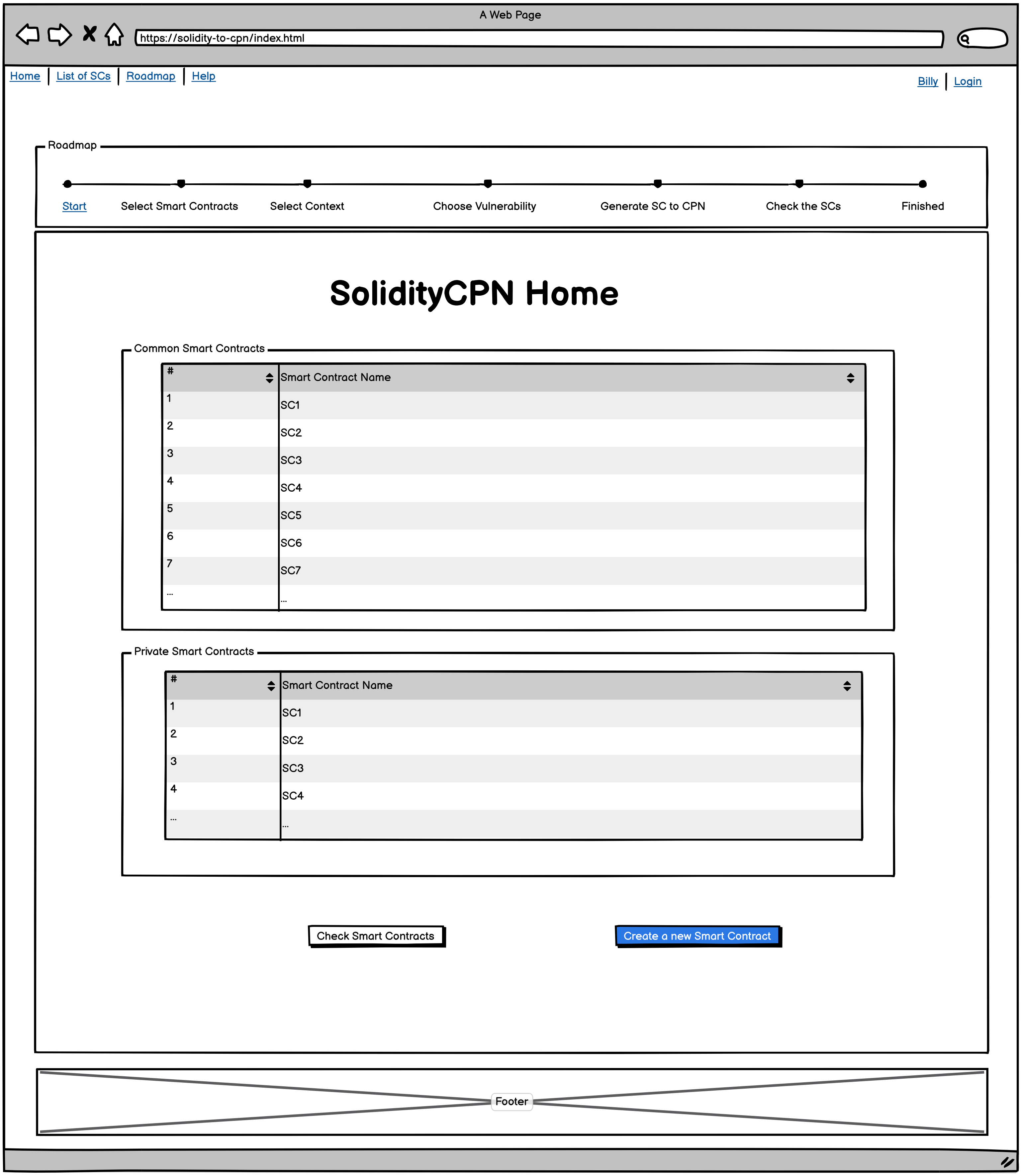


A Web Page

https://solidity-to-cpn/index.html

Home | List of SCs | Roadmap | Help

Billy | Login

Roadmap

Start — Select Smart Contracts — Select Context — Choose Vulnerability — Generate SC to CPN — Check the SCs — Finished

SolidityCPN Home

Common Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
5	SC5
6	SC6
7	SC7
...	...

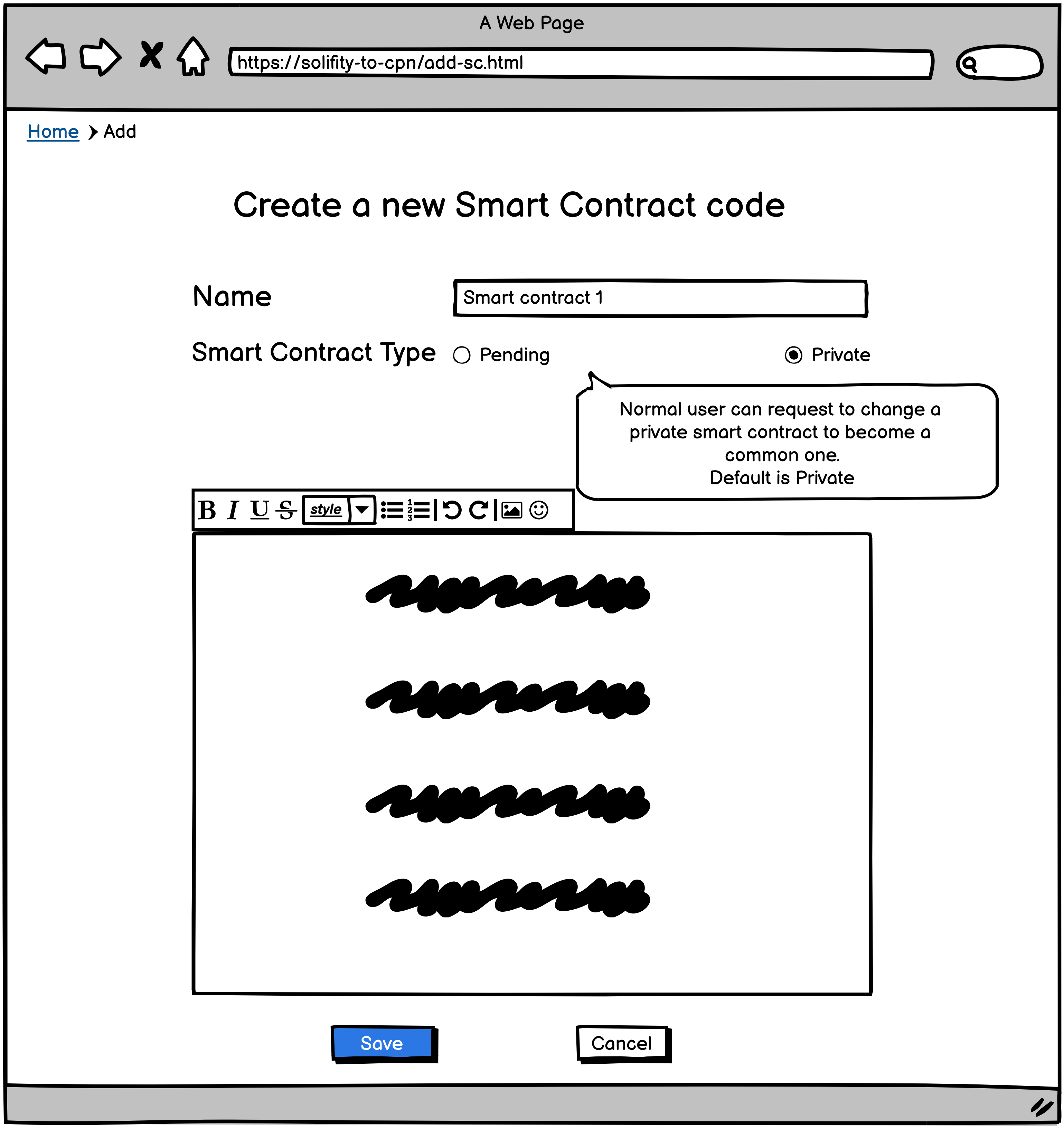
Private Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
...	...

Check Smart Contracts

Create a new Smart Contract

Footer

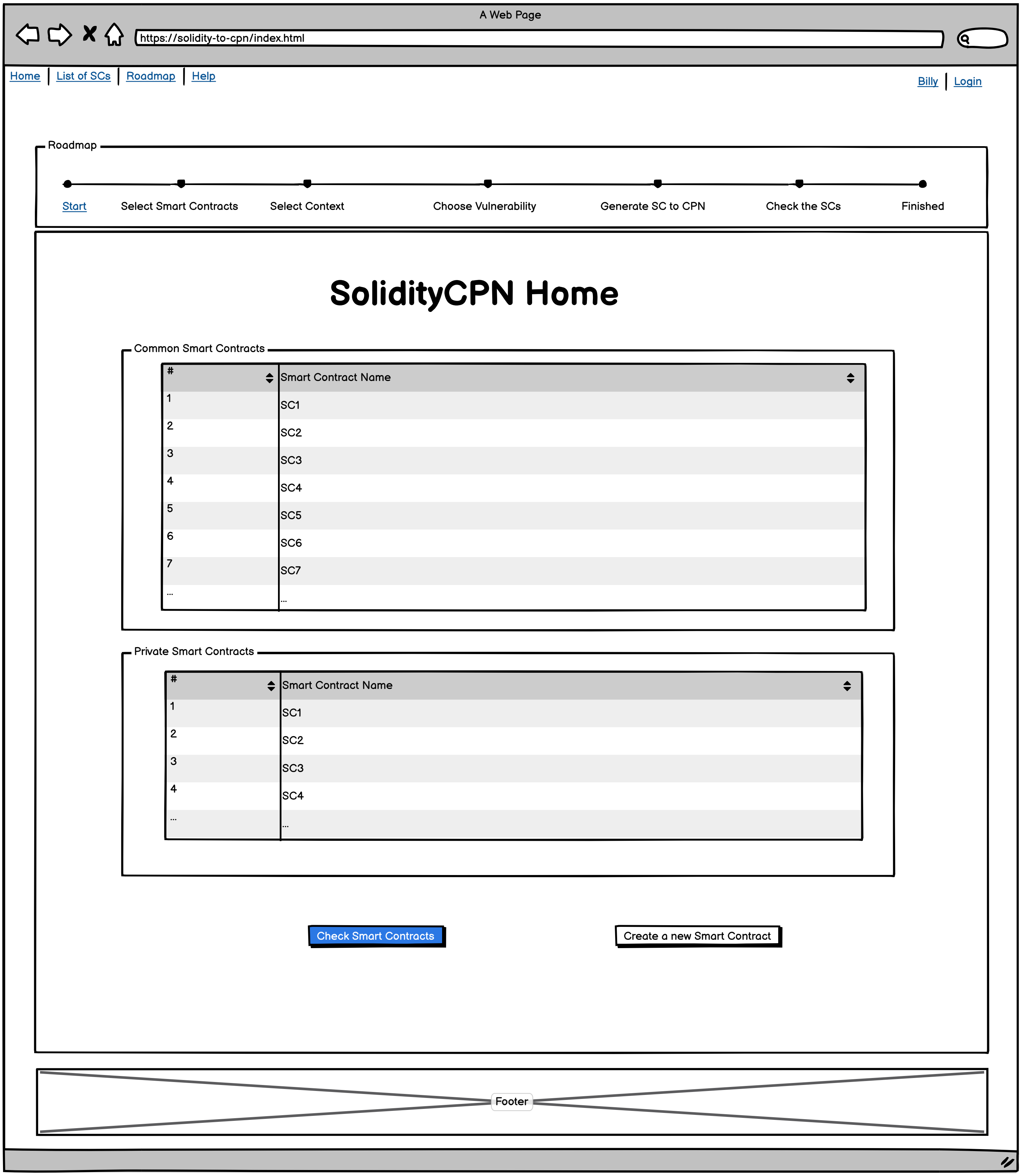


Create a new Smart Contract code

Name: Smart contract 1

Smart Contract Type ○ Pending ● Private

Normal user can request to change a private smart contract to become a common one.
Default is Private



A Web Page

https://solidity-to-cpn/index.html

Home | List of SCs | Roadmap | Help

Billy | Login

Roadmap

Start — Select Smart Contracts — Select Context — Choose Vulnerability — Generate SC to CPN — Check the SCs — Finished

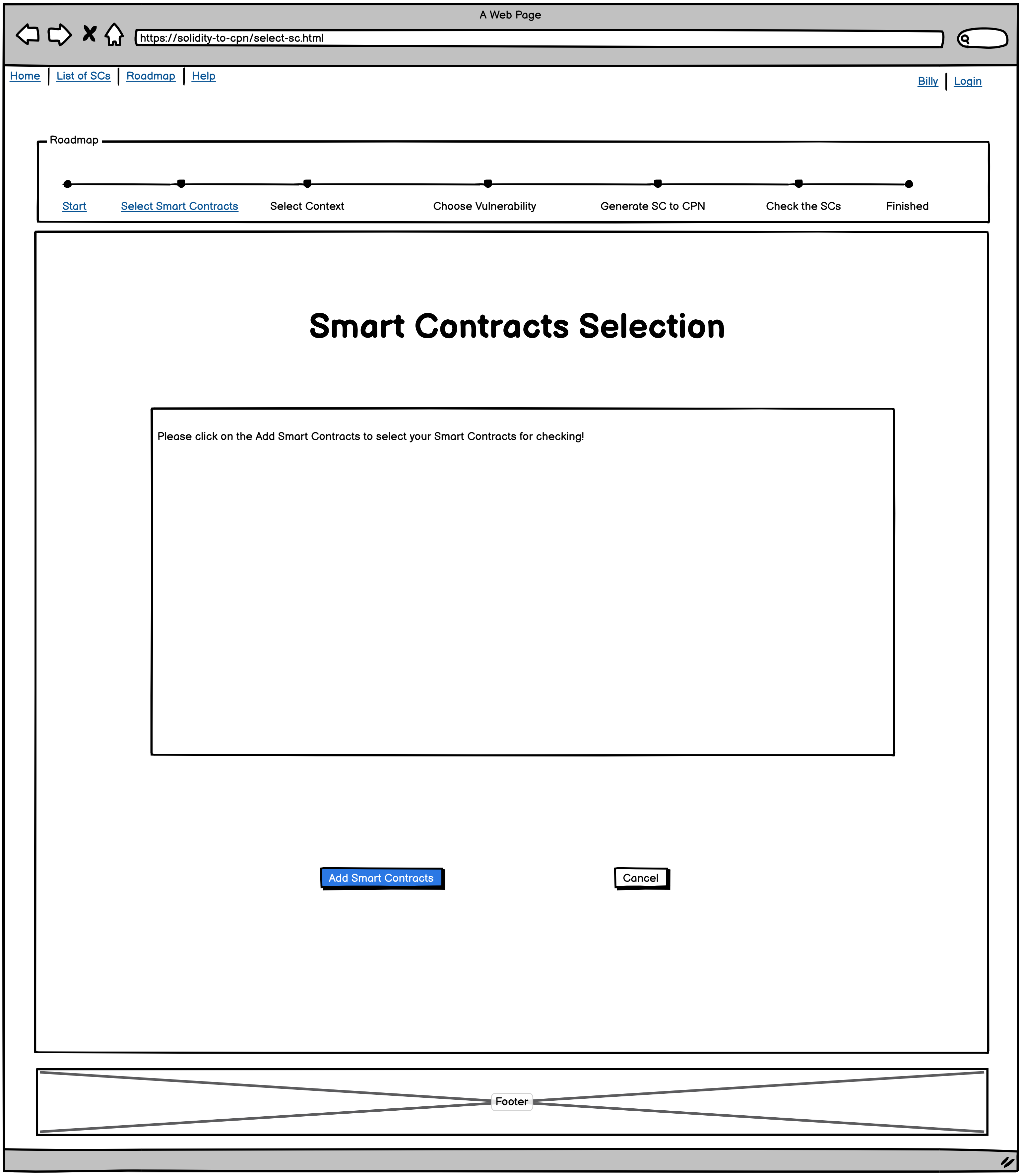
SolidityCPN Home

Common Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
5	SC5
6	SC6
7	SC7
...	...

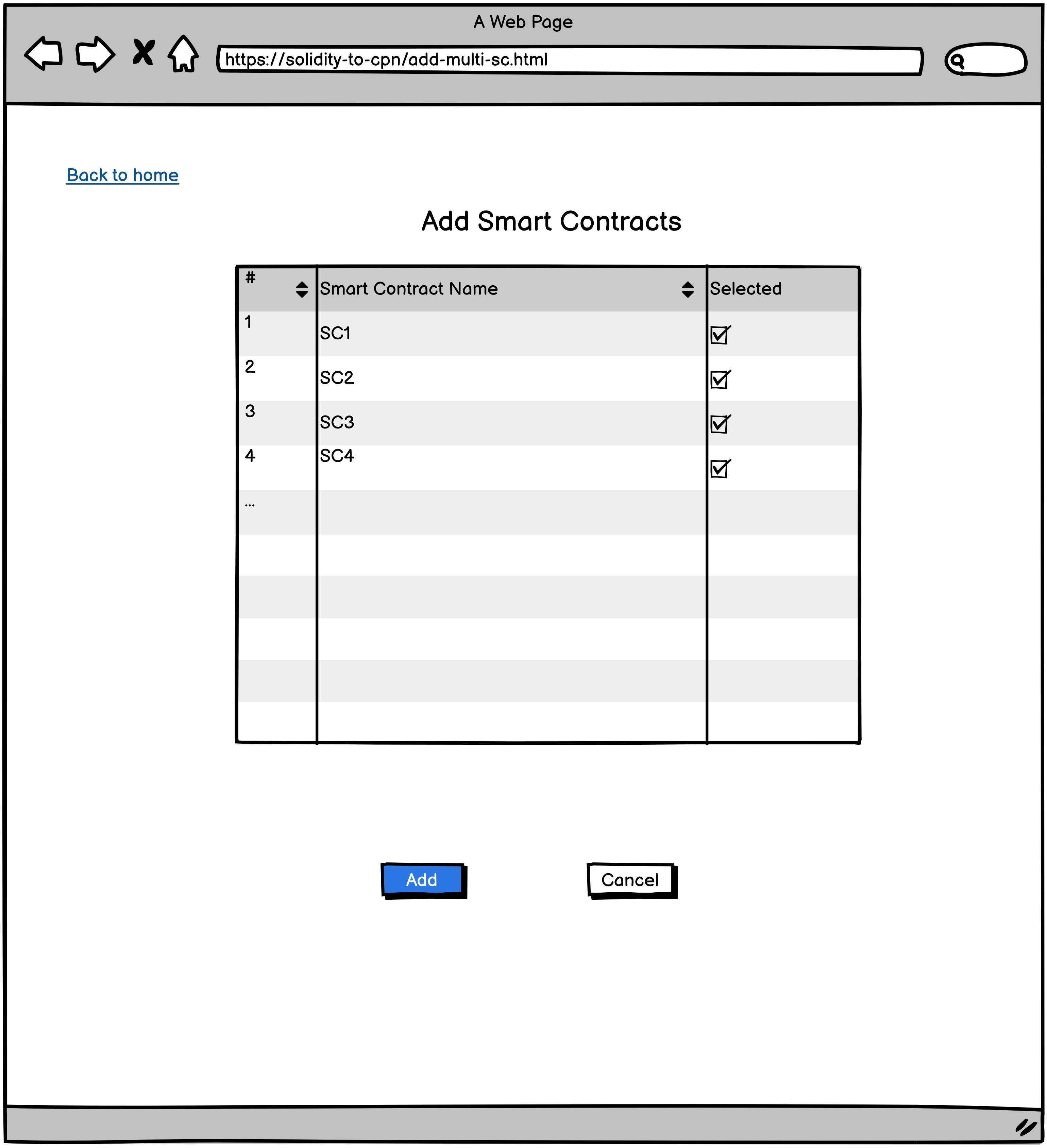
Private Smart Contracts

#	Smart Contract Name
1	SC1
2	SC2
3	SC3
4	SC4
...	...



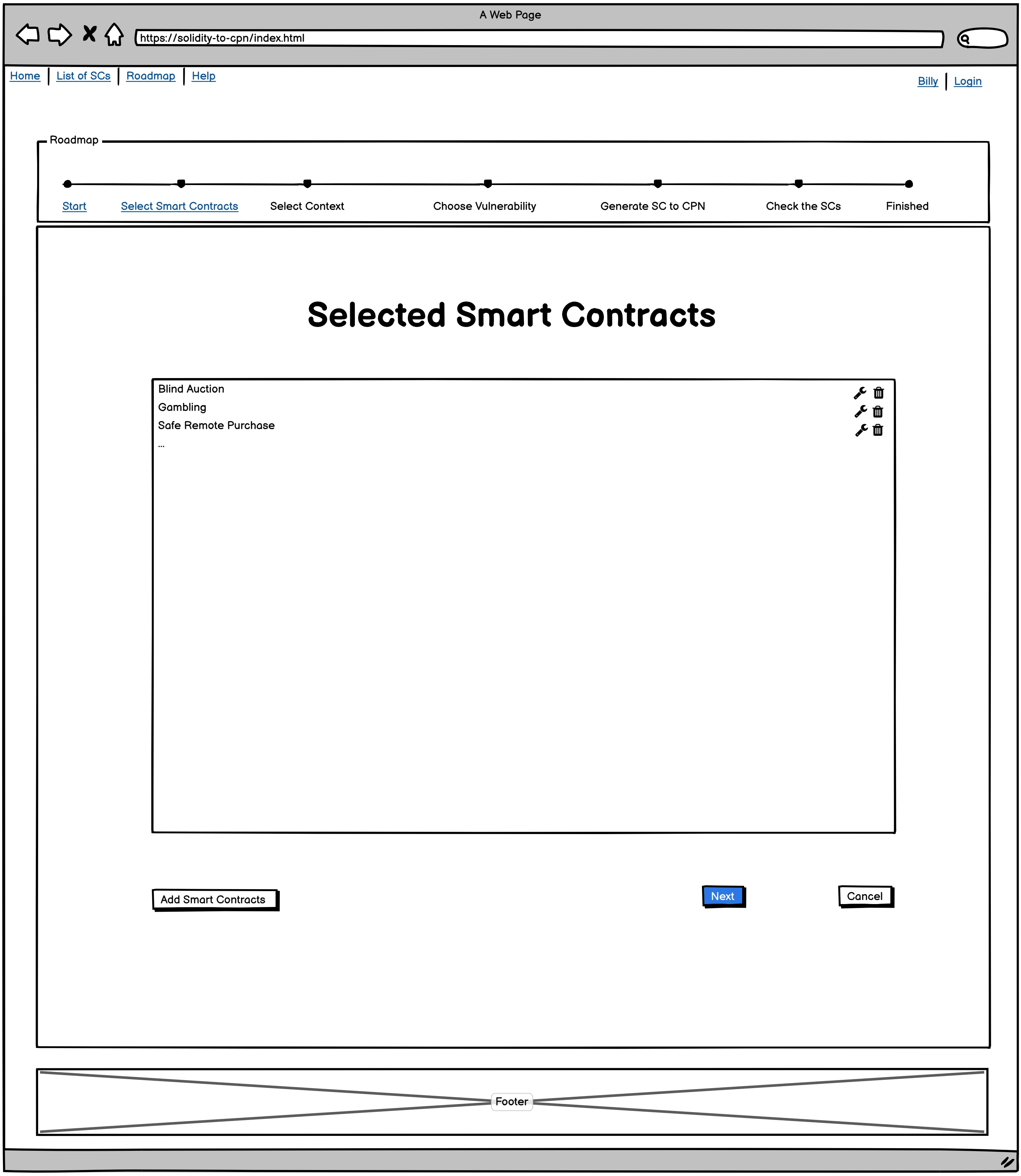
Smart Contracts Selection

Please click on the Add Smart Contracts to select your Smart Contracts for checking!



Add Smart Contracts

#	Smart Contract Name	Selected
1	SC1	☑
2	SC2	☑
3	SC3	☑
4	SC4	☑
...		



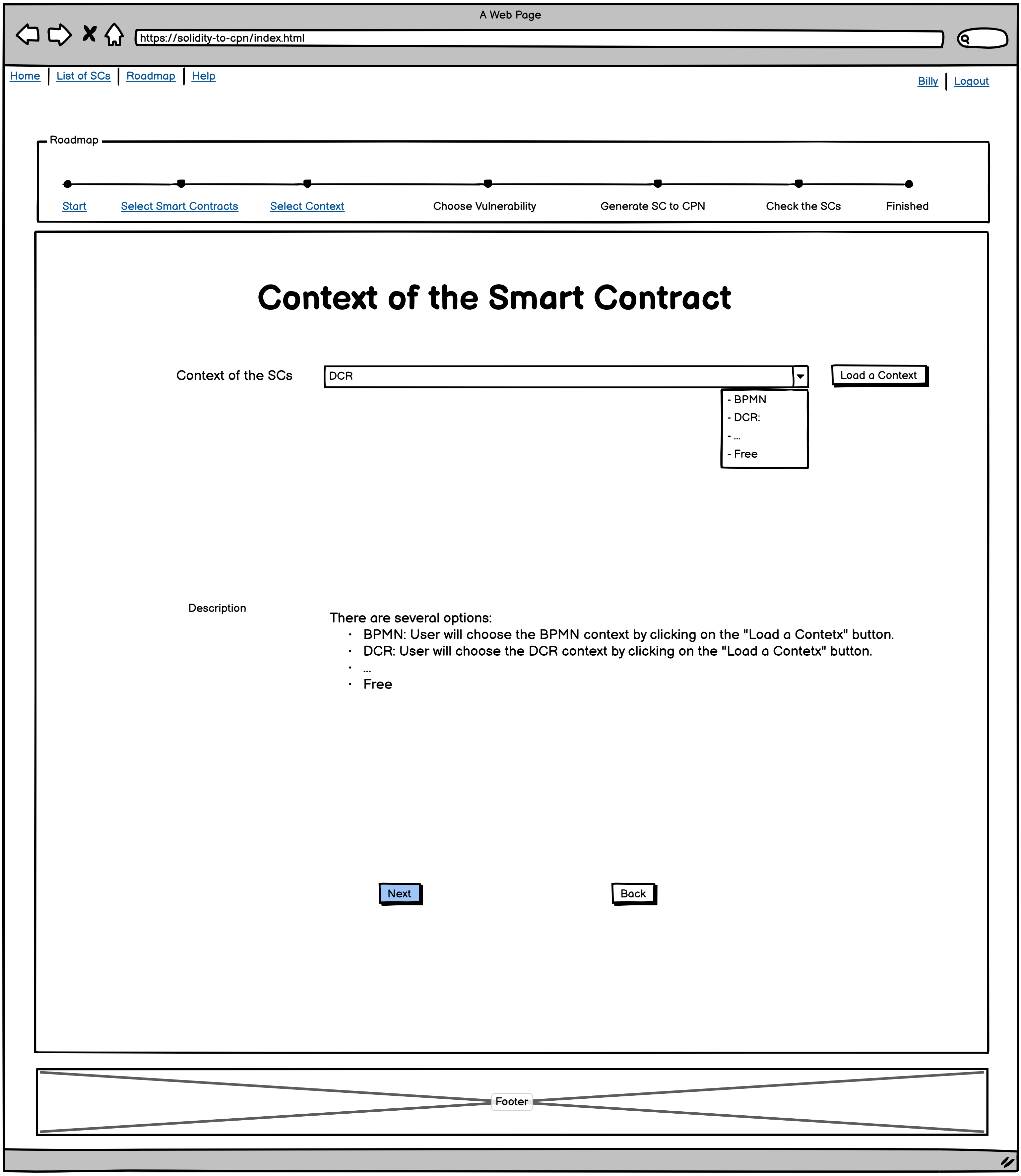
Selected Smart Contracts

Blind Auction

Gambling

Safe Remote Purchase

...



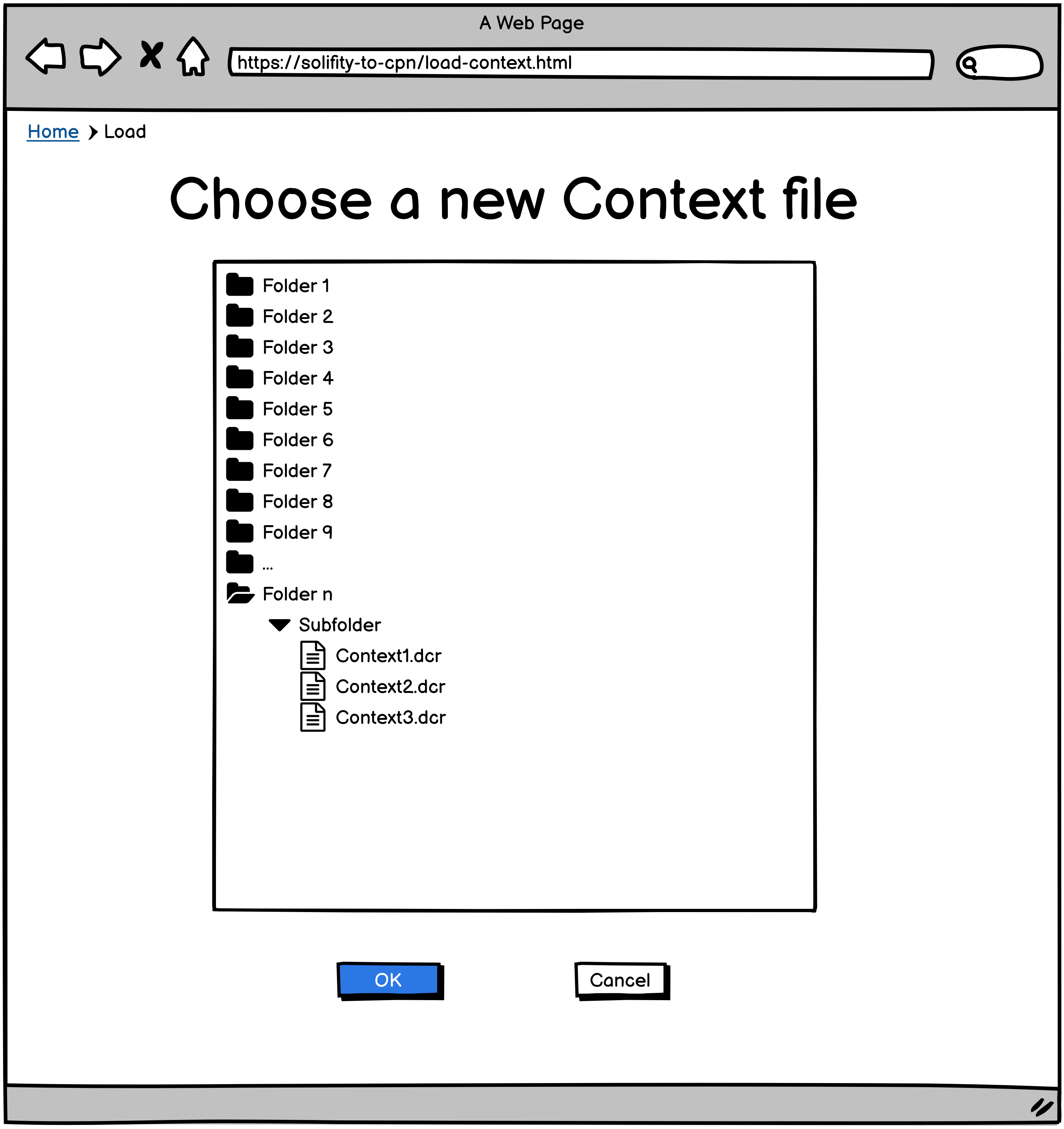
Context of the Smart Contract

Context of the SCs: DCR

Description

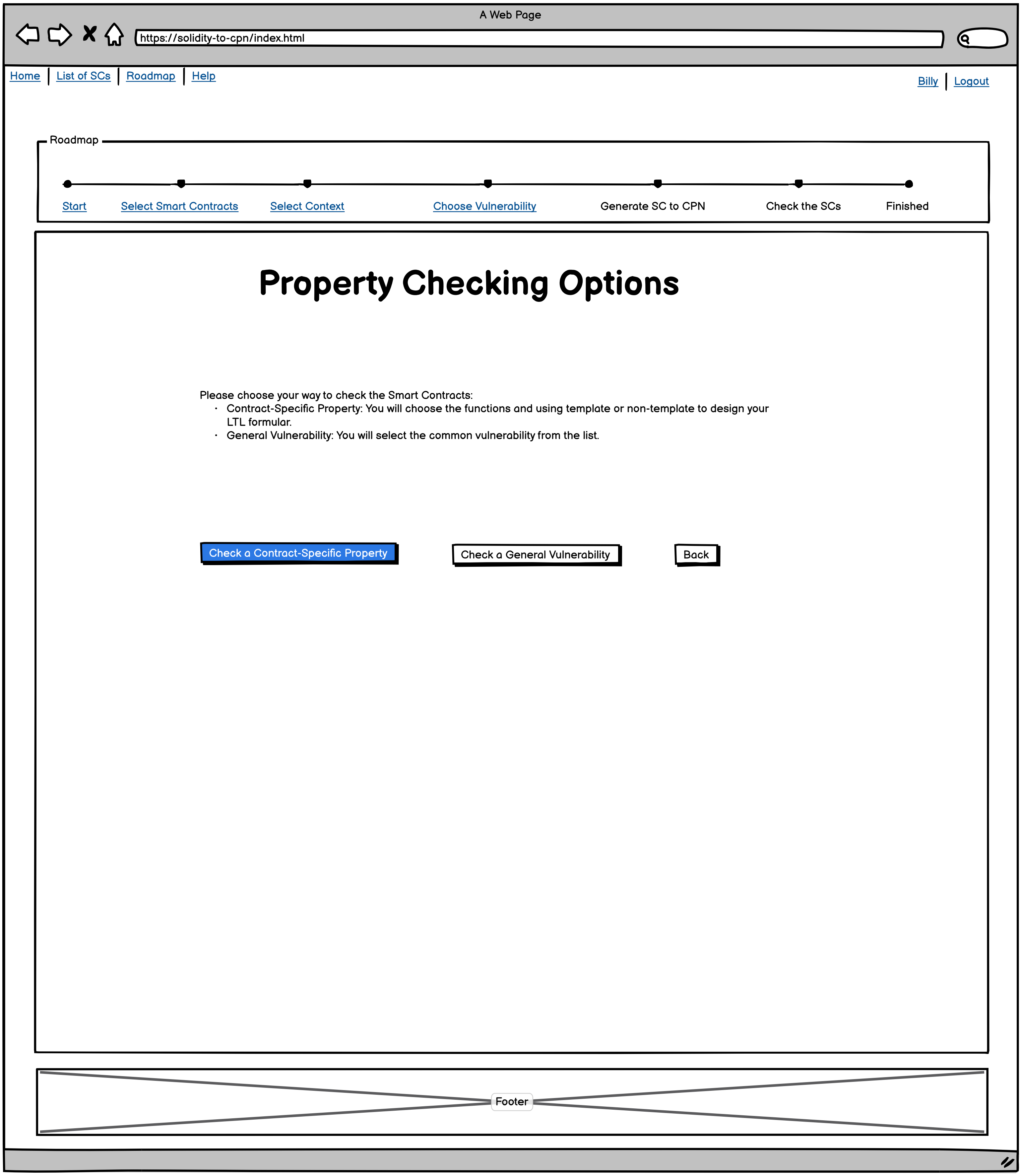
There are several options:

- BPMN: User will choose the BPMN context by clicking on the "Load a Contetx" button.
- DCR: User will choose the DCR context by clicking on the "Load a Contetx" button.
- ...
- Free



Choose a new Context file

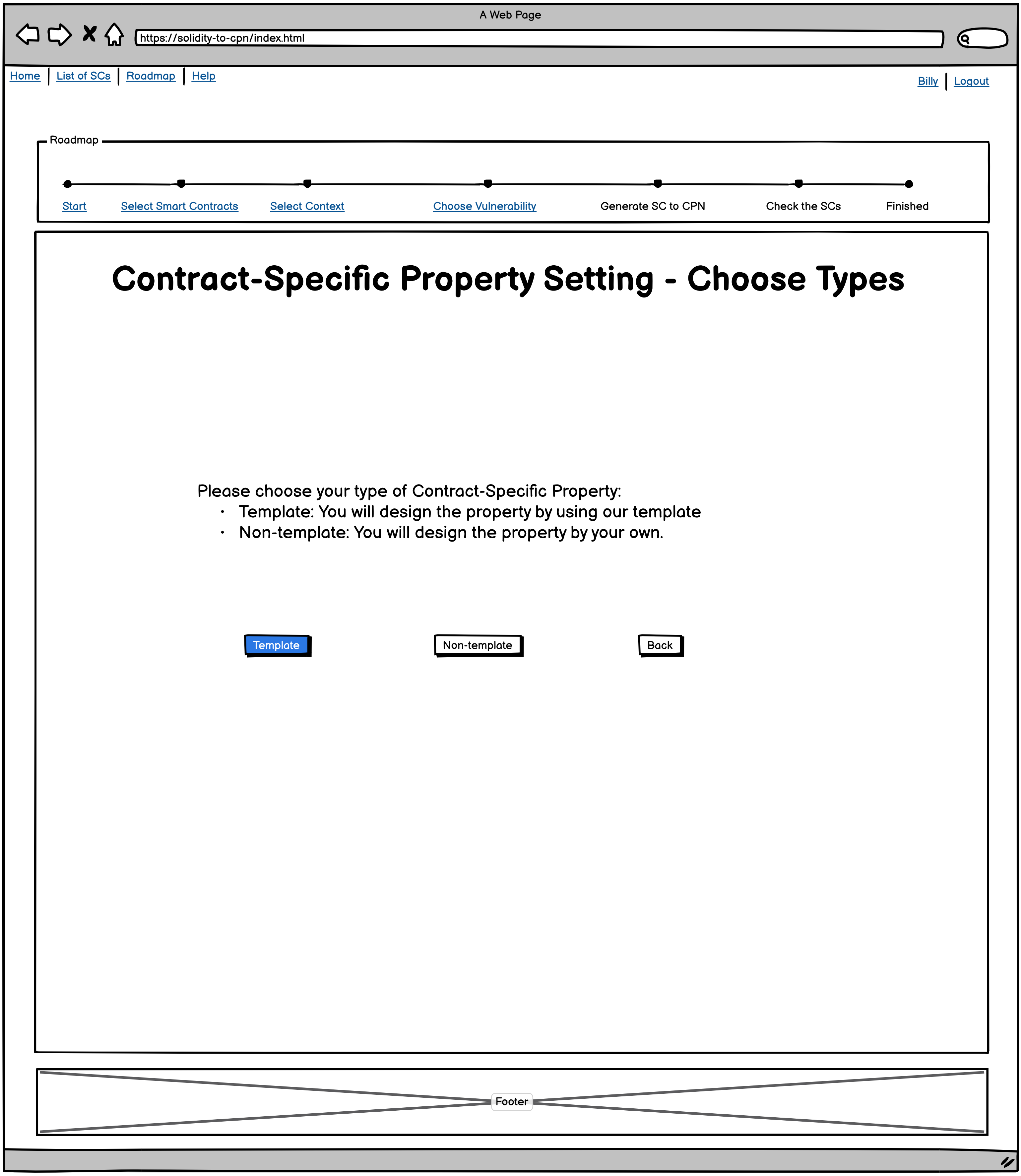
- Folder 1
- Folder 2
- Folder 3
- Folder 4
- Folder 5
- Folder 6
- Folder 7
- Folder 8
- Folder 9
- ...
- Folder n
  - ▼ Subfolder
    - Context1.dcr
    - Context2.dcr
    - Context3.dcr



Property Checking Options

Please choose your way to check the Smart Contracts:

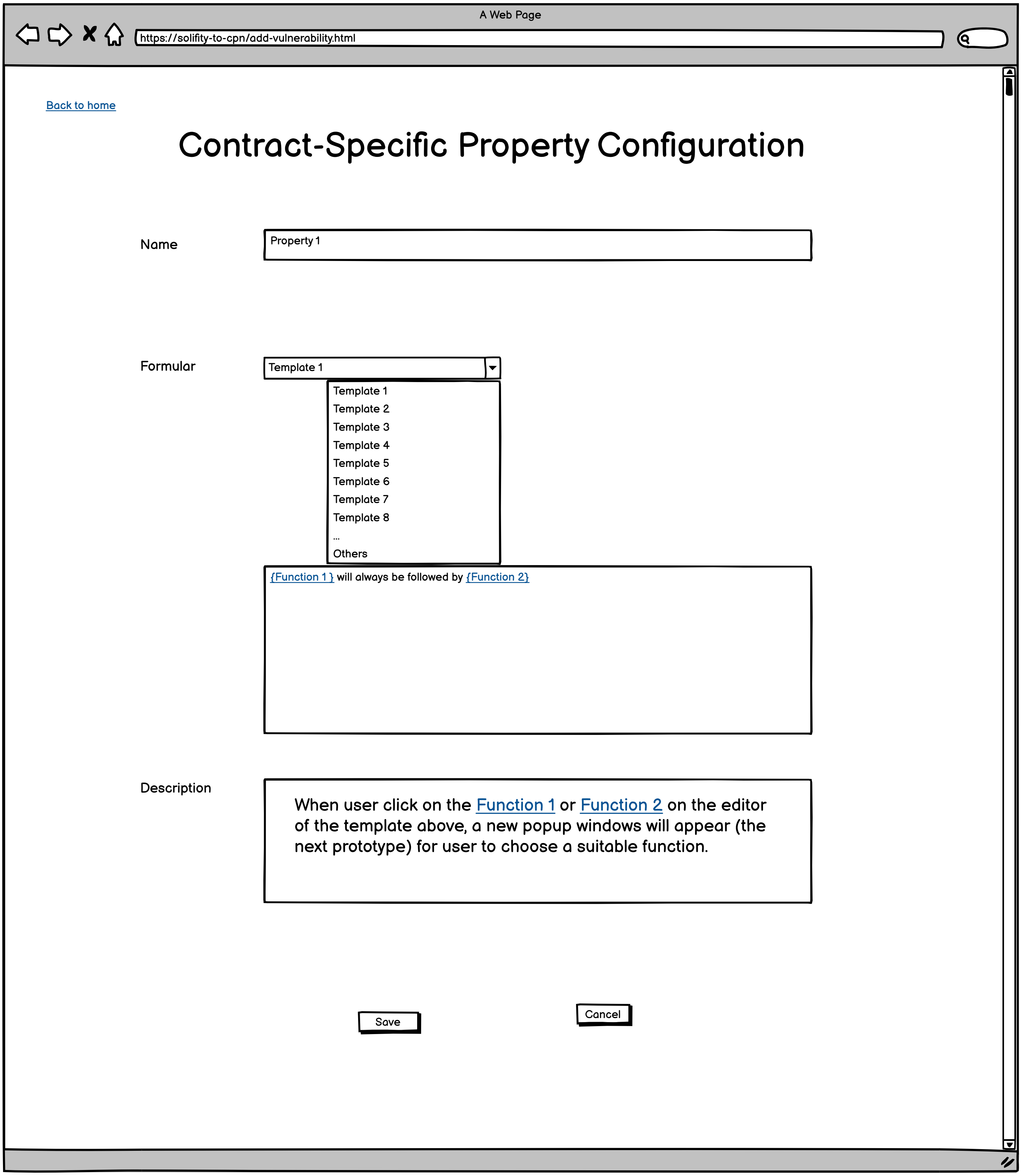
- Contract-Specific Property: You will choose the functions and using template or non-template to design your LTL formular.
- General Vulnerability: You will select the common vulnerability from the list.



Contract-Specific Property Setting - Choose Types

Please choose your type of Contract-Specific Property:

- Template: You will design the property by using our template
- Non-template: You will design the property by your own.



A Web Page

https://solifity-to-cpn/add-vulnerability.html

Back to home

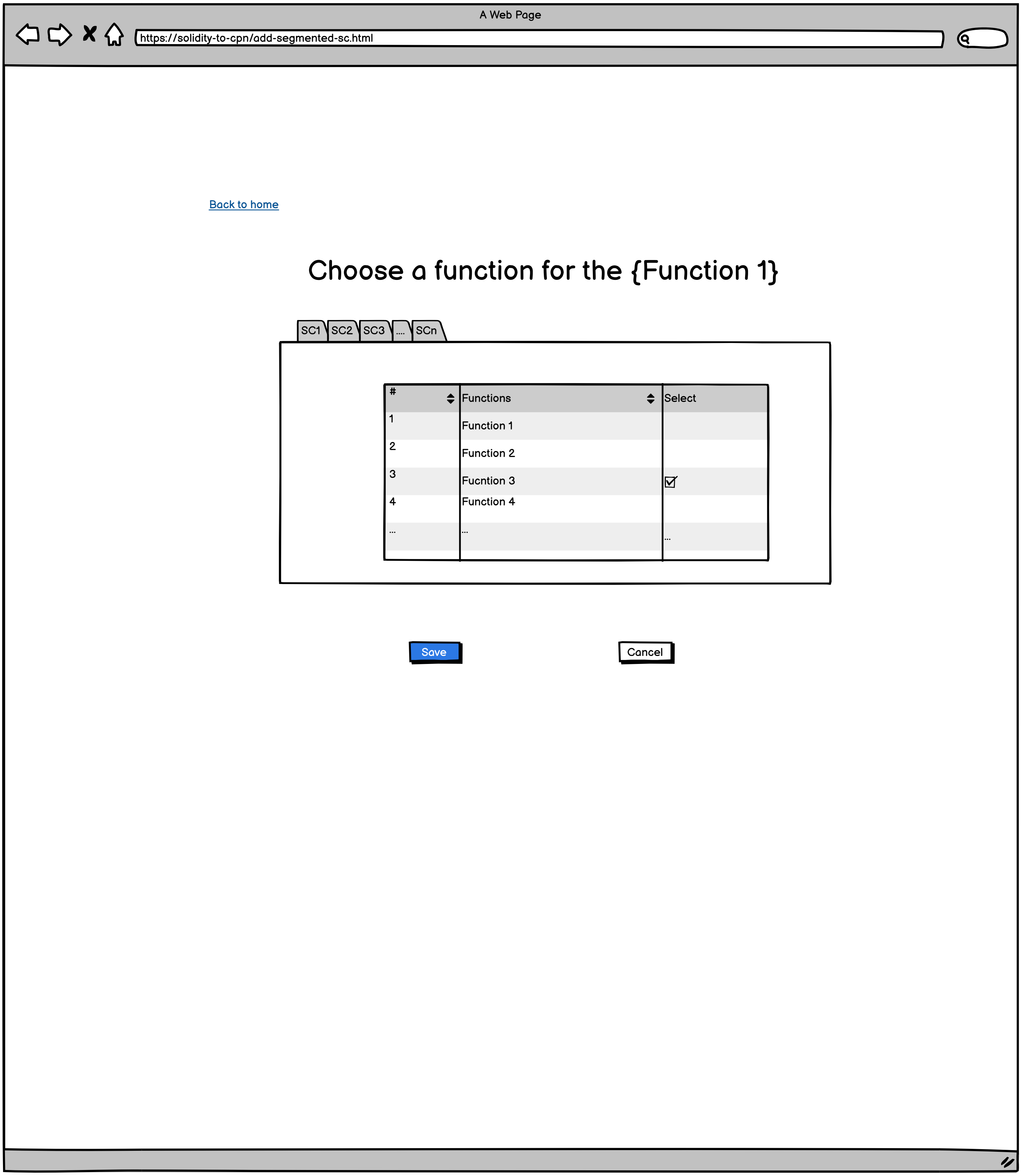
Contract-Specific Property Configuration

Name: Property 1

Formular: Template 1

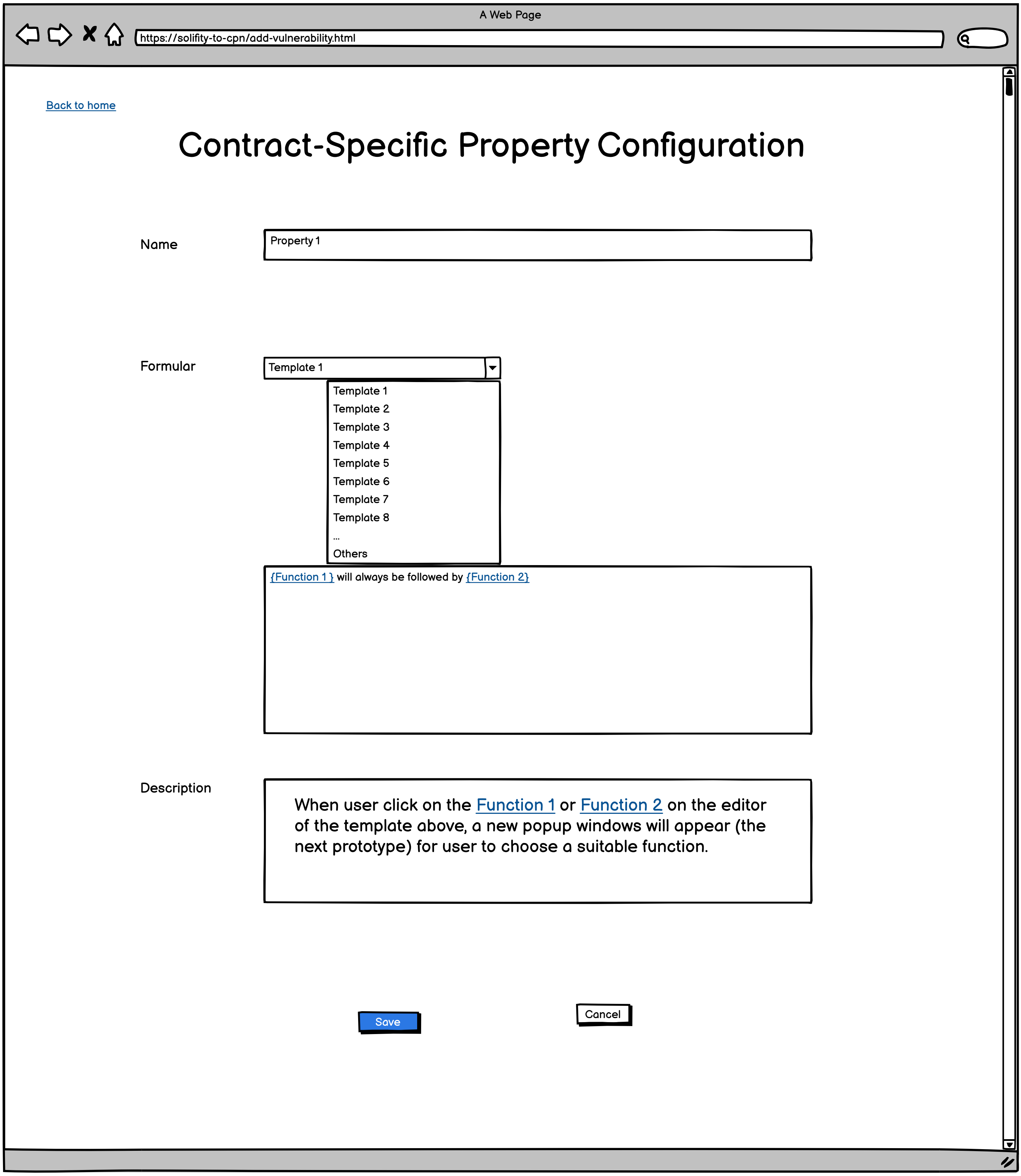
{Function 1 } will always be followed by {Function 2}

Description: When user click on the Function 1 or Function 2 on the editor of the template above, a new popup windows will appear (the next prototype) for user to choose a suitable function.



Choose a function for the {Function 1}

#	Functions	Select
1	Function 1	
2	Function 2	
3	Fucntion 3	☑
4	Function 4	
...	...	...



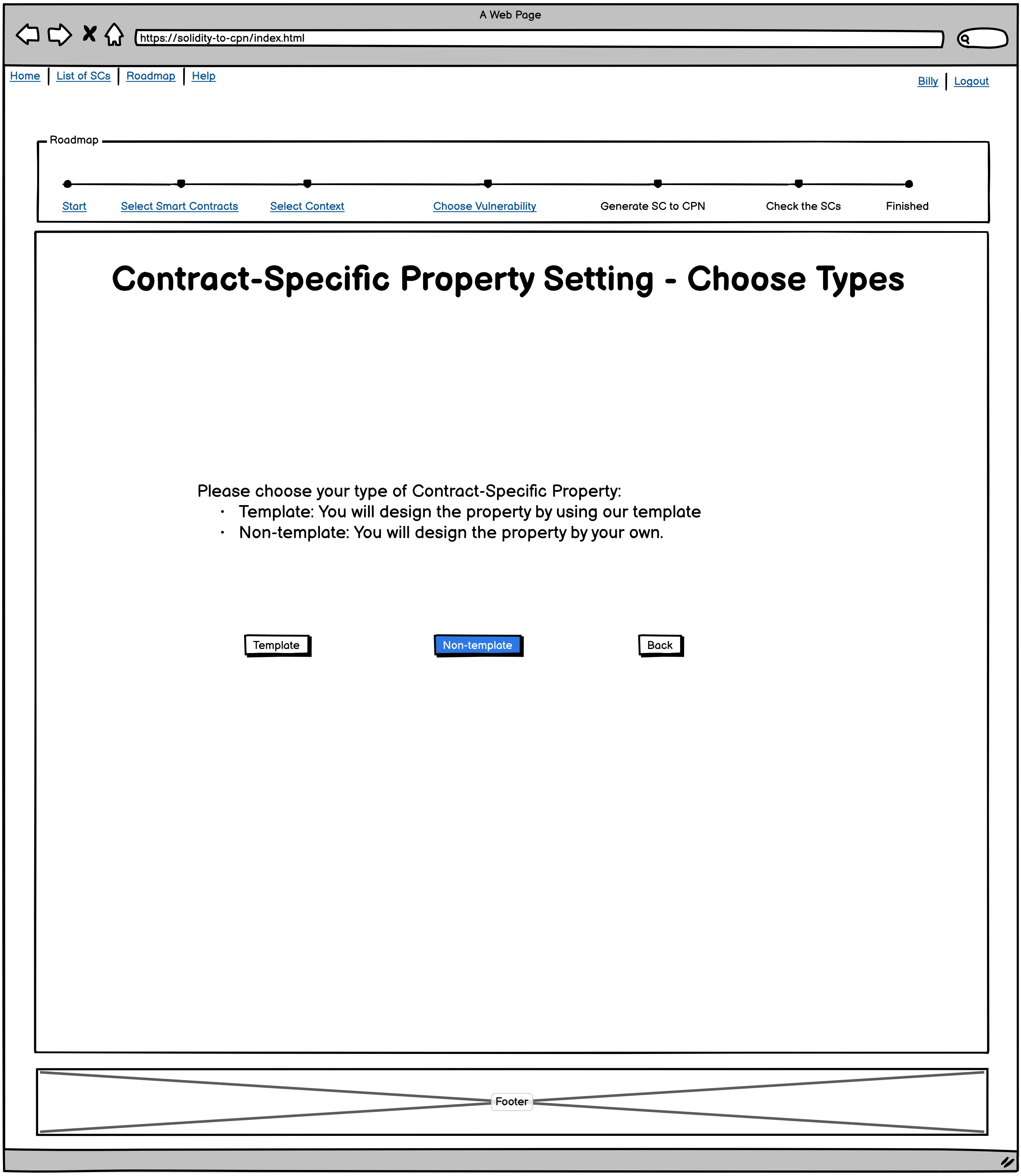
Contract-Specific Property Configuration

Name: Property 1

Formular: Template 1

{Function 1 } will always be followed by {Function 2}

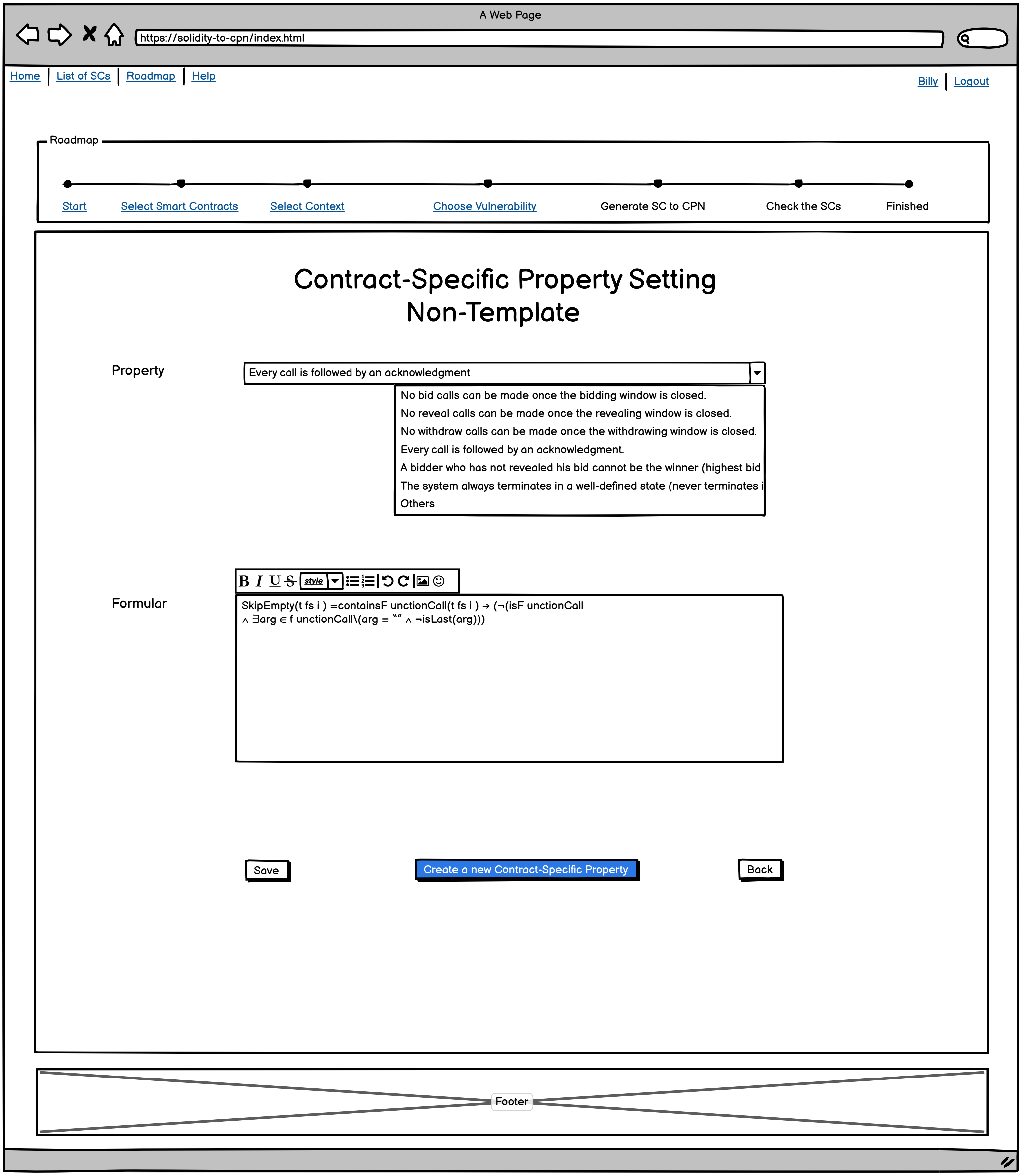
Description: When user click on the Function 1 or Function 2 on the editor of the template above, a new popup windows will appear (the next prototype) for user to choose a suitable function.



Contract-Specific Property Setting - Choose Types

Please choose your type of Contract-Specific Property:

- Template: You will design the property by using our template
- Non-template: You will design the property by your own.



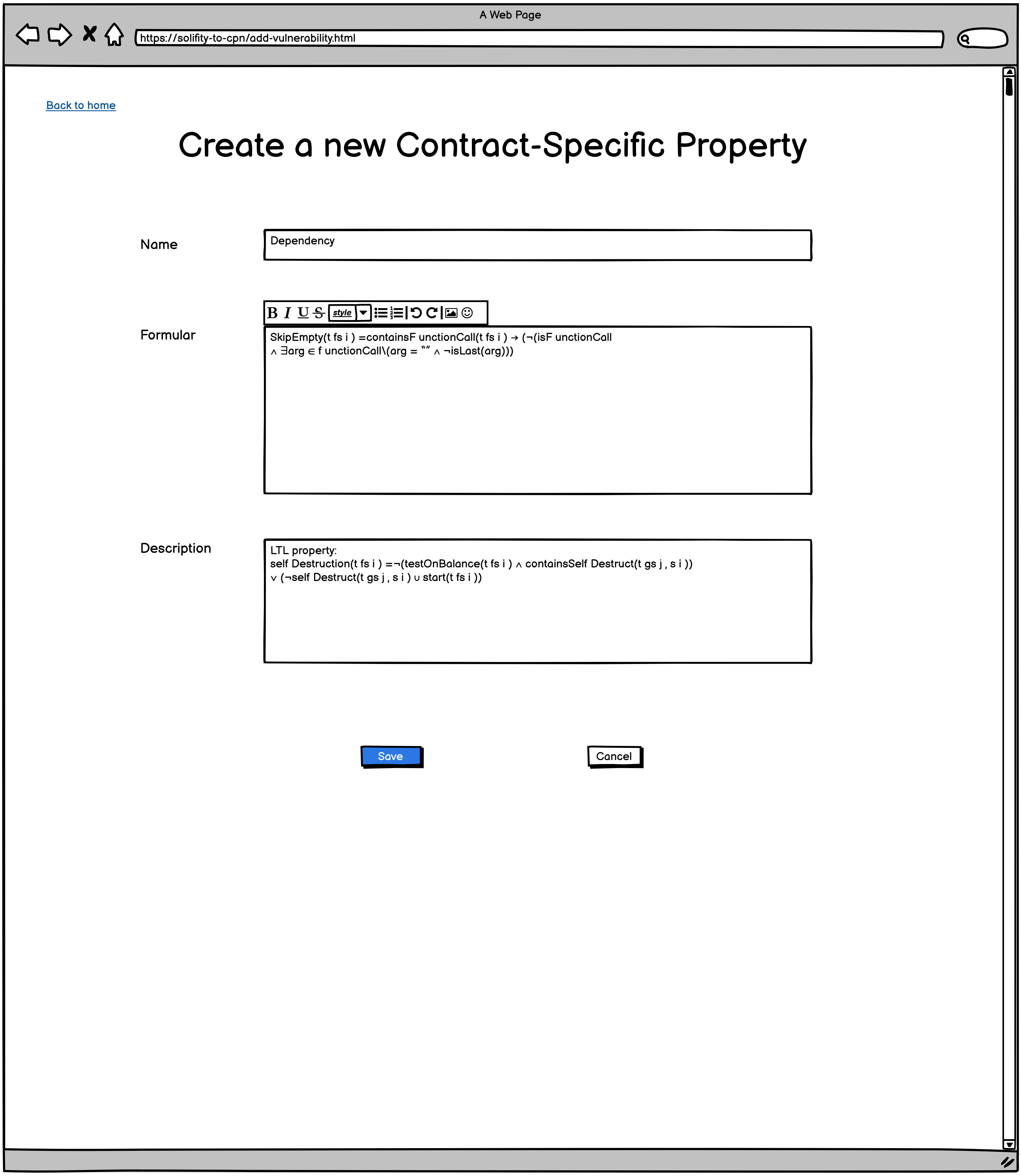
Contract-Specific Property Setting
Non-Template

Property: Every call is followed by an acknowledgment

- No bid calls can be made once the bidding window is closed.
- No reveal calls can be made once the revealing window is closed.
- No withdraw calls can be made once the withdrawing window is closed.
- Every call is followed by an acknowledgment.
- A bidder who has not revealed his bid cannot be the winner (highest bid
- The system always terminates in a well-defined state (never terminates i
- Others

Formular:

SkipEmpty(t fs i) =containsF unctionCall(t fs i) → (¬(isF unctionCall
∧ ∃arg ∈ f unctionCall\(arg = “” ∧ ¬isLast(arg)))



Create a new Contract-Specific Property

Name

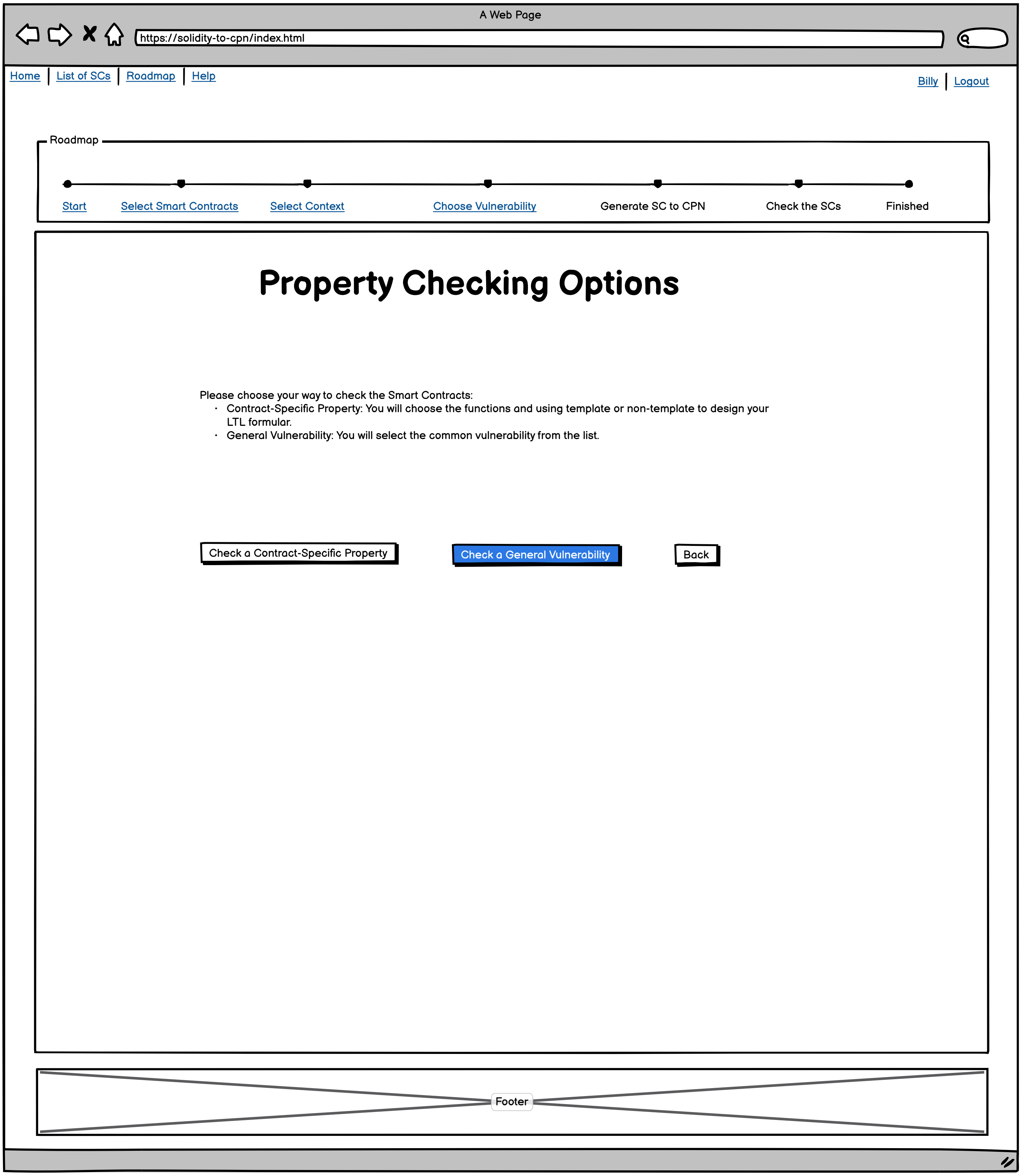
Dependency

Formular

SkipEmpty(t fs i) =containsF unctionCall(t fs i) → (¬(isF unctionCall
∧ ∃arg ∈ f unctionCall\(arg = “” ∧ ¬isLast(arg)))

Description

LTL property:
self Destruction(t fs i) =¬(testOnBalance(t fs i) ∧ containsSelf Destruct(t gs j , s i))
∨ (¬self Destruct(t gs j , s i) ∪ start(t fs i))

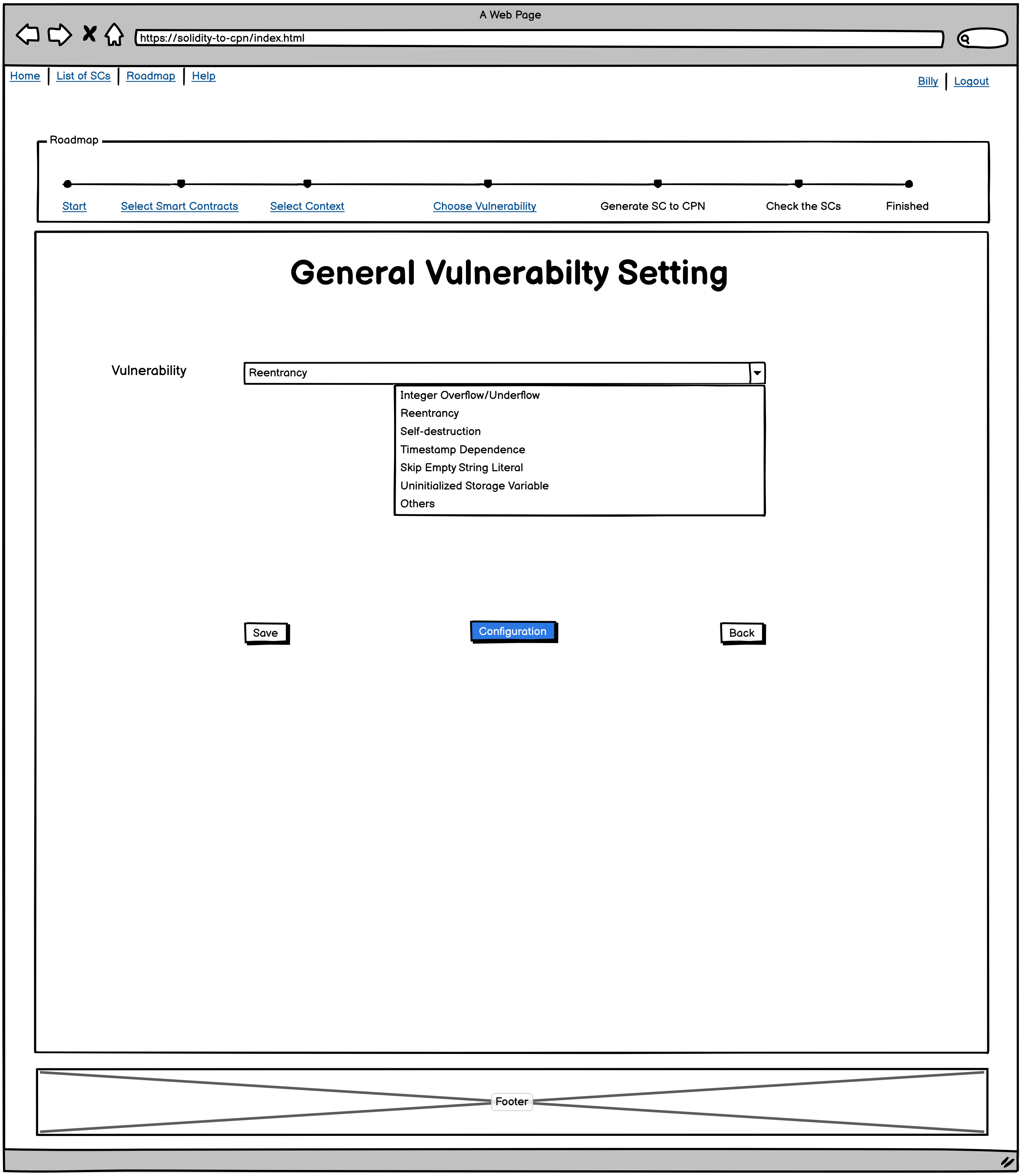


Property Checking Options

Please choose your way to check the Smart Contracts:

- Contract-Specific Property: You will choose the functions and using template or non-template to design your LTL formular.
- General Vulnerability: You will select the common vulnerability from the list.

Check a Contract-Specific Property
Check a General Vulnerability
Back
Footer

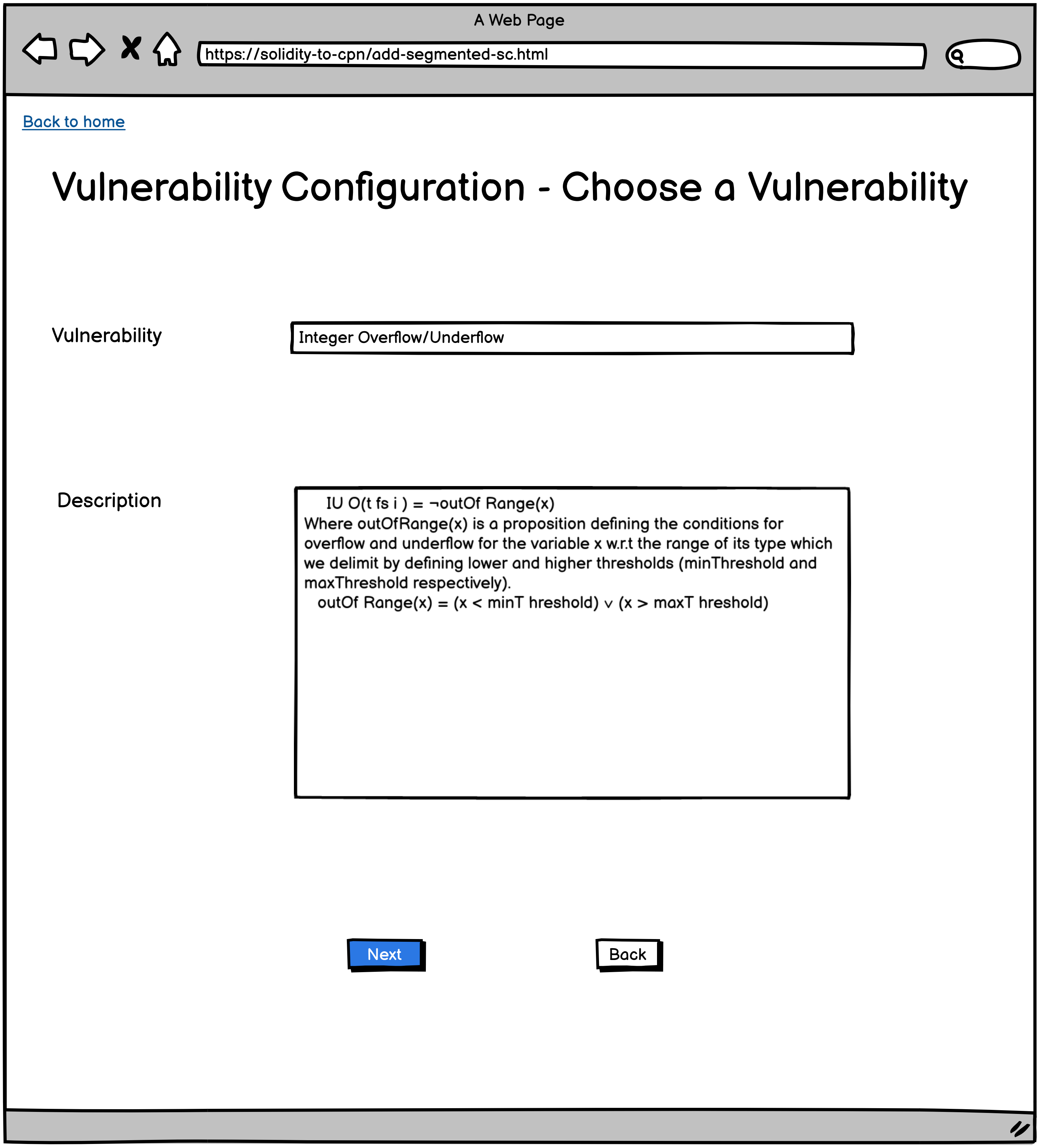


A Web Page

https://solidity-to-cpn/index.html

General Vulnerabilty Setting

Vulnerability: Reentrancy

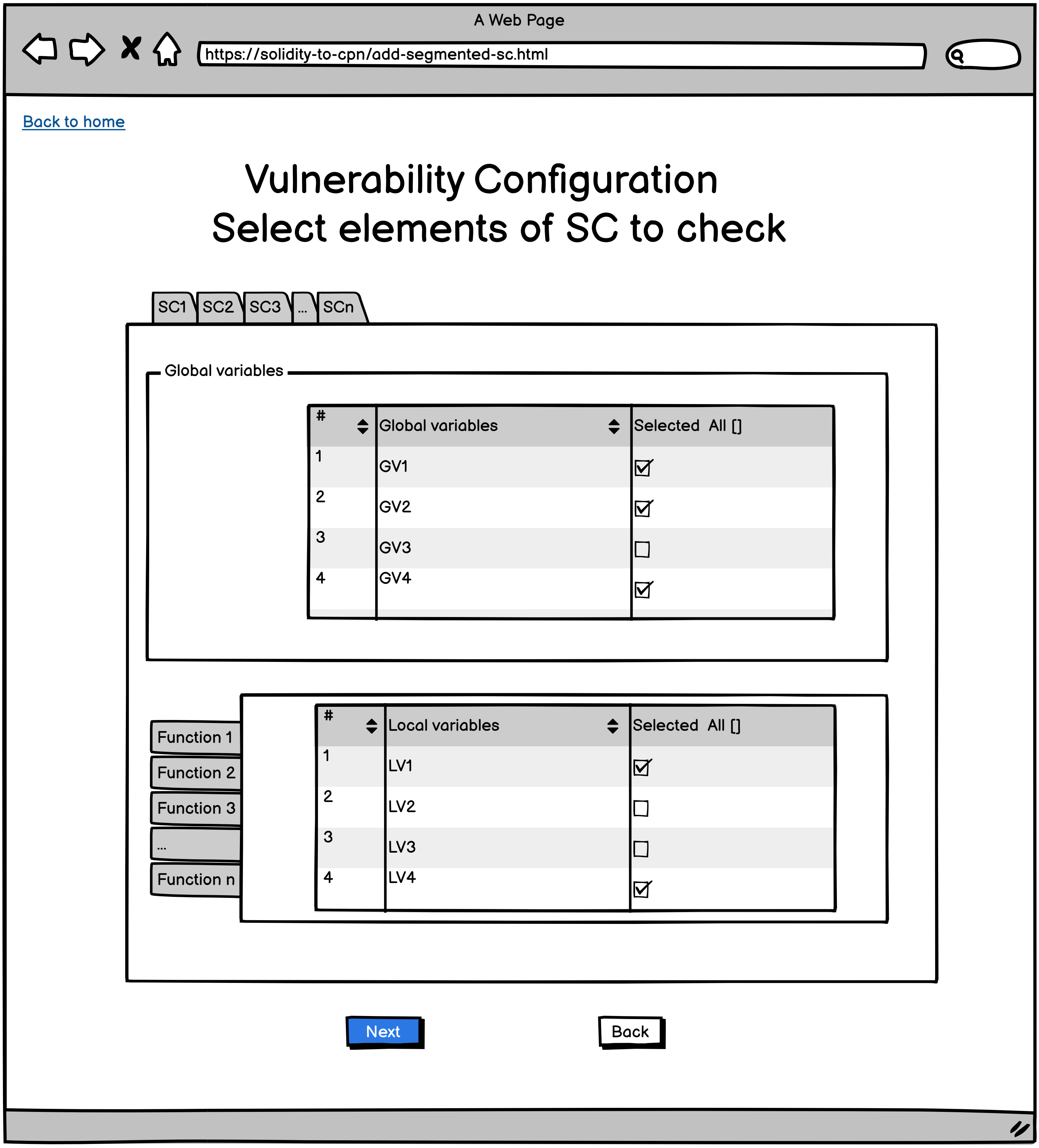


Vulnerability Configuration - Choose a Vulnerability

Vulnerability: Integer Overflow/Underflow

Description:

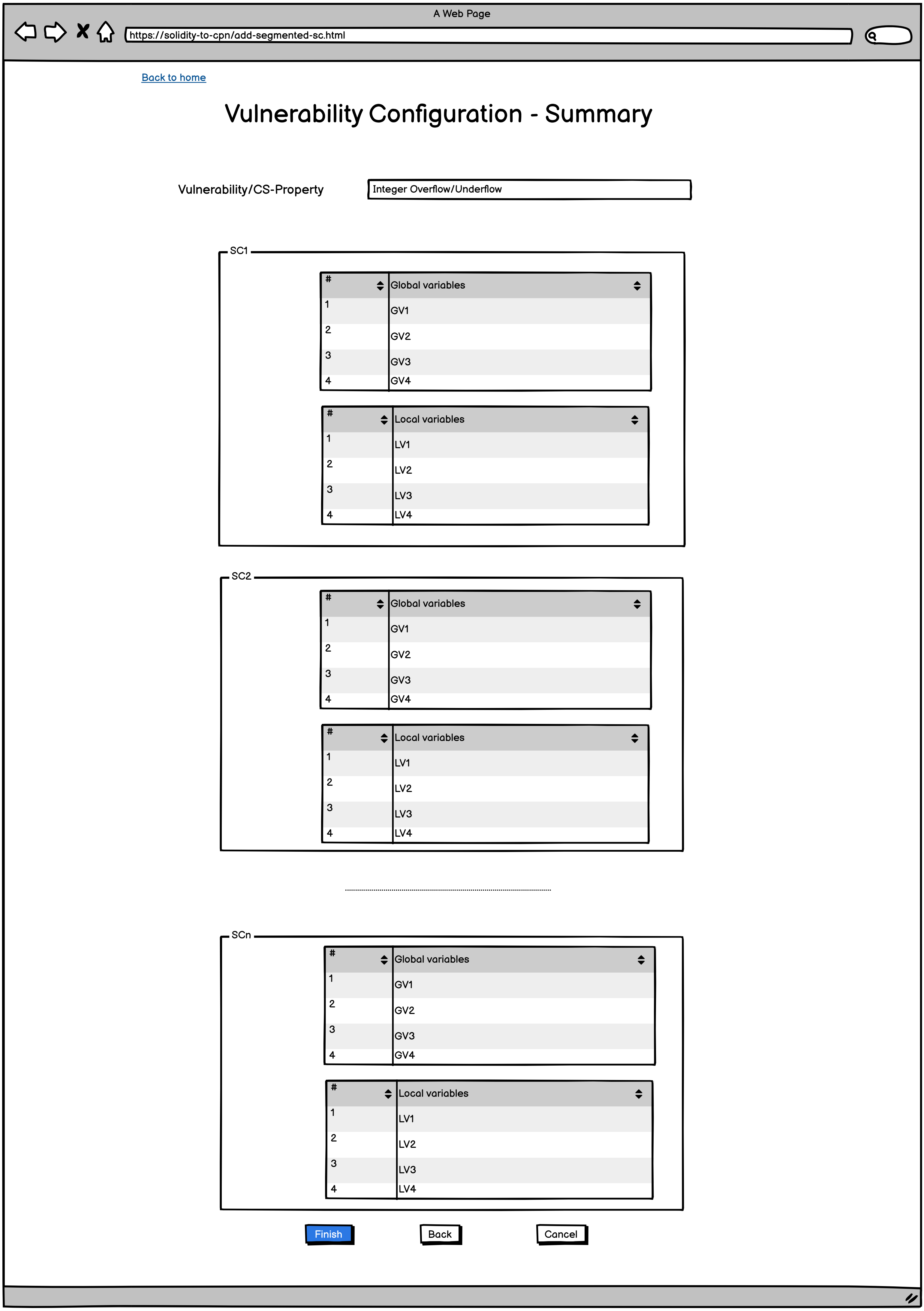
IU O(t fs i) = ¬outOf Range(x)
Where outOfRange(x) is a proposition defining the conditions for overflow and underflow for the variable x w.r.t the range of its type which we delimit by defining lower and higher thresholds (minThreshold and maxThreshold respectively).
outOf Range(x) = (x < minT hreshold) ∨ (x > maxT hreshold)



Vulnerability Configuration
Select elements of SC to check

#	Global variables	Selected All []
1	GV1	☑
2	GV2	☑
3	GV3	□
4	GV4	☑

#	Local variables	Selected All []
1	LV1	☑
2	LV2	□
3	LV3	□
4	LV4	☑



Vulnerability Configuration - Summary

Vulnerability/CS-Property: Integer Overflow/Underflow

SC1

#	Global variables
1	GV1
2	GV2
3	GV3
4	GV4

#	Local variables
1	LV1
2	LV2
3	LV3
4	LV4

SC2

#	Global variables
1	GV1
2	GV2
3	GV3
4	GV4

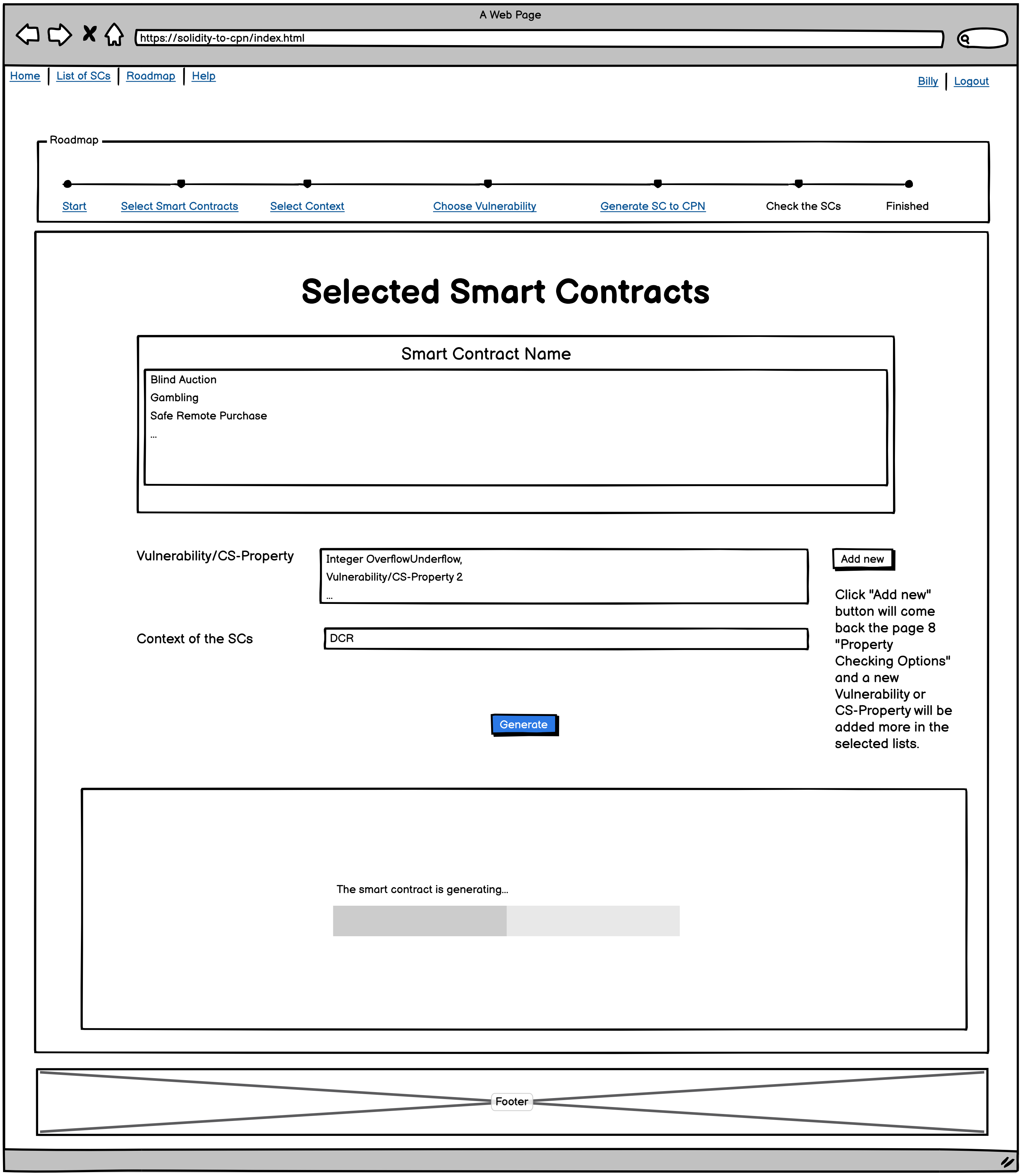
#	Local variables
1	LV1
2	LV2
3	LV3
4	LV4

....

SCn

#	Global variables
1	GV1
2	GV2
3	GV3
4	GV4

#	Local variables
1	LV1
2	LV2
3	LV3
4	LV4



Selected Smart Contracts

Smart Contract Name

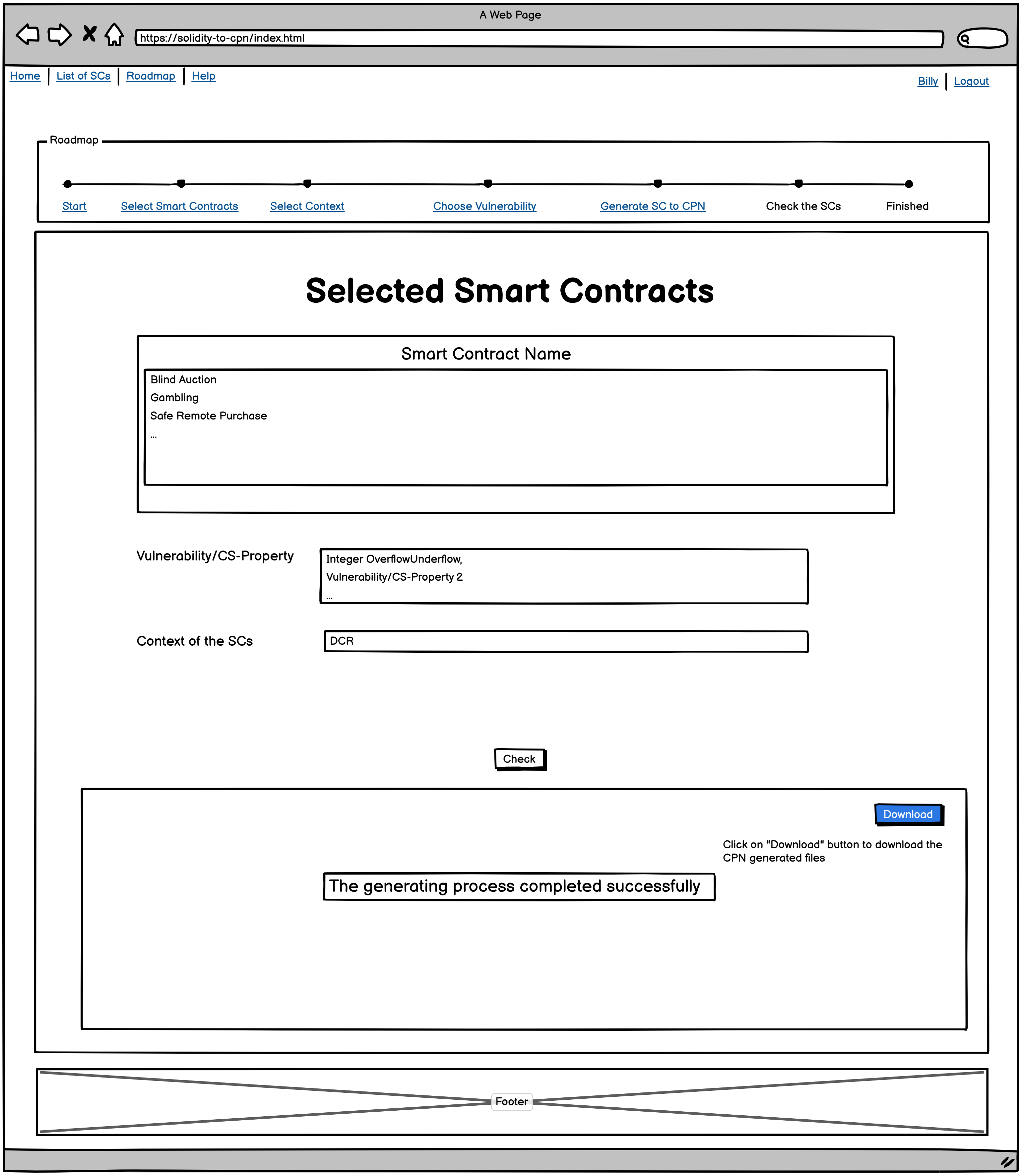
Blind Auction
Gambling
Safe Remote Purchase
...

Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

Click "Add new" button will come back the page 8 "Property Checking Options" and a new Vulnerability or CS-Property will be added more in the selected lists.

The smart contract is generating...



Selected Smart Contracts

Smart Contract Name

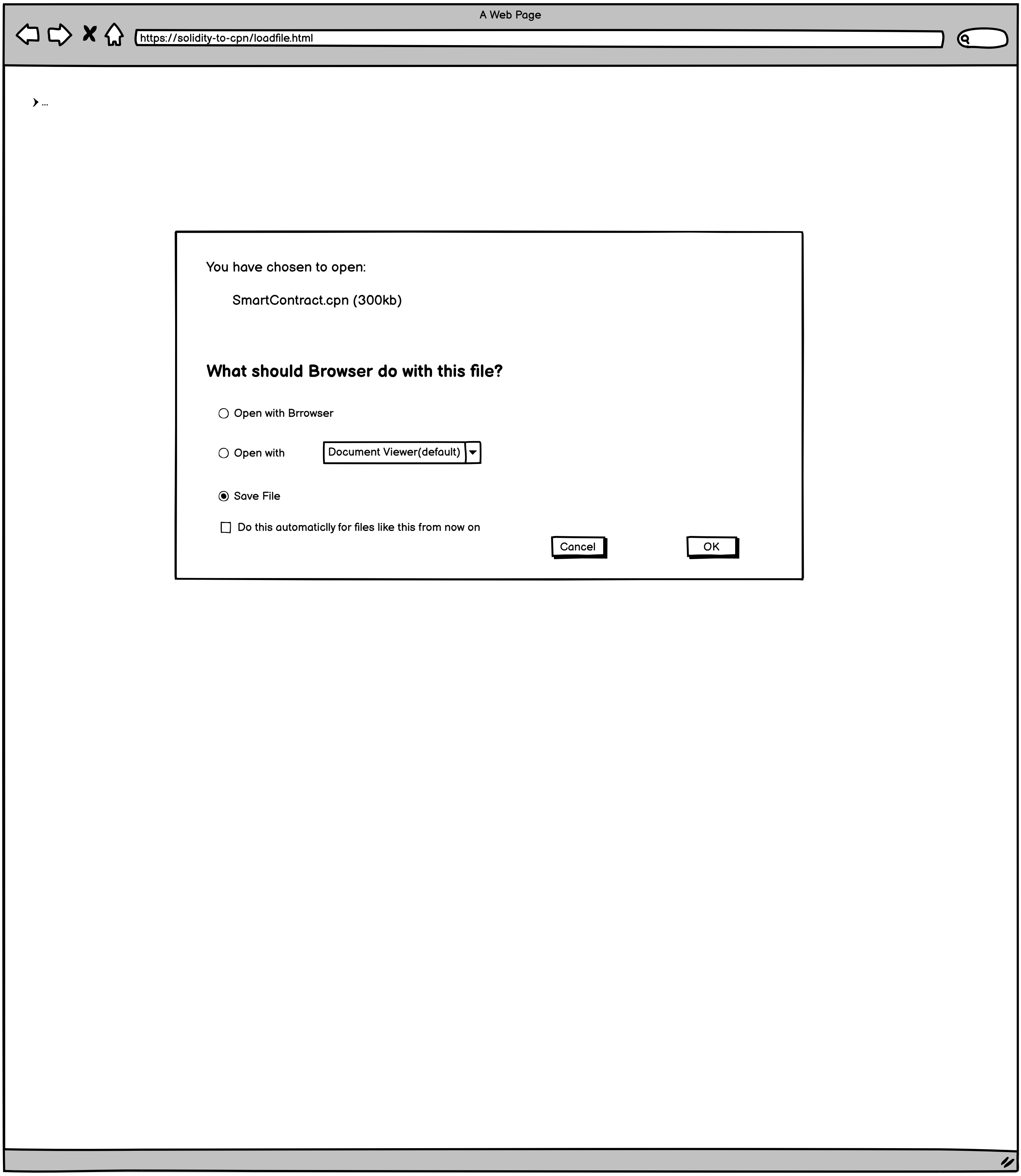
Blind Auction
Gambling
Safe Remote Purchase
...

Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

Click on "Download" button to download the CPN generated files

The generating process completed successfully



You have chosen to open:

SmartContract.cpn (300kb)

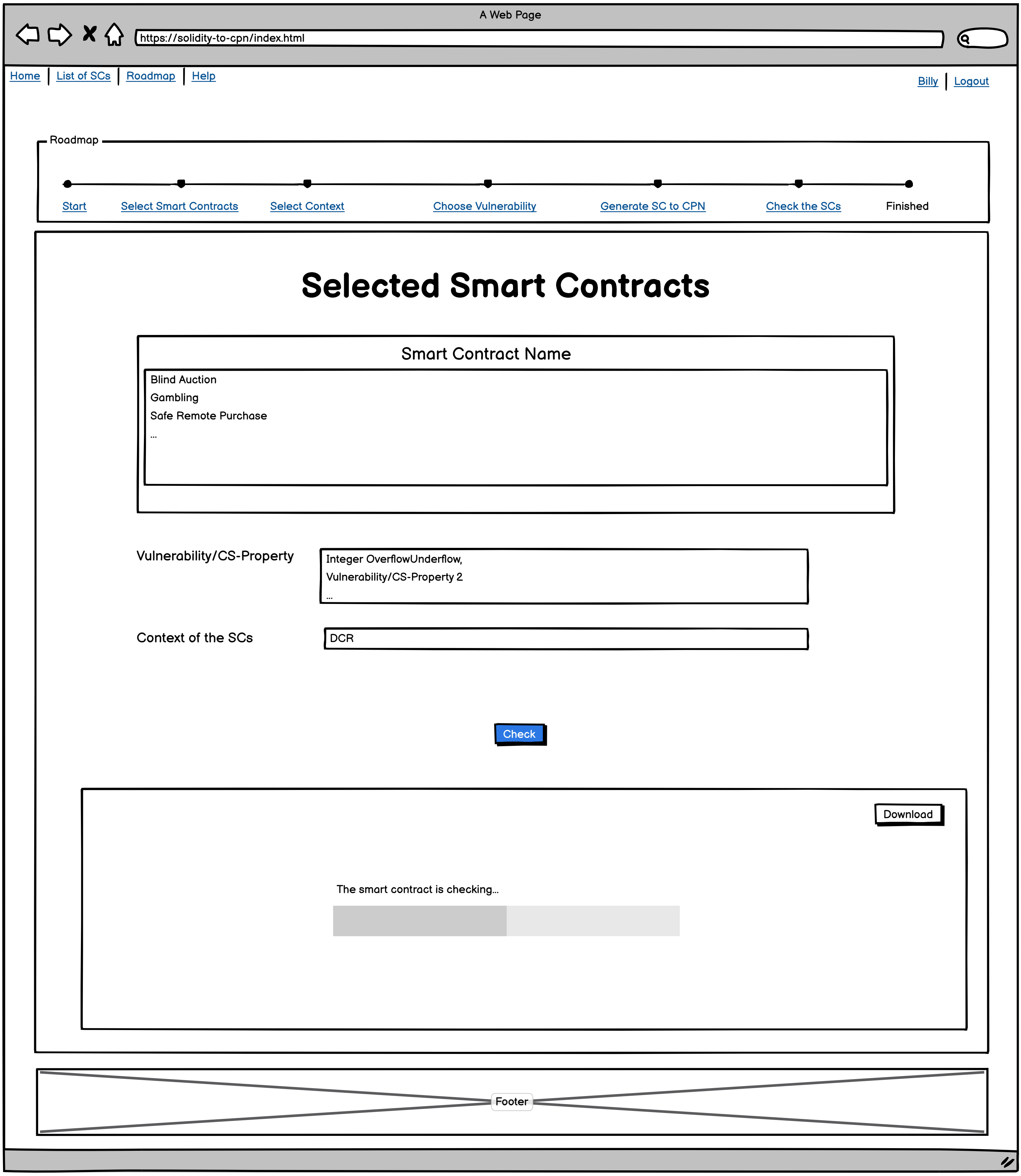
What should Browser do with this file?

○ Open with Brrowser

○ Open with Document Viewer(default) ▾

● Save File

□ Do this automaticlly for files like this from now on



Selected Smart Contracts

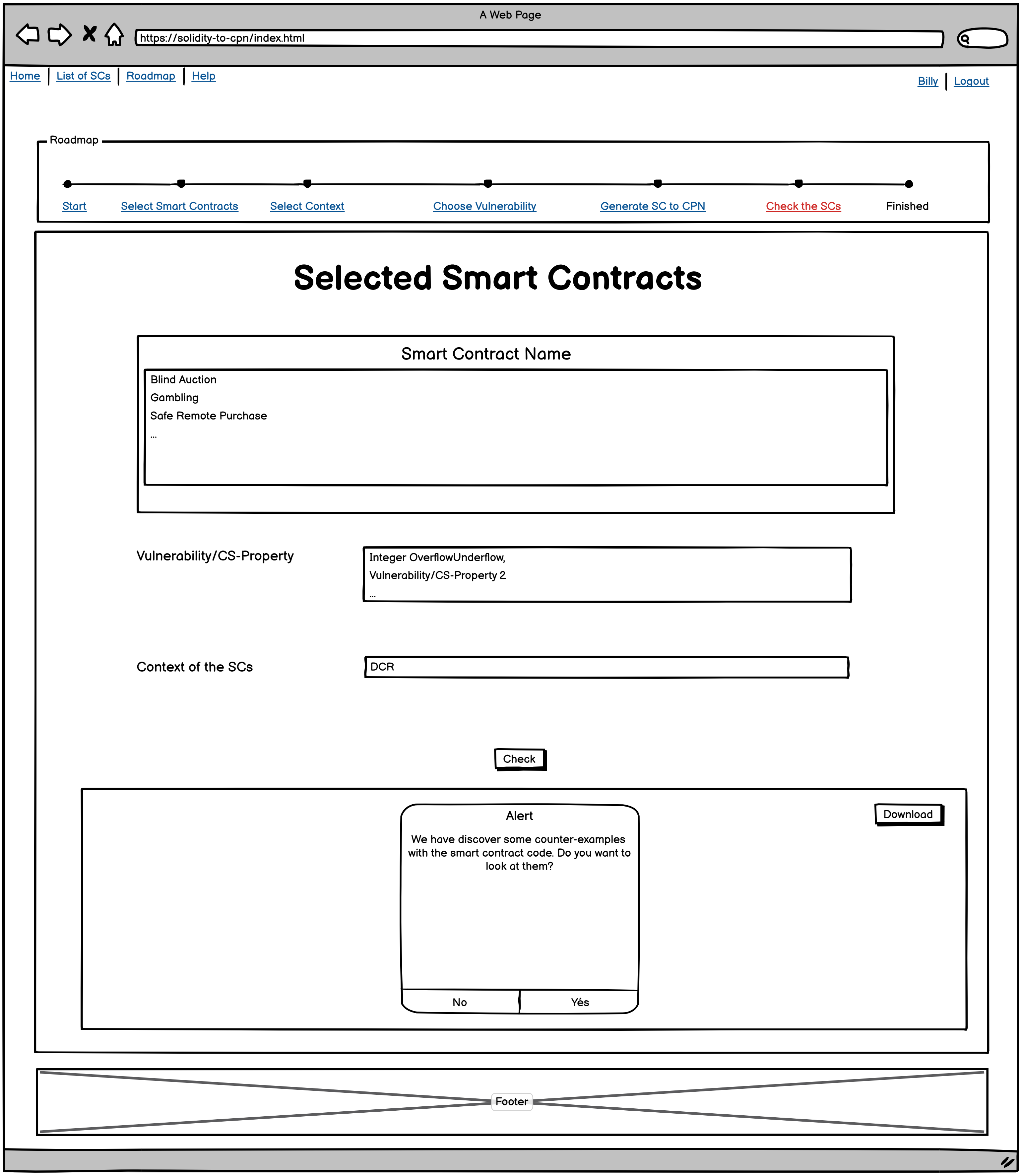
Smart Contract Name

Blind Auction
Gambling
Safe Remote Purchase
...

Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

The smart contract is checking...



Selected Smart Contracts

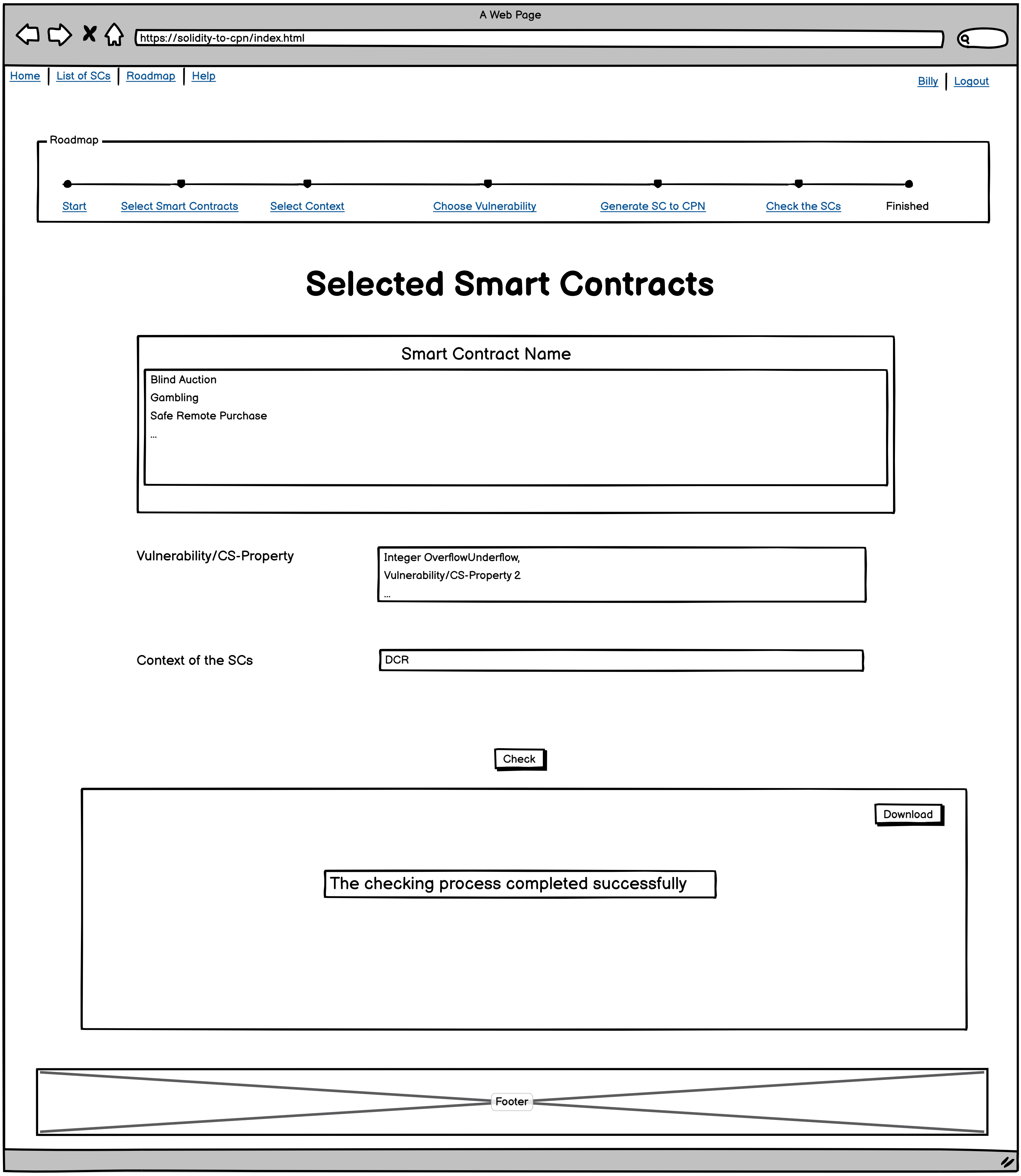
Smart Contract Name

Blind Auction
Gambling
Safe Remote Purchase
...

Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

We have discover some counter-examples with the smart contract code. Do you want to look at them?



Selected Smart Contracts

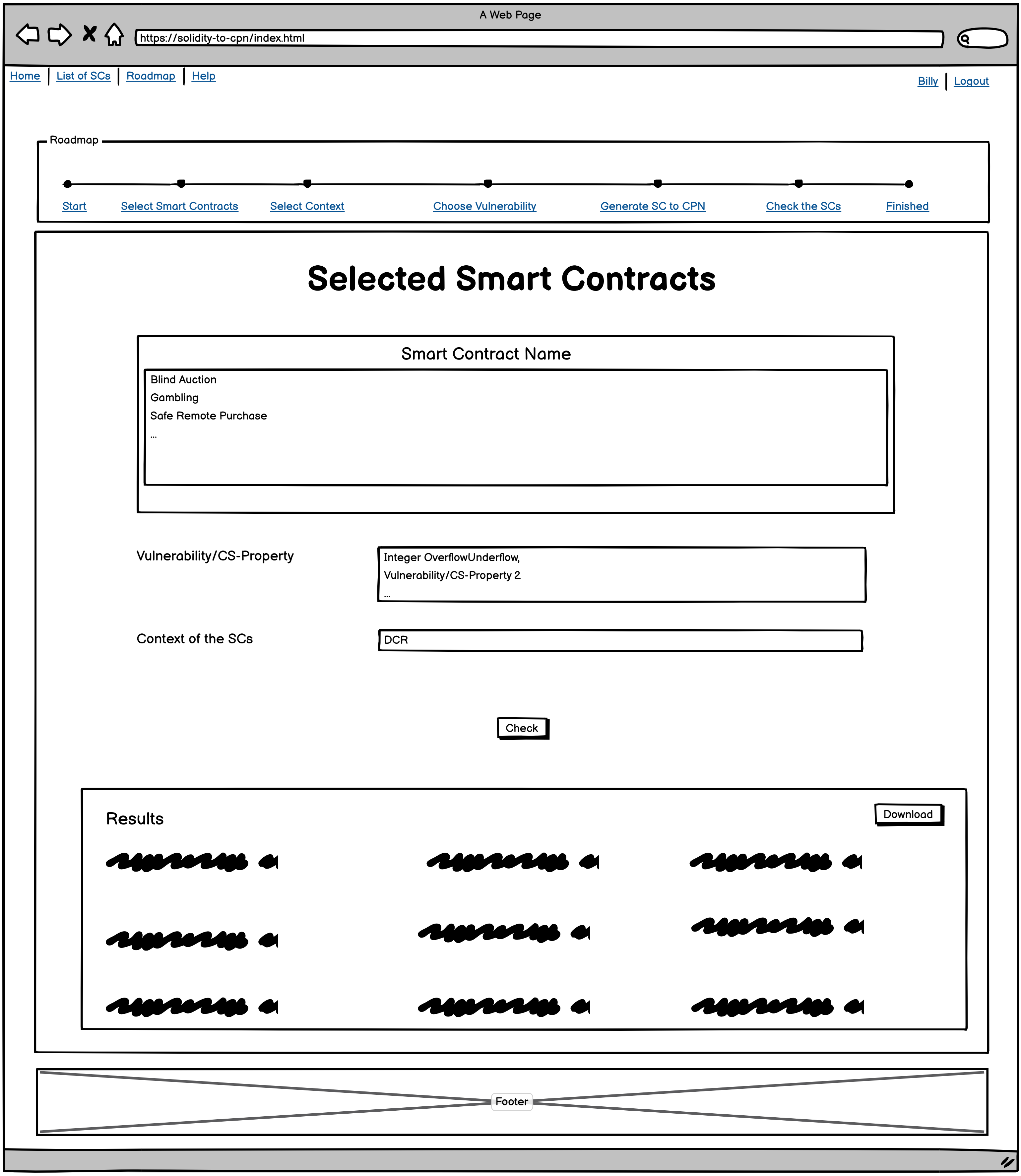
Smart Contract Name

Blind Auction
Gambling
Safe Remote Purchase
...

Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

The checking process completed successfully



Selected Smart Contracts

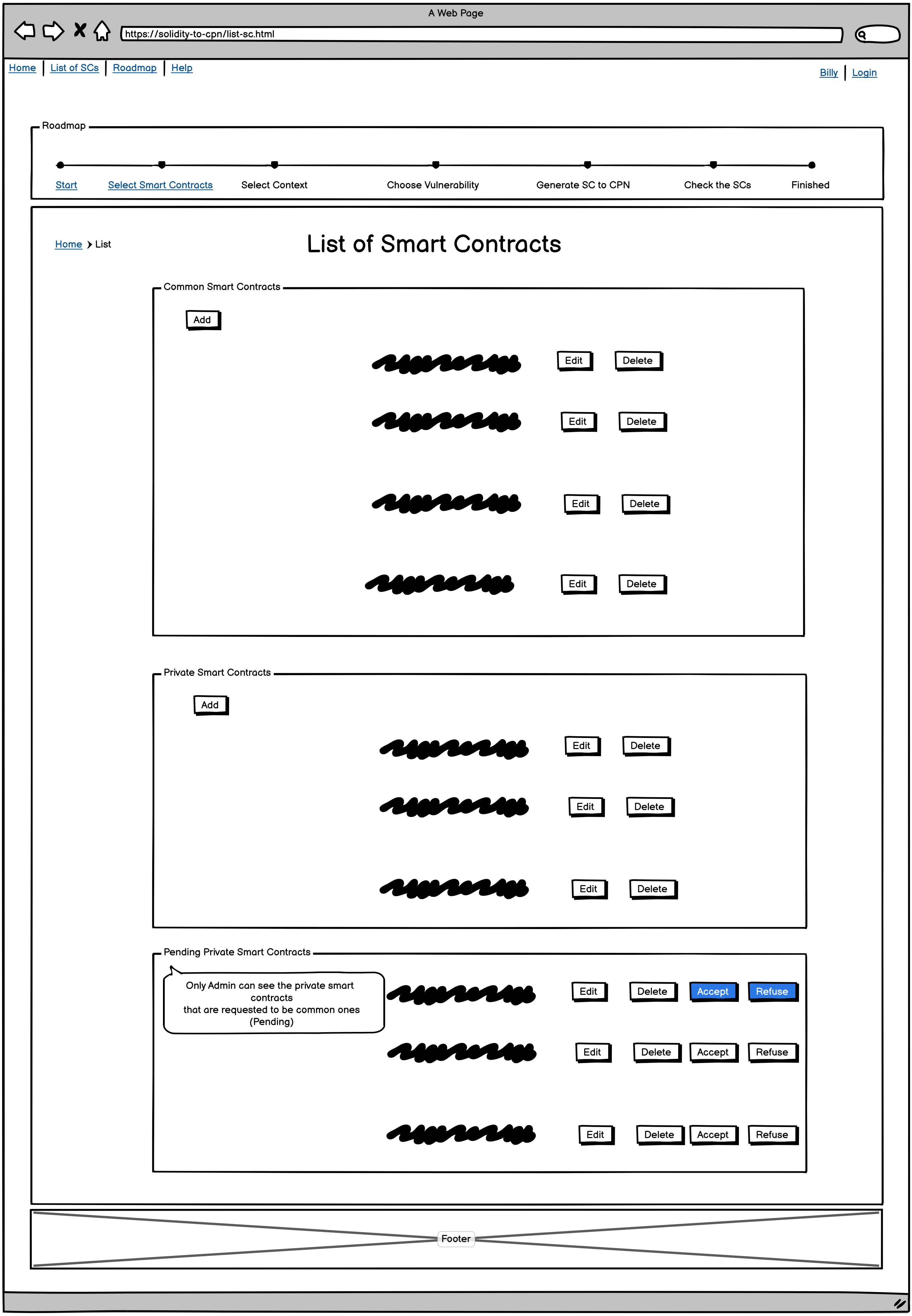
Smart Contract Name

Blind Auction
Gambling
Safe Remote Purchase
...

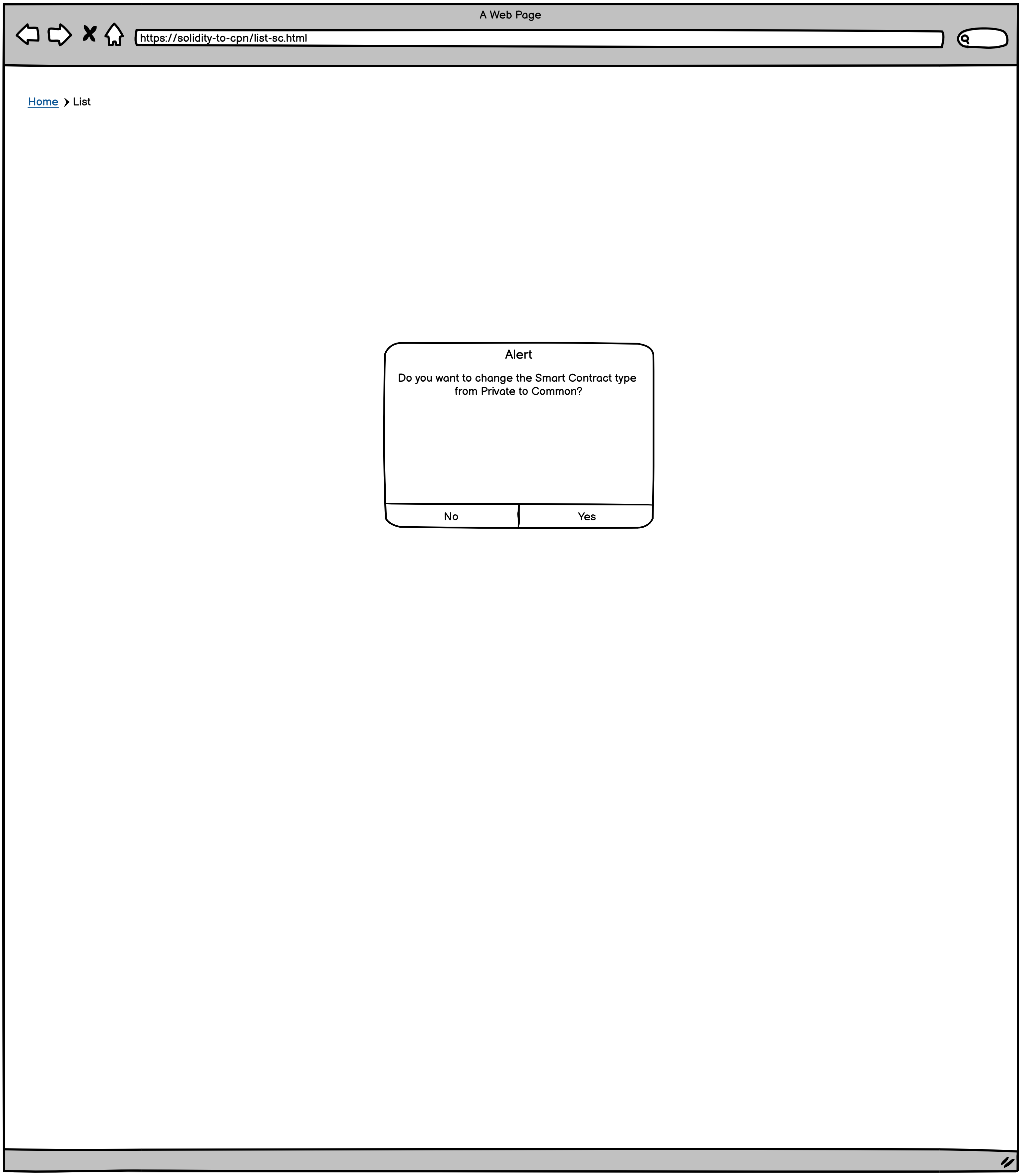
Vulnerability/CS-Property: Integer OverflowUnderflow,
Vulnerability/CS-Property 2
...

Context of the SCs: DCR

Results



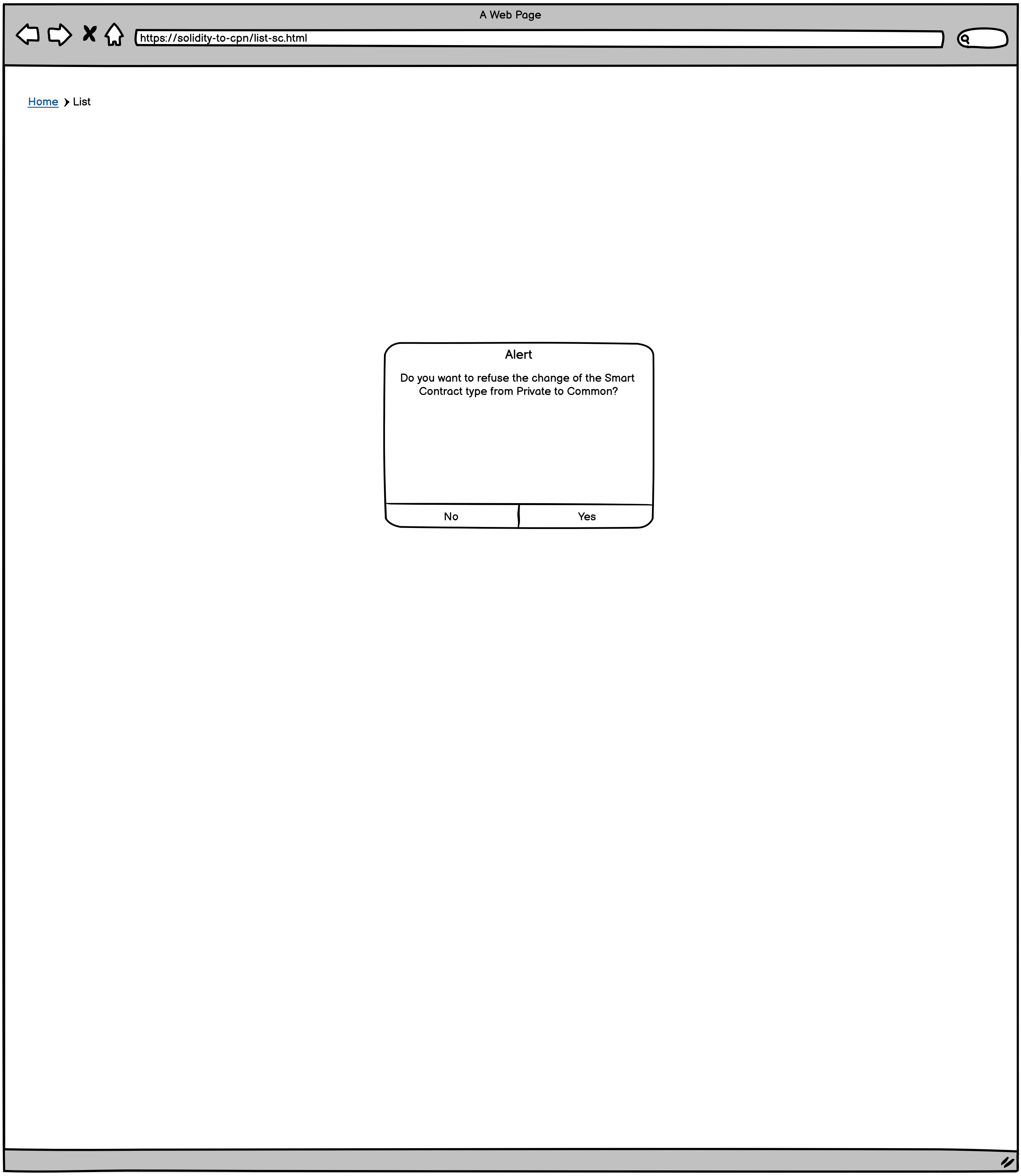
Only Admin can see the private smart contracts that are requested to be common ones (Pending)



https://solidity-to-cpn/list-sc.html

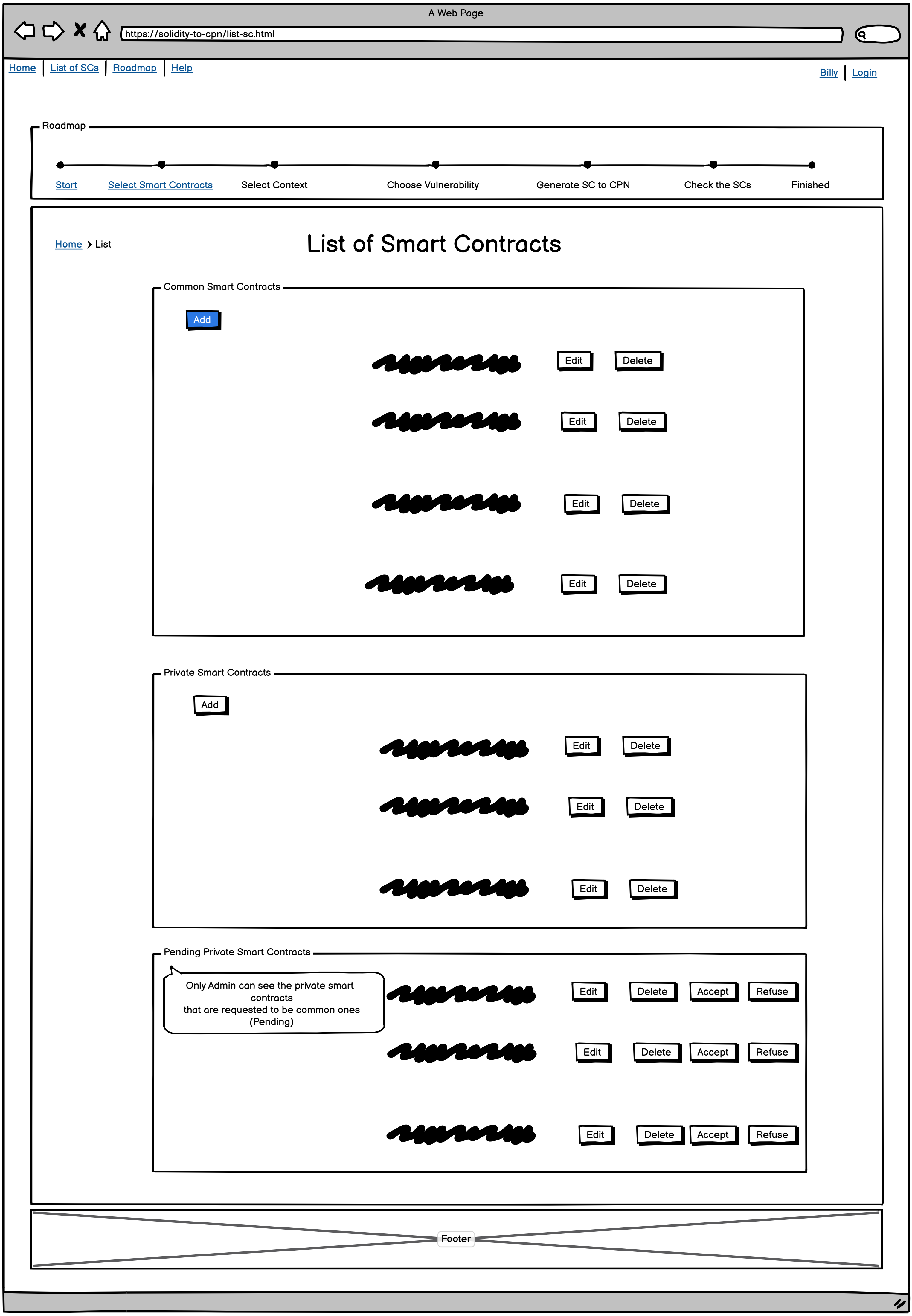
Alert

Do you want to change the Smart Contract type from Private to Common?



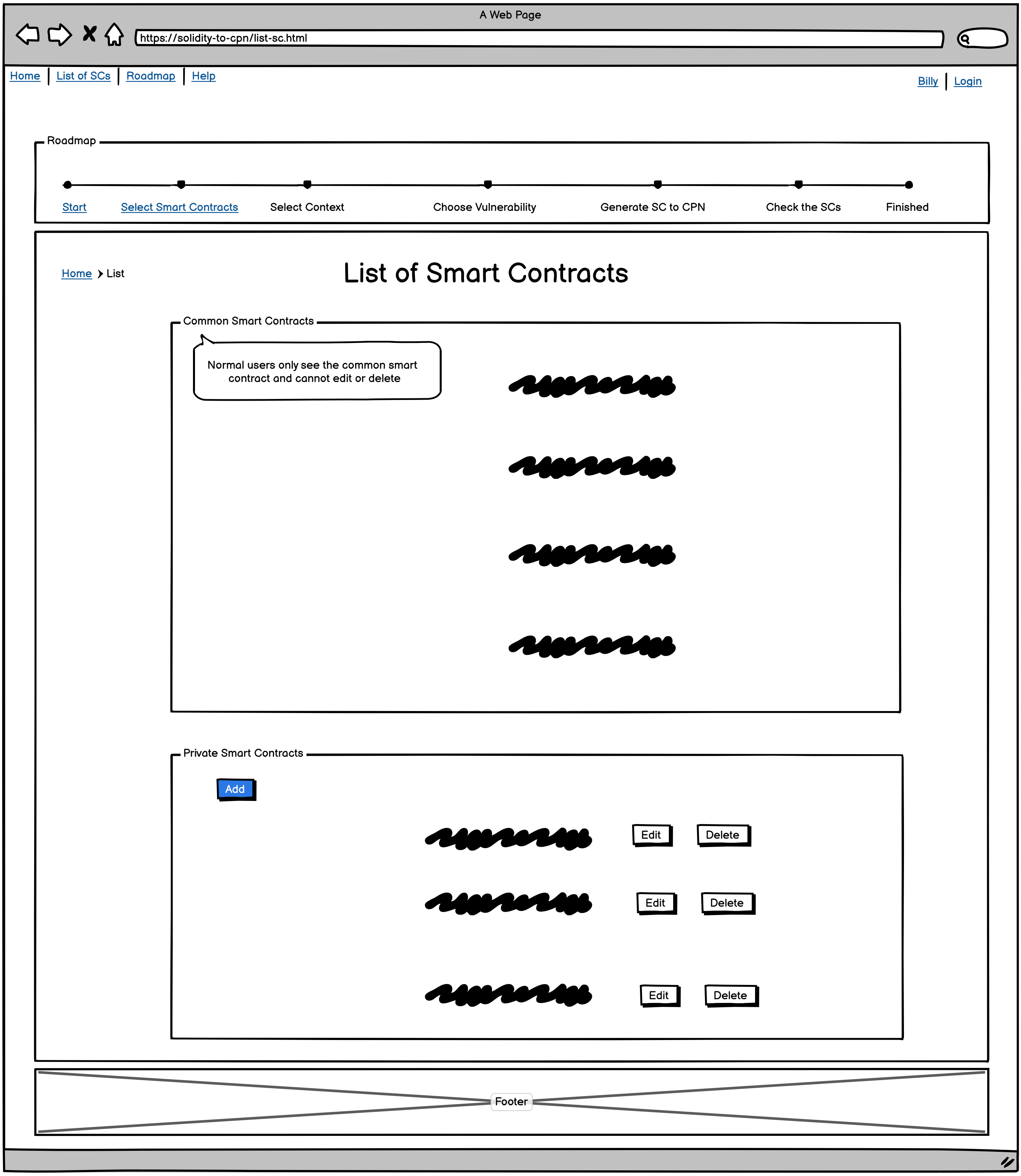
Alert

Do you want to refuse the change of the Smart Contract type from Private to Common?



List of Smart Contracts

Only Admin can see the private smart contracts
that are requested to be common ones
(Pending)



A Web Page

https://solidity-to-cpn/list-sc.html

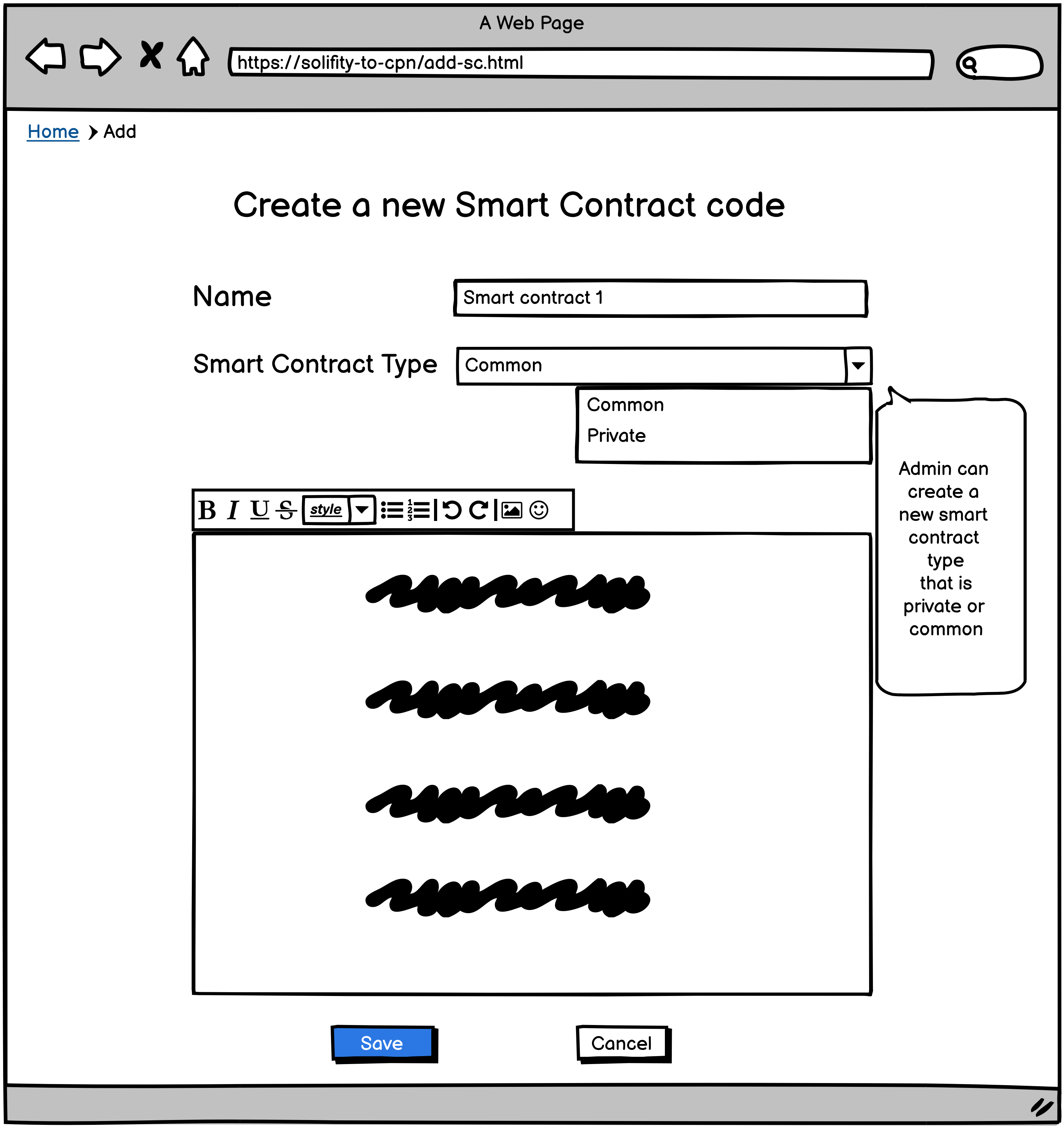
Roadmap

List of Smart Contracts

Common Smart Contracts

Normal users only see the common smart contract and cannot edit or delete

Private Smart Contracts

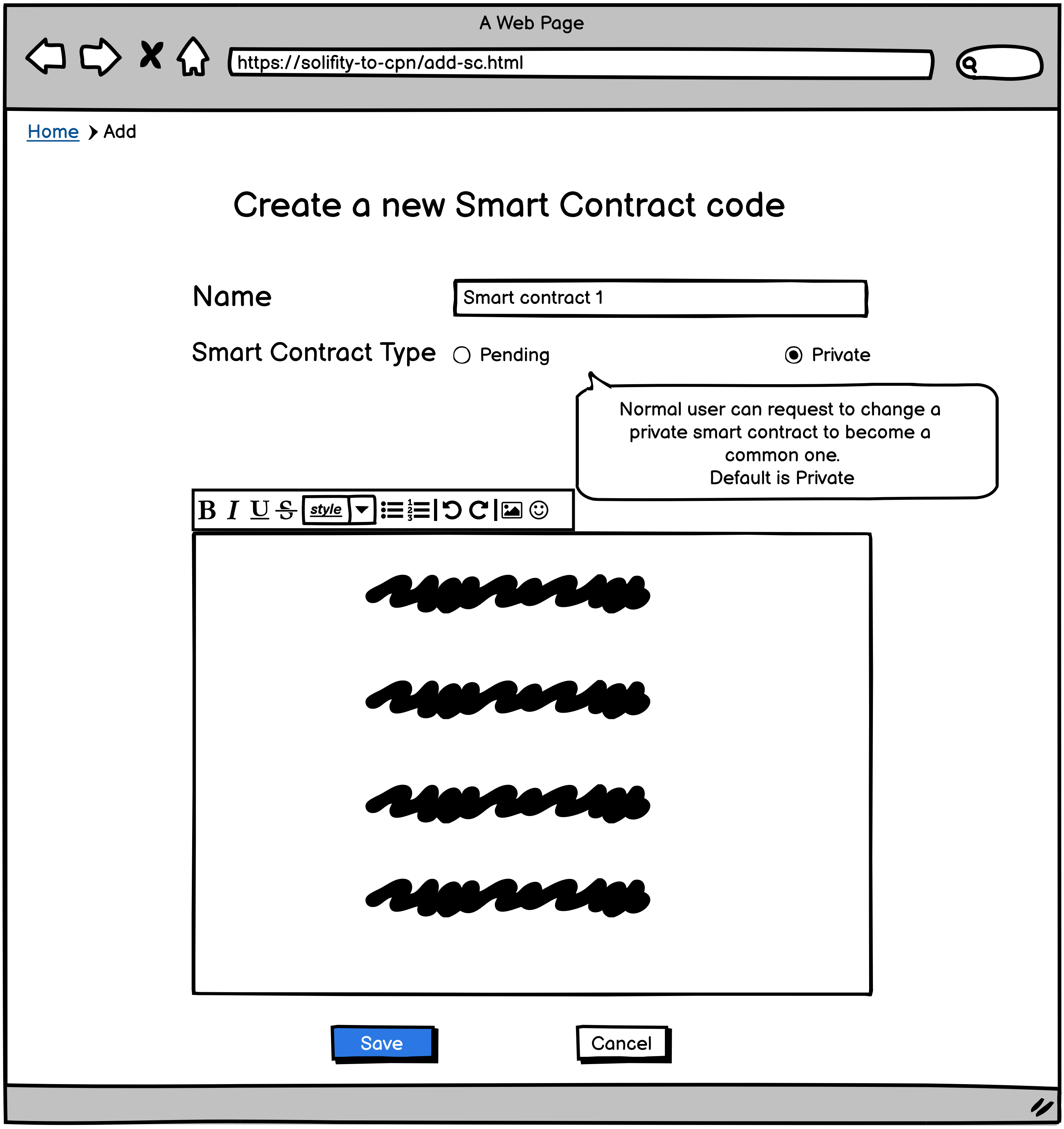


Create a new Smart Contract code

Name: Smart contract 1

Smart Contract Type: Common

Admin can create a new smart contract type that is private or common

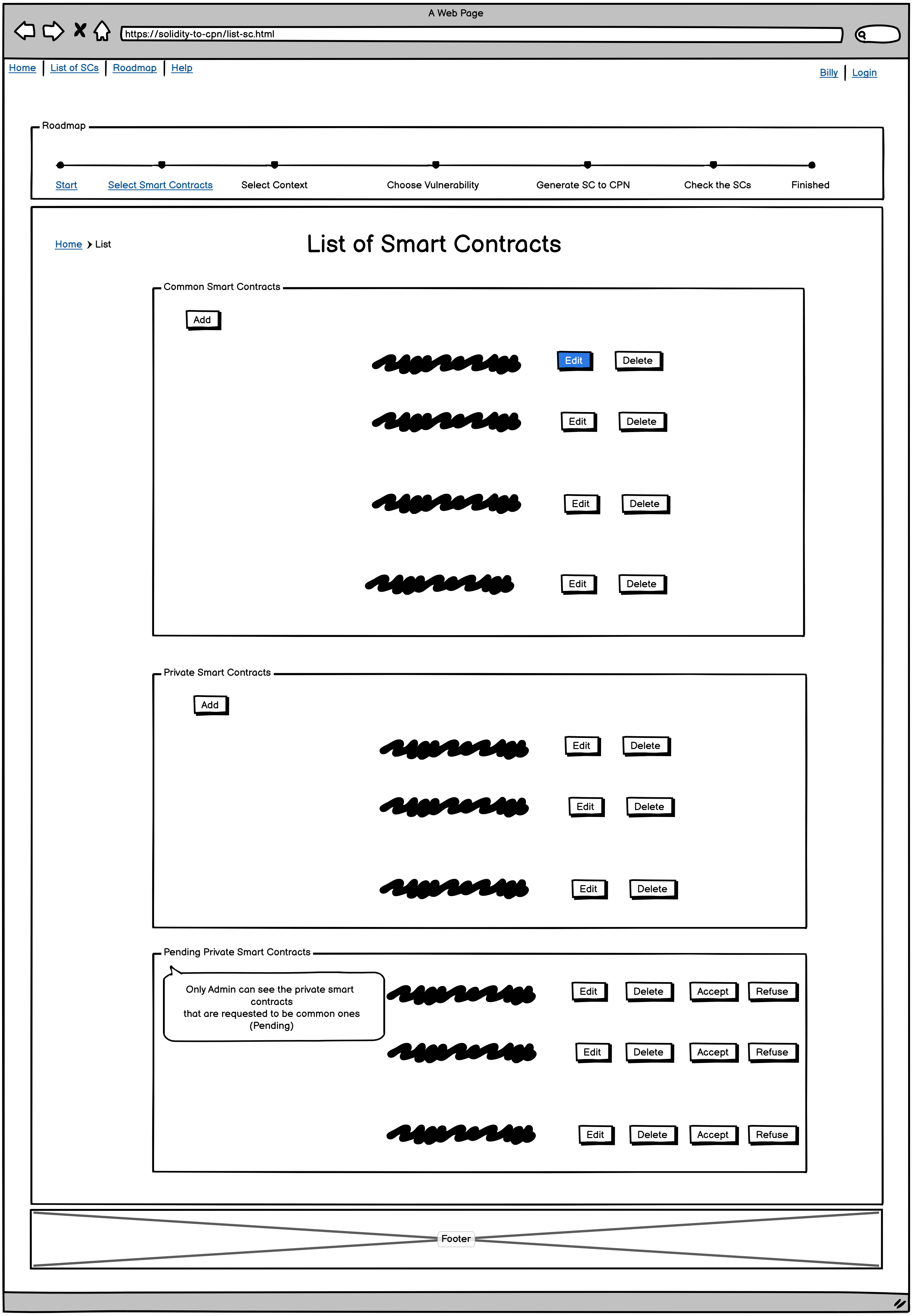


Create a new Smart Contract code

Name: Smart contract 1

Smart Contract Type ○ Pending ● Private

Normal user can request to change a private smart contract to become a common one.
Default is Private

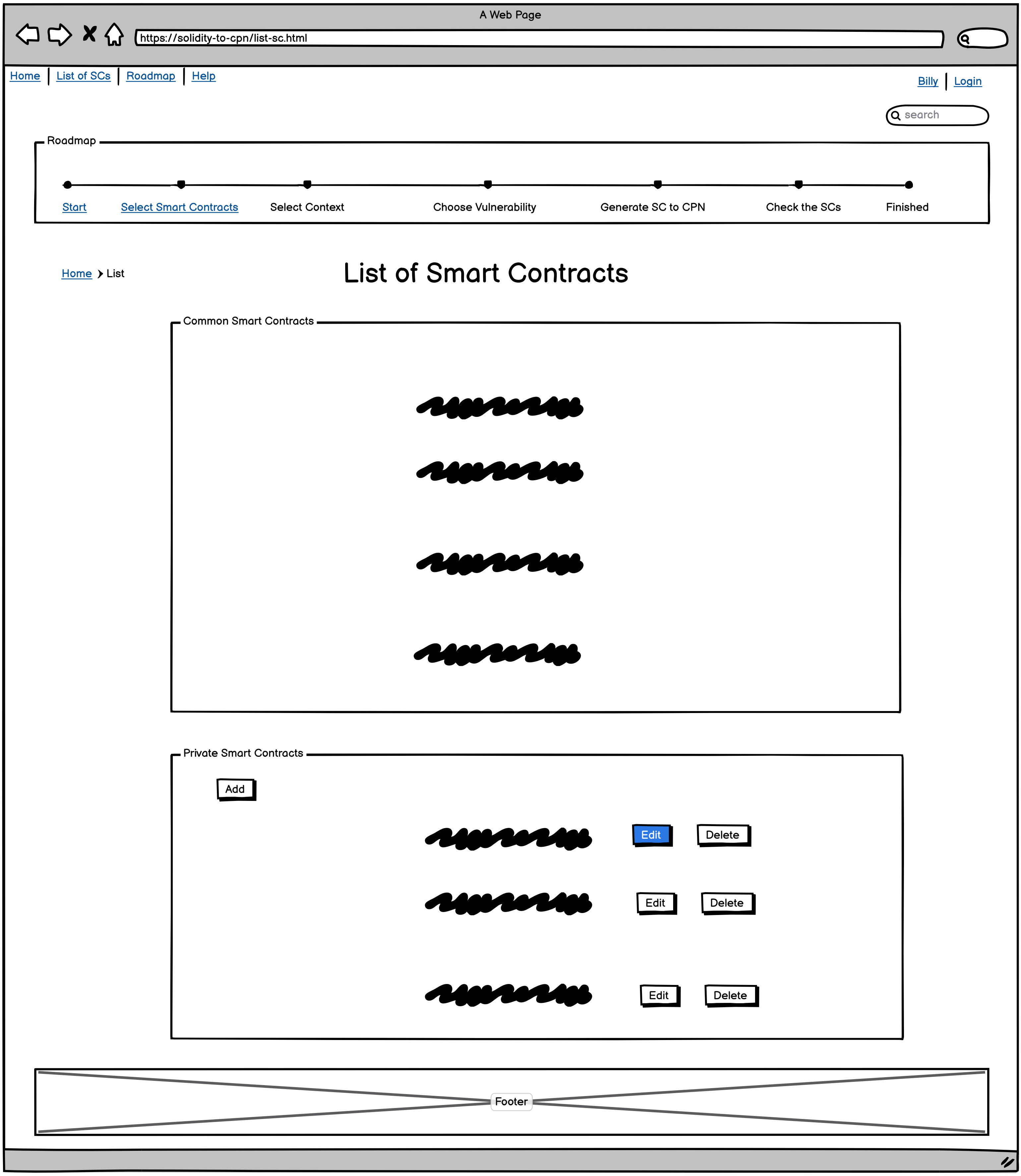


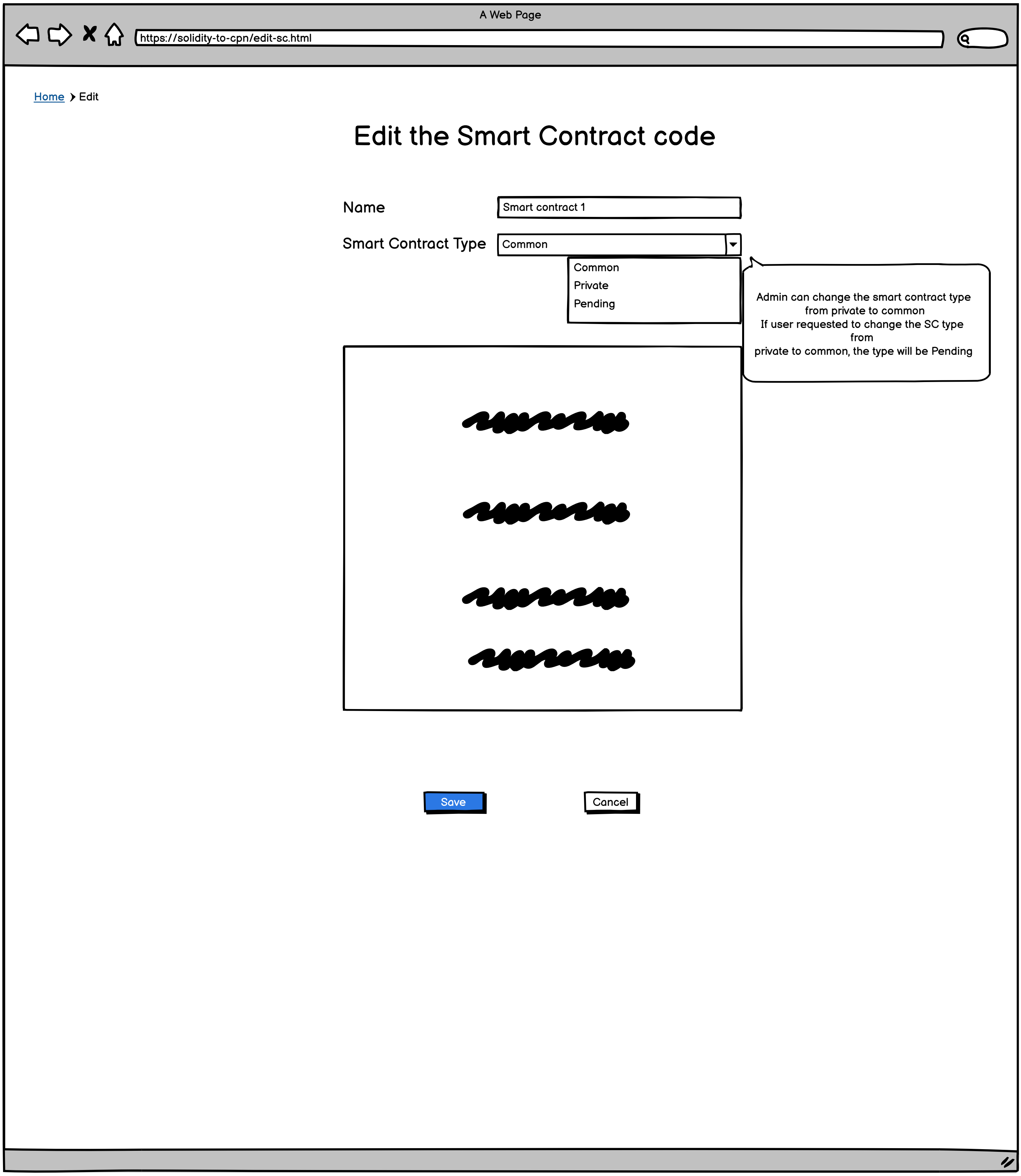
A Web Page

https://solidity-to-cpn/list-sc.html

List of Smart Contracts

Only Admin can see the private smart contracts
that are requested to be common ones
(Pending)


A Web Page
https://solidity-to-cpn/list-sc.html
Home
List of SCs
Roadmap
Help
Billy
Login
search
Roadmap
Start
Select Smart Contracts
Select Context
Choose Vulnerability
Generate SC to CPN
Check the SCs
Finished
Home
List
List of Smart Contracts
Common Smart Contracts
Private Smart Contracts
Add
Edit
Delete
Edit
Delete
Edit
Delete
Footer

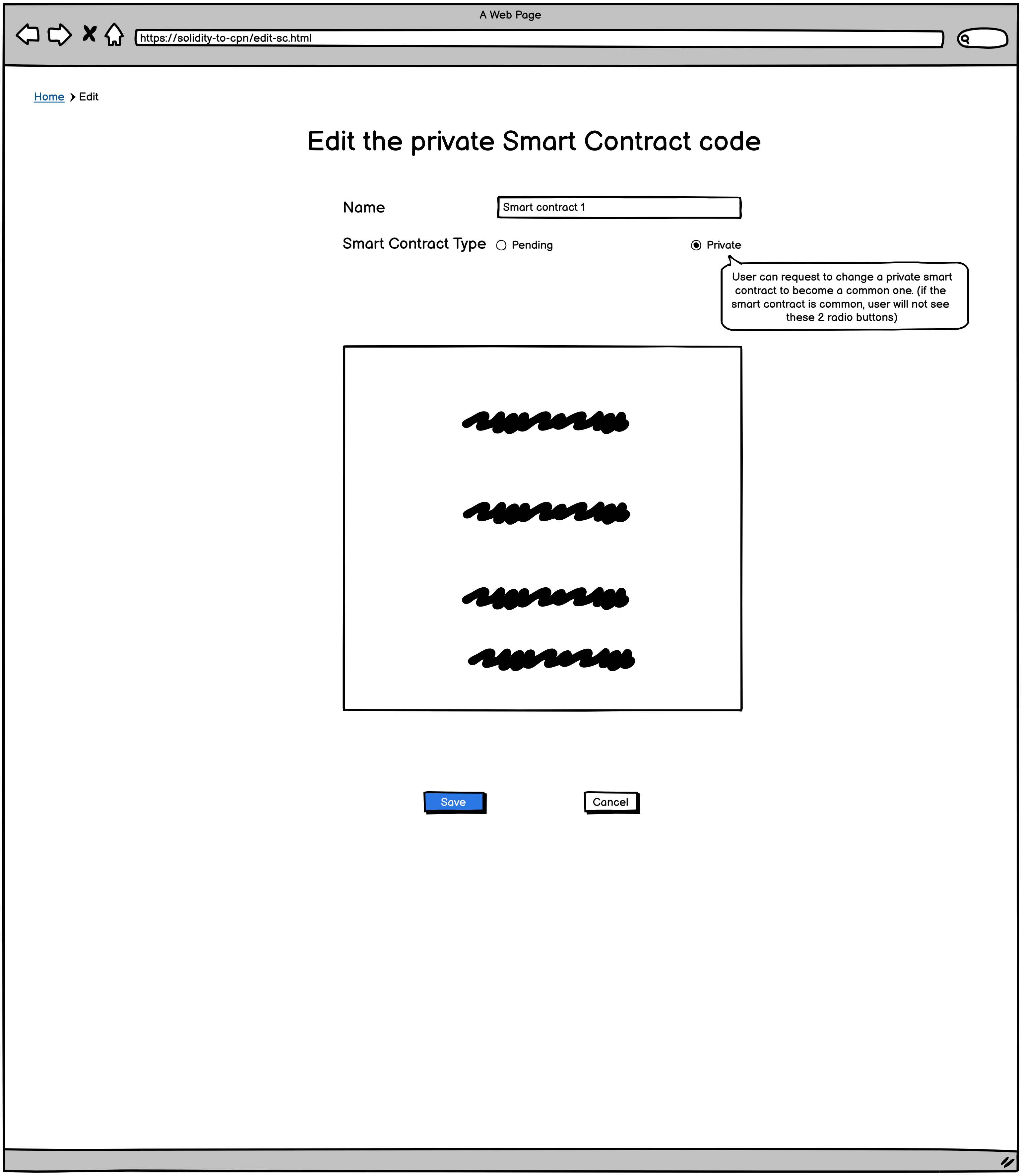


Edit the Smart Contract code

Name: Smart contract 1

Smart Contract Type: Common

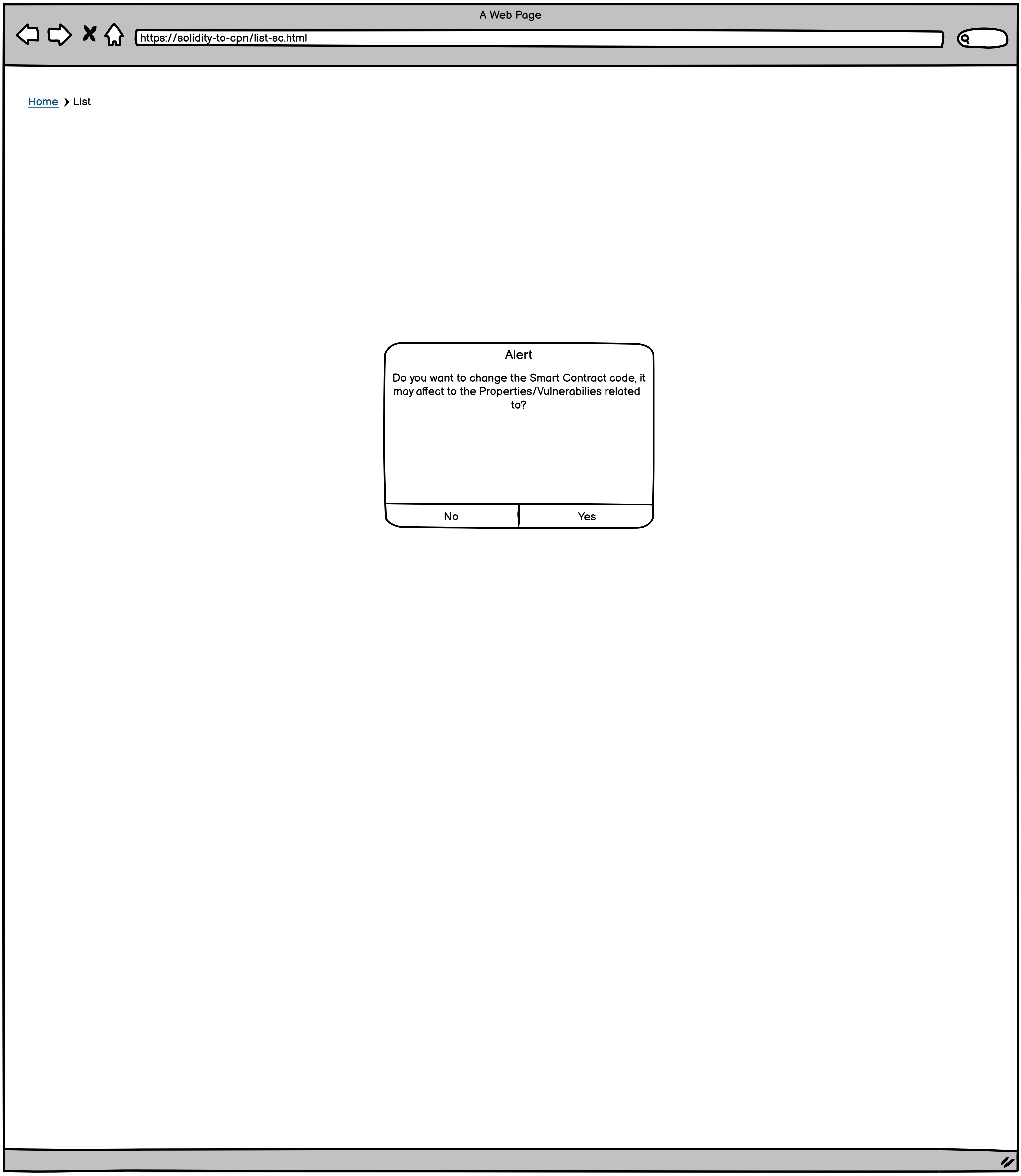
Admin can change the smart contract type from private to common
If user requested to change the SC type from
private to common, the type will be Pending



Edit the private Smart Contract code

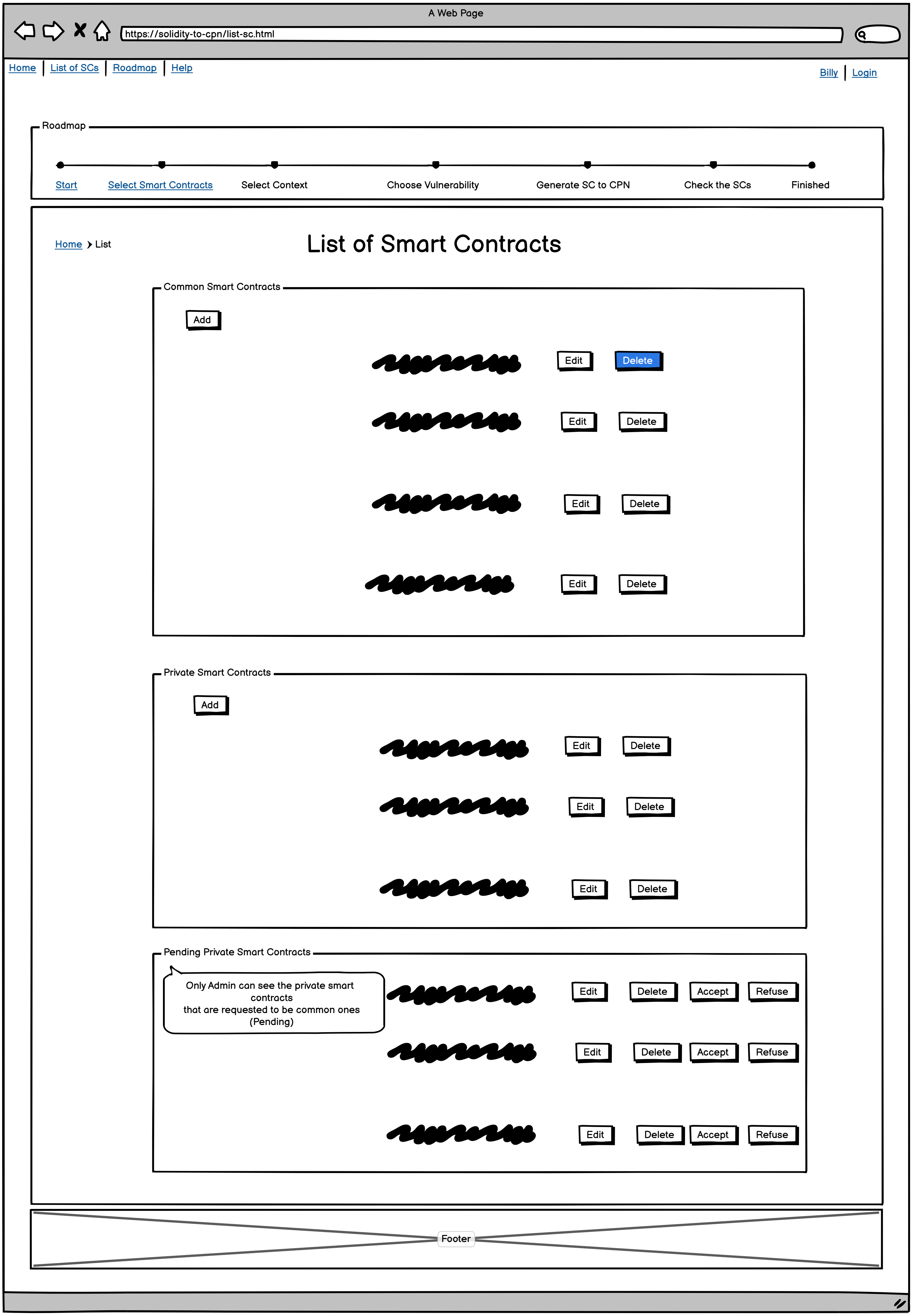
Name	Smart contract 1
Smart Contract Type	○ Pending ● Private

User can request to change a private smart contract to become a common one. (if the smart contract is common, user will not see these 2 radio buttons)



Alert

Do you want to change the Smart Contract code, it may affect to the Properties/Vulnerabilies related to?



A Web Page

https://solidity-to-cpn/list-sc.html

Home | List of SCs | Roadmap | Help

Billy | Login

Roadmap

Start — Select Smart Contracts — Select Context — Choose Vulnerability — Generate SC to CPN — Check the SCs — Finished

Home > List

List of Smart Contracts

Common Smart Contracts

Add

Edit Delete

Edit Delete

Edit Delete

Edit Delete

Private Smart Contracts

Add

Edit Delete

Edit Delete

Edit Delete

Pending Private Smart Contracts

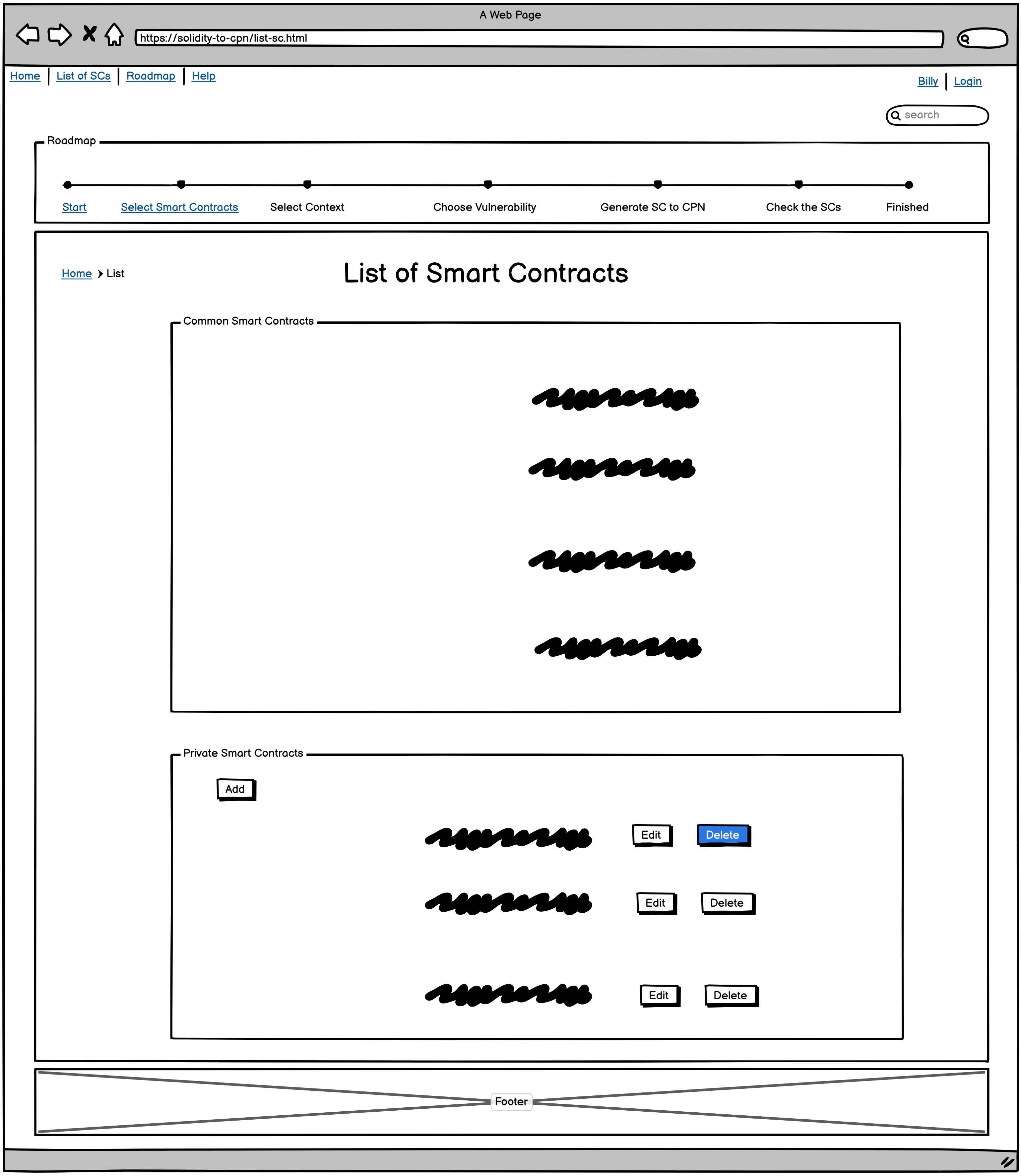
Only Admin can see the private smart contracts
that are requested to be common ones
(Pending)

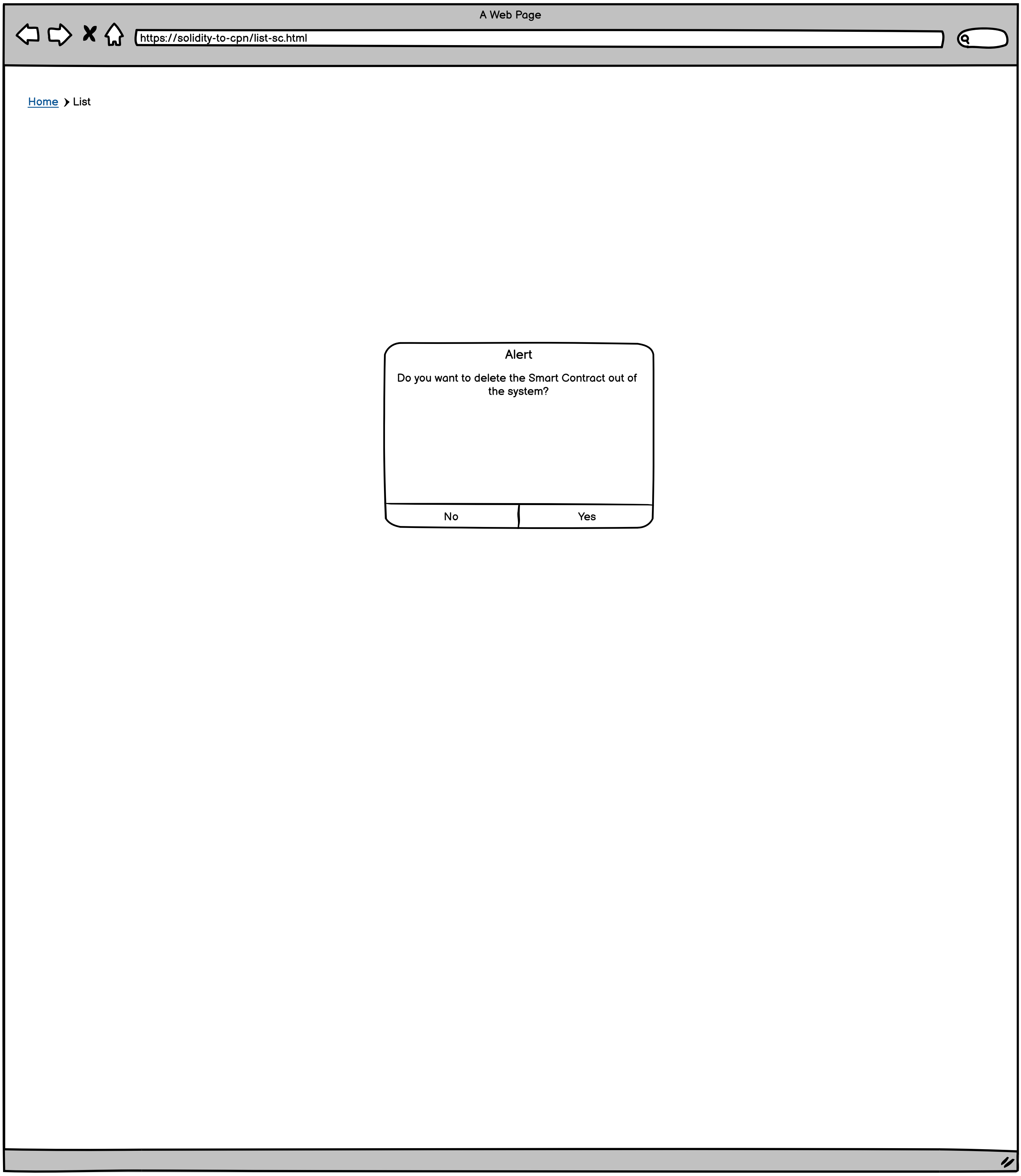
Edit Delete Accept Refuse

Edit Delete Accept Refuse

Edit Delete Accept Refuse

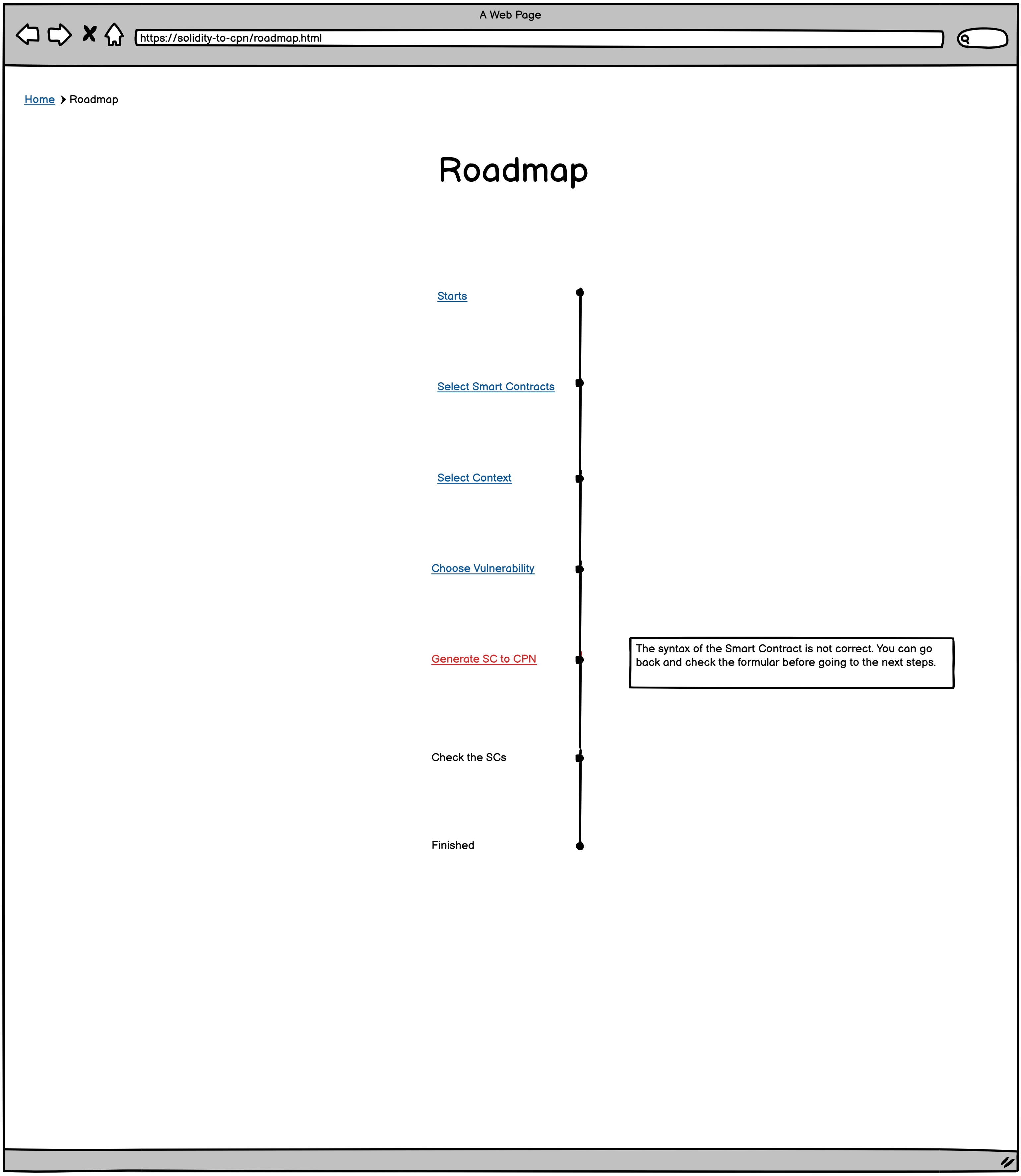
Footer


A Web Page
https://solidity-to-cpn/list-sc.html
Home
List of SCs
Roadmap
Help
Billy
Login
search
Roadmap
Start
Select Smart Contracts
Select Context
Choose Vulnerability
Generate SC to CPN
Check the SCs
Finished
Home
List
List of Smart Contracts
Common Smart Contracts
Private Smart Contracts
Add
Edit
Delete
Edit
Delete
Edit
Delete
Footer



Alert

Do you want to delete the Smart Contract out of the system?



Home ❯ Roadmap

Roadmap

Starts

Select Smart Contracts

Select Context

Choose Vulnerability

Generate SC to CPN

The syntax of the Smart Contract is not correct. You can go back and check the formular before going to the next steps.

Check the SCs

Finished