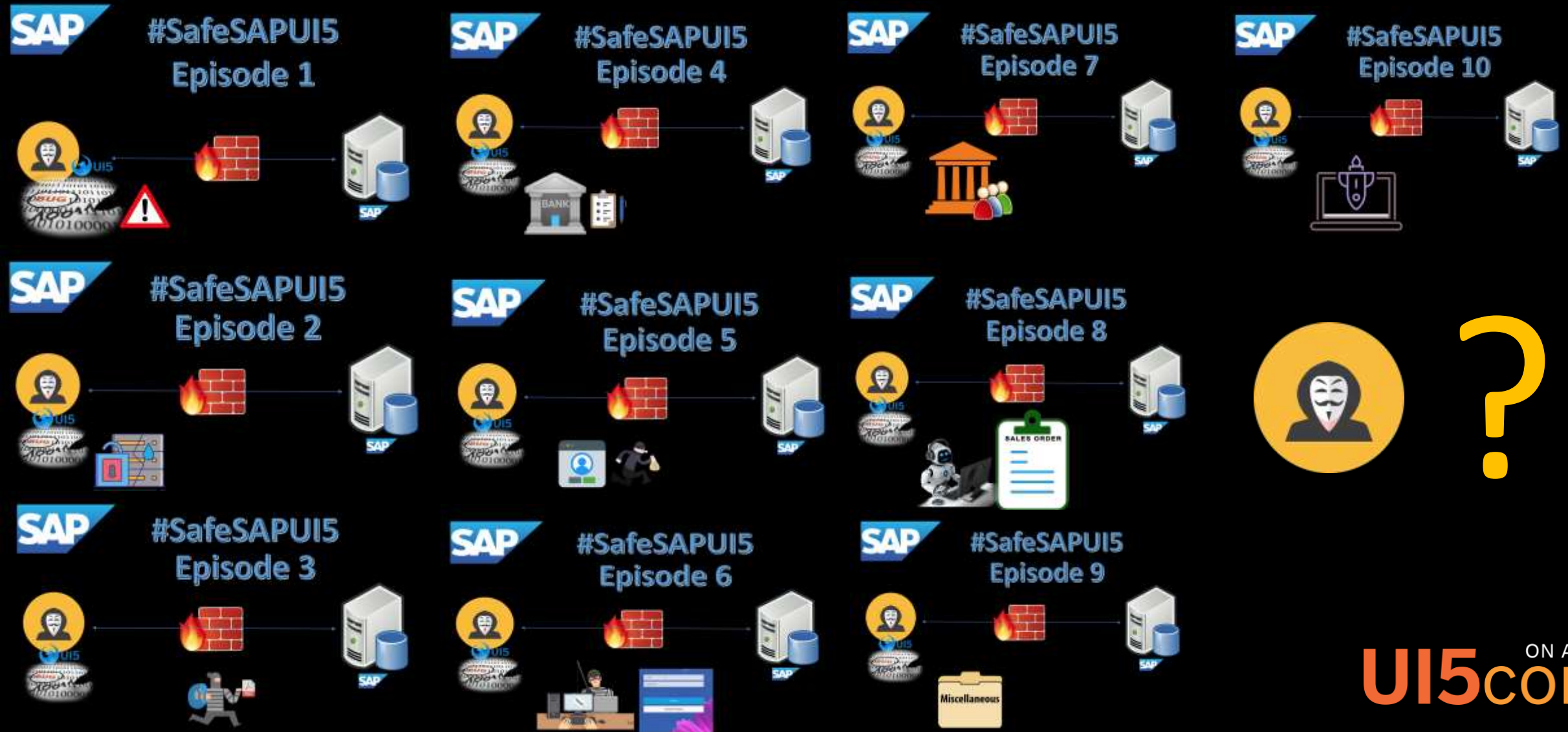
<https://wiki.scn.sap.com/wiki/display/PSR/The+Official+SAP+Product+Security+Response+Space>

Let's see some **code!**



The Blog Series

Hosted on the SAP Community – “Season” 01:



ON AIR
UI5con

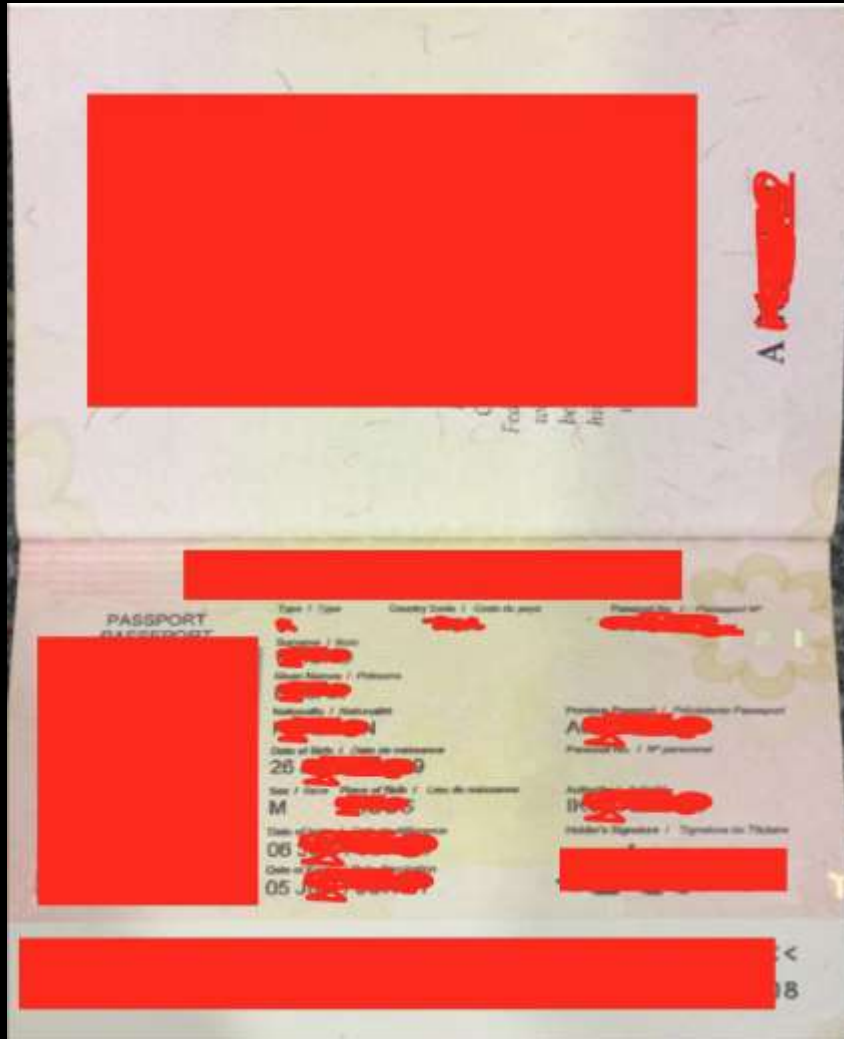
The Blog Series - Global View

Same mistakes



Real Examples

with responsible disclosure



User [REDACTED]

Password *****

Language EN - English

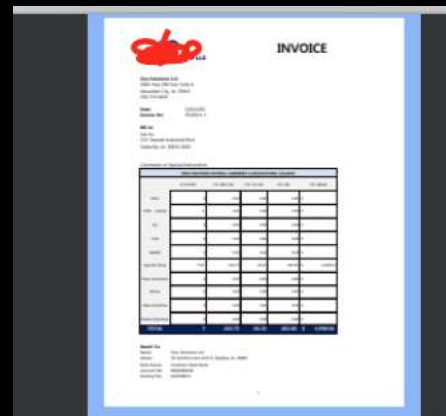
Log On

Change Password

	G	H	I	J	K
1	Mobile	Username	Newpassword	Verifypassword	Securitycode
2	[REDACTED]15	[REDACTED]19	[REDACTED]	[REDACTED]	[REDACTED]
3	[REDACTED]12	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
4	000000000000	11	1 04	1 04	75 7 1

```

<m:properties xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.m
  <d:Kunnr>1 [REDACTED] /d:Kunnr>
  <d:Name1>B [REDACTED] /d:Name1>
  <d:Vbeln>B [REDACTED] /d:Vbeln>
  <d:Bldat>2021-04-22T00:00:00</d:Bldat>
  <d:Wadat>2021-04-24T00:00:00</d:Wadat>
  <d:Wadatlst m:null="true"/>
  <d:Btgew>1 [REDACTED] /d:Btgew>
  <d:Gewei>KG</d:Gewei>
  <d:Anzpk> [REDACTED] /d:Anzpk>
</m:properties>
  
```



```

<d:Netpr> [REDACTED] 7.00</d:Netpr>
<d: [REDACTED] Discount>0.0000</d:AutoDiscount>
<d: [REDACTED] 0.0000</d:TraspUrgent>
<d: [REDACTED] Discount>0.0000</d:ManualDis>
<d:Bstdk>2021-01- [REDACTED] 00:00</d:Bstdk>
<d:Edatu>2021-01- [REDACTED] 00:00</d:Edatu>
<d:BstdkE m:null="true"/>
  
```

Dos and Don'ts

Let's get technical!

Dos

- Security Testing phases;
- Help to promote the security awareness on your SAP customers;
- Solid Captchas (front and back);
- OData services filters;
- Security Layers to protect against attacks like Dos/DDos;
- Promote the **Cloud**;
- Use **standard** login and user roles functionalities;

Don'ts


- Leave hardcoded credentials and “sensitive” comments on your code;
- “Open” OData services entities, and reusable services (remember your **\$metadata** will get **scanned!**). SAPU5 + OData services is not the **only** way to go...;
- Forget to implement filters on your entities;
- Create “Custom Login” screens/functionalities (trying to avoid licensing costs) or as I call, the “fake login”;
- Return sensitive information on internet facing OData services (like user names, addresses, hashed passwords, etc). Most of the time the cause are the Search Help entities.



Let's see some **code!**




#SafeSAPUI5 Main Page

www.safesapui5.web.app


 Conteúdo #SafeSAPUI5

 SAP e outros produtos e serviços SAP mencionados aqui, bem como seus respectivos logotipos, são marcas comerciais ou marcas registradas da SAP SE (ou uma empresa afiliada da SAP) na Alemanha e em outros países. Esta página/iniciativa não está relacionada a SAP, tem como objetivo ajudar a comunidade de desenvolvedores SAP. 


O que é
#SafeSAPUI5?...
Definição




Reportar uma
vulnerabilidade
Canal Oficial SAP®





Caçador de Bugs
SAP®
bounty@sap.com





▼ Conteúdo Relacionado

▼  #SafeSAPUI5 Series (11)

  0 - Being extra careful with "exposed" Fiori / OData solutions



<https://blogs.sap.com/2021/02/10/being-extra-careful-with-exposed-fiori-odata-solutions/>

02/10/2021


  1 - #SafeSAPUI5 Series Episode 01: "Hardcode is never a good solution"

<https://blogs.sap.com/2021/03/03/safesapui5-ep01/>

03/03/2021

  2 - #SafeSAPUI5 Series Episode 02: "User and Password list leaked? Like the ones you see on the news..."

<https://blogs.sap.com/2021/05/06/safesaoui5-ep02>

 "THE WAY TO BE SAFE IS NEVER TO BE SECURE" BY BENJAMIN FRANKLIN



ON AIR 
UI5con

What was the “final” output?



The UI5 Hacker Ebook!

It's free! No registration needed...



UI5 HACKER

- UI5 (SAPUI5/OpenUI5) & SAP Gateway
- SAP Fiori
- SAP Cloud (BTP)
- Cyber Security
- Real Vulnerabilities fixed and more...

JOSÉ AUGUSTO DE MELLO SEQUEIRA



UI5 HACKER

- UI5 (SAPUI5/OpenUI5) & SAP Gateway
- SAP Fiori
- SAP Cloud (BTP)
- Cyber Security
- Real Vulnerabilities fixed and more...

JOSÉ AUGUSTO DE MELLO SEQUEIRA

What's in here?

- Extra history and background;
- 4 extra “episodes”;
- Extra recommendations;
- And it's only 90 pages long!

ON AIR
UI5con

Download it here (in Portuguese and English):

www.ui5hacker.web.app




SCAN ME

ON AIR
UI5con

UI5 Hacker Ebook

Download - Escolher idioma



The book cover features a white Guy Fawkes mask on a dark background, with a Brazilian flag in the top right corner. The title "UI5 HACKER" is prominently displayed in white. Below the title, a list of topics is shown: SAP UI5, SAP Fiori, SAP Cloud (BTP), Cyber Security, and Real Vulnerabilities fixed and more... The author's name, JOSÉ AUGUSTO DE MELLO SEQUEIRA, is at the bottom.

Feedbacks


Procurar



José Sequeira Ebook Review

03/05/2021 às 23:23

Aqui estarão os reviews do ebook enviados pelos leitores, envie o seu também através de algum dos canais de comunicação acima.



José Sequeira Ebook Review

03/05/2021 às 23:23

Here will be the ebook reviews sent by the readers, send yours through one of the communication channels above.

#SafeSAPUI5

Atualizar

Thank you!

José Sequeira

As the SAP "Hacker"

www.safesapui5.web.app

www.ui5hacker.web.app



UI5con^{ON AIR}