

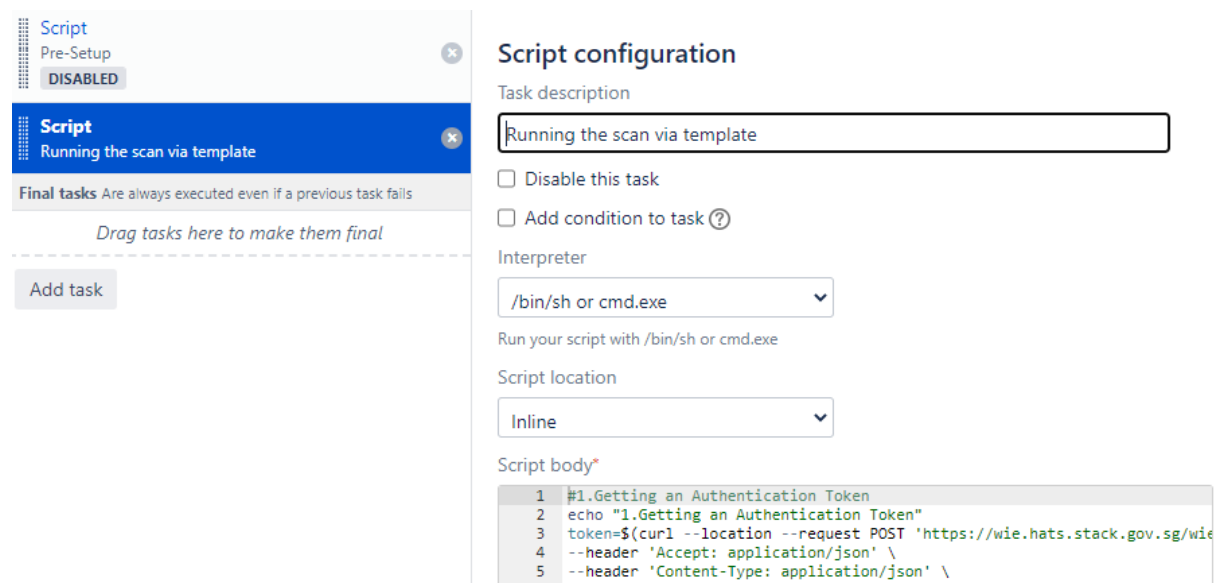
WIE Setup in Bamboo

Parameterized Login Macros in WebInspect

<https://www.youtube.com/watch?v=08EvLzrpCs8>

The above link shows how to parameterise your WIE login macro, this is useful if your login credentials changes frequently.

Achieve Way – Call scanTemplateId



The screenshot shows the Bamboo Script configuration interface. On the left, a sidebar lists tasks: 'Script Pre-Setup' (DISABLED) and 'Script Running the scan via template' (selected). Below this is a section for 'Final tasks' with a note 'Are always executed even if a previous task fails' and a dashed line with the text 'Drag tasks here to make them final'. An 'Add task' button is at the bottom of this section. The main area is titled 'Script configuration' and contains the following fields:

- Task description:** A text box containing 'Running the scan via template'.
- Disable this task:** An unchecked checkbox.
- Add condition to task:** An unchecked checkbox with a help icon.
- Interpreter:** A dropdown menu showing '/bin/sh or cmd.exe'.
- Run your script with /bin/sh or cmd.exe:** A checkbox that is checked.
- Script location:** A dropdown menu showing 'Inline'.
- Script body:** A text area containing a shell script for getting an authentication token.

```
1 #1.Getting an Authentication Token
2 echo "1.Getting an Authentication Token"
3 token=$(curl --location --request POST 'https://wie.hats.stack.gov.sg/wie
4 --header 'Accept: application/json' \
5 --header 'Content-Type: application/json' \
```

#1.Getting an Authentication Token

```
echo "1.Getting an Authentication Token"
```

```
token=$(curl --location --request POST 'https://wie.hats.stack.sg/wie/rest/api/v1/auth' \
```

```
--header 'Accept: application/json' \
```

```
--header 'Content-Type: application/json' \
```

```
--data-raw '{"username": "${bamboo.buildmaster.username}", "password":
```

```
"${bamboo.buildmaster.password}"}
```

```
)
```

```
#echo $token
```

```
#encodedToken=$(echo $token | cut -c 26-73)
```

```
encodedToken=$(echo $ token | grep -oE '^[^ ]+$' | sed -E 's/^Authorization Token: ([a-zA-Z0-9-]+)$/\1/')
```

#2. Running the scan with Login Macro template

```
curl --location --request POST 'https://wie.hats.stack.sg/wie/rest/api/v2/scans' \  
--header 'Accept: application/json' \  
--header 'Content-Type: application/json' \  
--header "Authorization: FORTIFYTOKEN ${encodedToken}" \  
--data-raw '{  
  "name": "${bamboo.fortify.ssc.scanName}",  
  "projectVersion": {"id": ${bamboo.fortify.ssc.projectVersion.id}, "name":  
    "${bamboo.fortify.ssc.appver}", "siteId": "${bamboo.fortify.ssc.siteId}"},  
  "scanTemplateId": "${bamboo.fortify.ssc.template}" }'
```

Variables parsing

bamboo.buildmaster.username - ur account

bamboo.buildmaster.password - get from ur admin

bamboo.fortify.ssc.scanName - define scanName, eg. eCOA.\${bamboo.buildNumber}

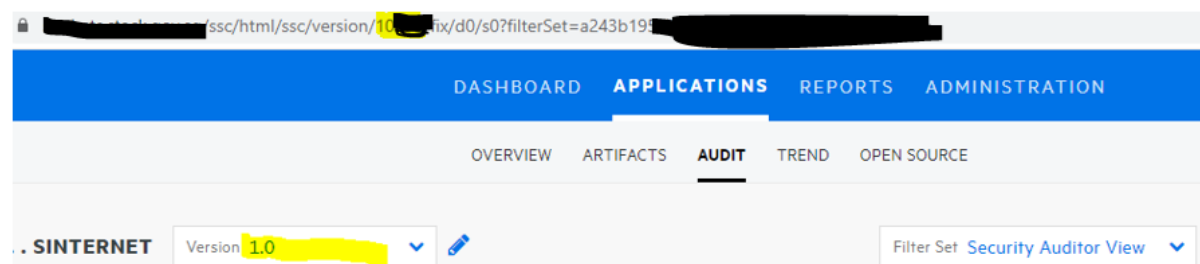
noted - add buildNumber to distinguish ur build as below

	Name	Scan URL	Status	Application - Version	Policy	Sensor
	...ss.2	https://...	Complete	...TERNE	OWASP Top 10	Sensor1

bamboo.fortify.ssc.projectVersion.id - eg. 12345

bamboo.fortify.ssc.appver - eg. 1.0

noted - u can get above 2 info from ur SSC as below



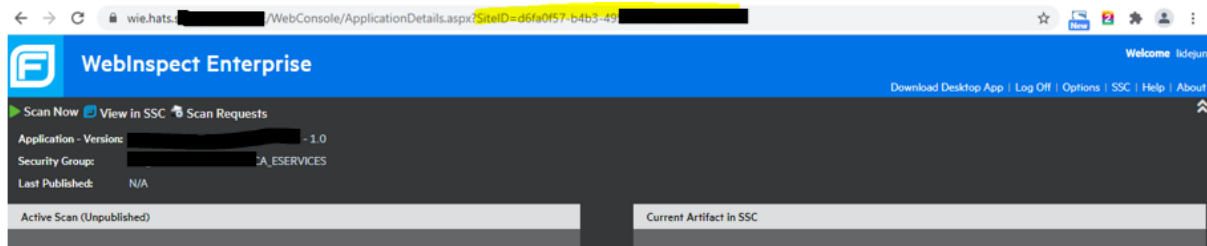
bamboo.fortify.ssc.siteId - get through below **Pre-Setup** task to get

bamboo.fortify.ssc.template - get though below **template** to Create

Pre-Setup - get siteld

1. Go to <https://wie.hats.stack.sg>

Then click it



Get template

2. Go to <https://wie.hats.stack.sg>

Install Desktop App and click GUIDE SCAN



3. Create standard scan

Predefined Templates



Create a Standard Web Site Scan

Default scan settings are designed to focus more on coverage then performance. Larger sites could take days to crawl with these settings.

Recent Templates

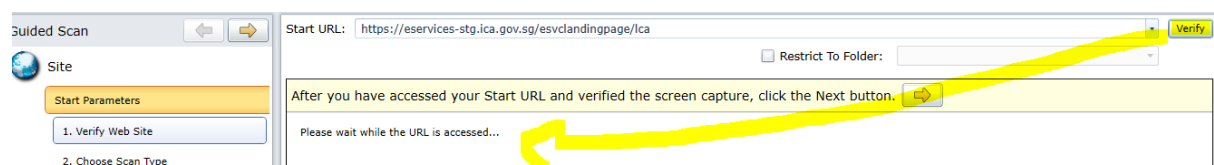


Default



Default

4. Fill in scan url and click Verify button



5. U will see page if can access

Start URL: Verify

☐ Restrict To Folder:

After you have accessed your Start URL and verified the screen capture, click the Next button. ➔

A Singapore Government Agency Website

6. Go to Scan Type
Fill in ur Scan Name, change other setting by ur App.

Guided Scan ⬅ ➡

Site

Start Parameters

1. Verify Web Site

2. Choose Scan Type

Login

Network Authentication

Application Authentication

Active Learning

Optimization Tasks

Settings

Final Review

Scan Name:

Scan Type

☒ Standard
Use the Start URL to start crawling and/or auditing your site.

☐ Workflows
Use pre-recorded macros to start crawling and/or auditing your site.

Scan Method

☐ Crawl Only
Map the attack surface of the entire site.

☒ Crawl and Audit
Map the attack surface and attack for vulnerabilities.

☐ Audit Only
Attack only the specific URL provided.

Policy

A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities, as well as poor error handling and weak SSL configuration at the web server, web application server, and database.

7. Create Login Macro

Guided Scan ⬅ ➡

Site

Start Parameters

Login

Network Authentication

Application Authentication

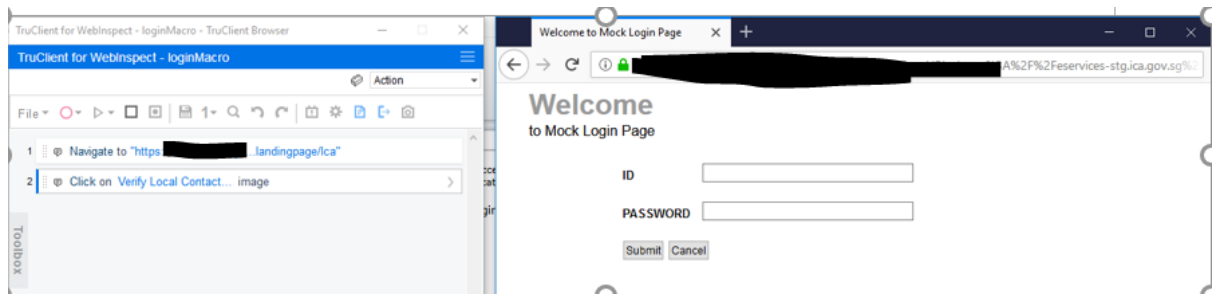
Configure Application Authentication

☒ Use a login macro for this site

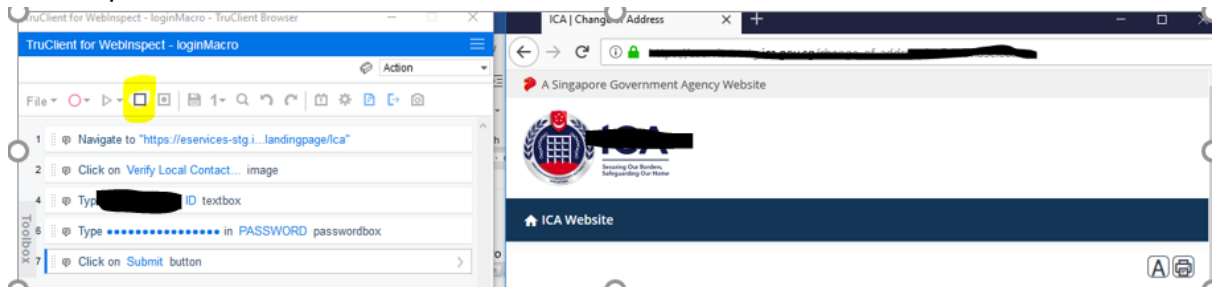
Login macros provide WebInspect access to protected locations of your application. Therefore, using a login macro is highly recommended to increase the coverage of your scan. If your application does not use authentication, you can skip this step.

Automated Login Sequence (Login Macro) Create... Download ...

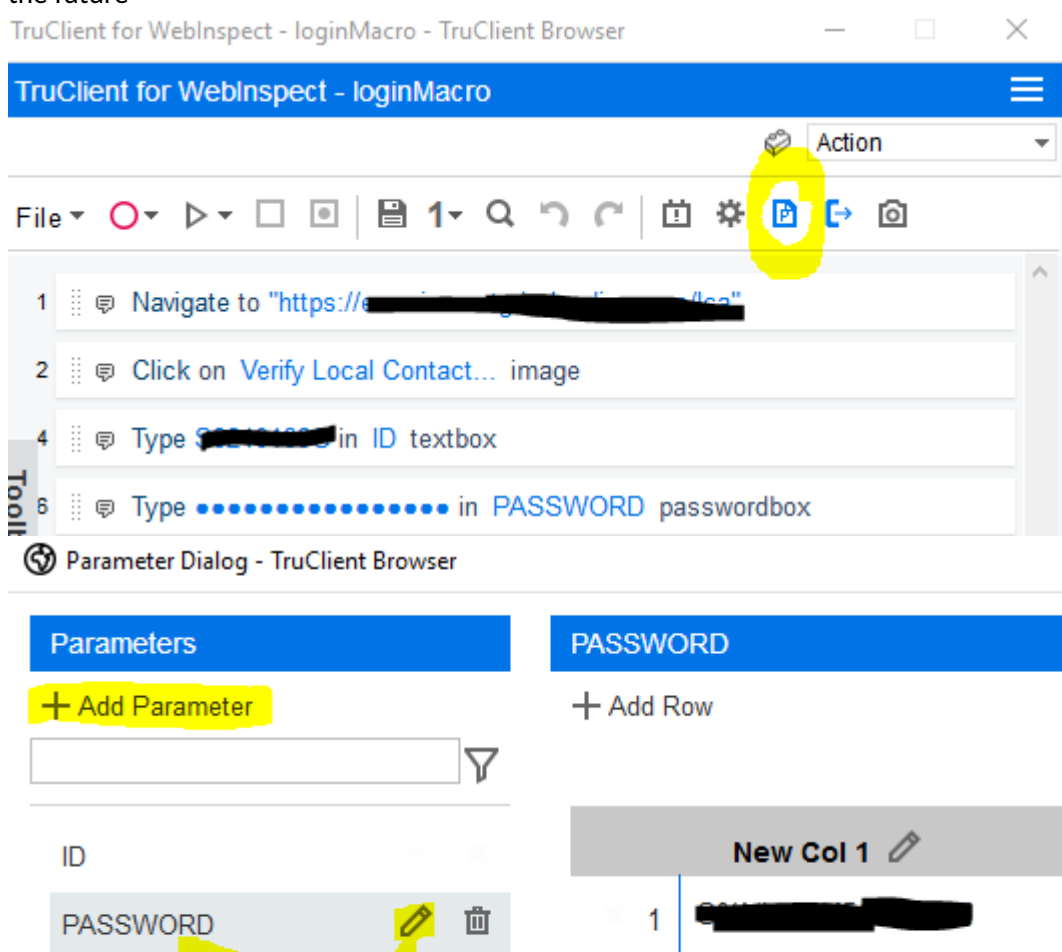
8. Fill in ur ID/PW and Submit



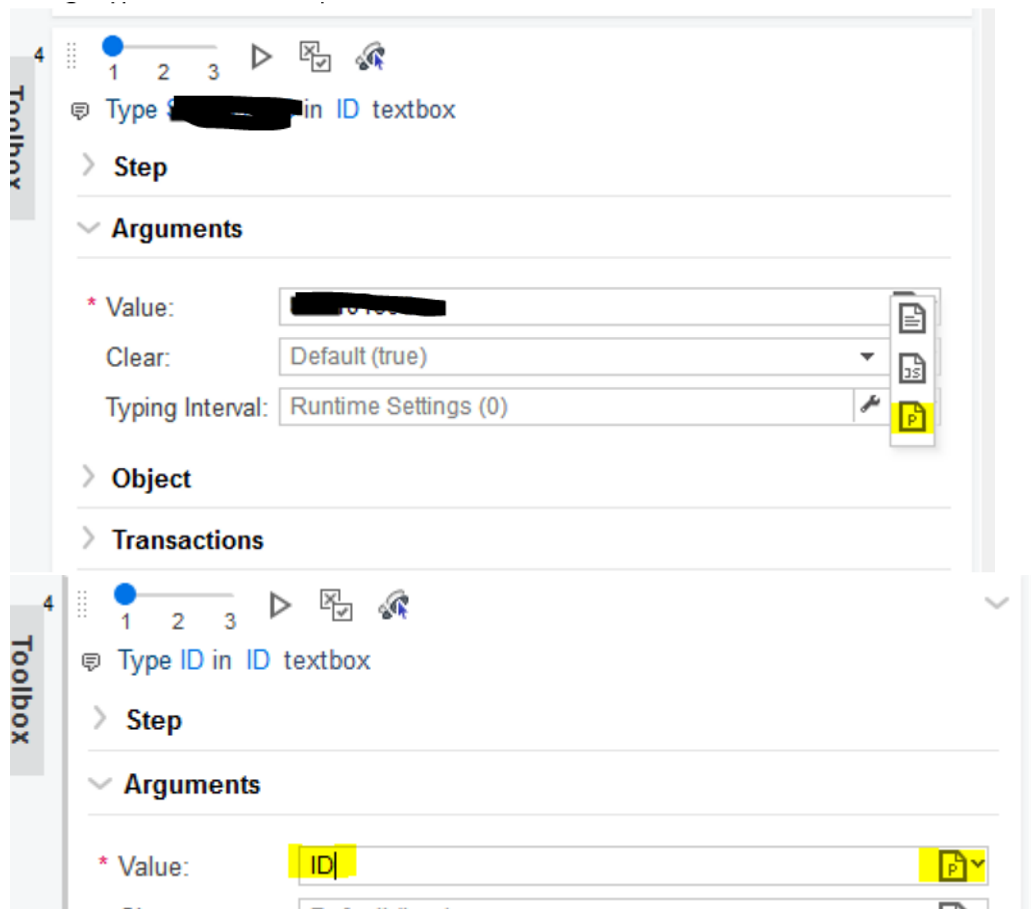
9. Click Stop icon



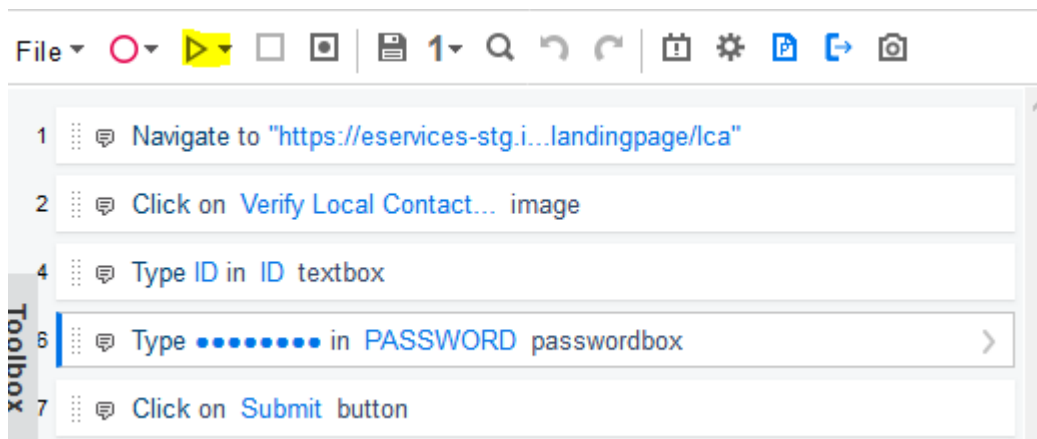
10. Click P icon to create parameter for ID and PASSWORD so that is easy to update/maintain in the future



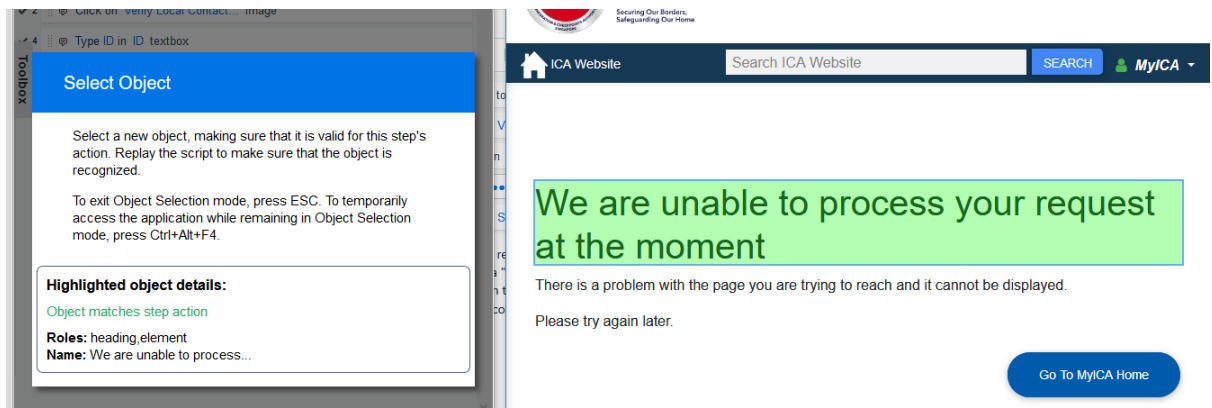
11. change type of ID/PW into parameter



12. Click 'Reply' icon



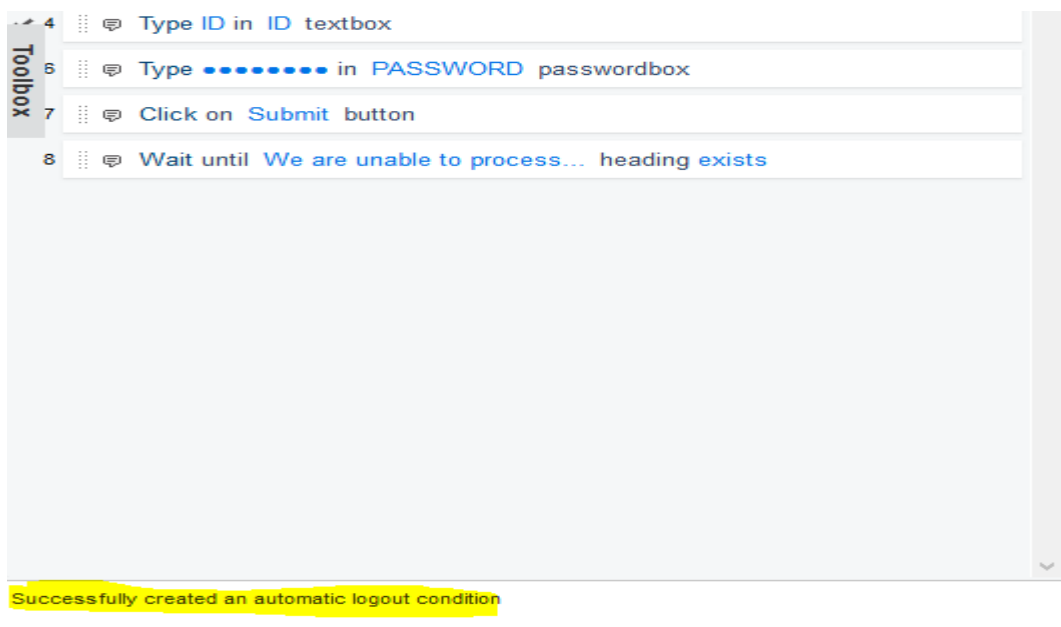
Upon completing the replay, the macro would require final step to verify that it has successfully reached a "login" state. As shown in the instruction below, you would need to select a new object on the right panel - annotated in green to make sure that the macro knows that the login condition has been fulfilled.



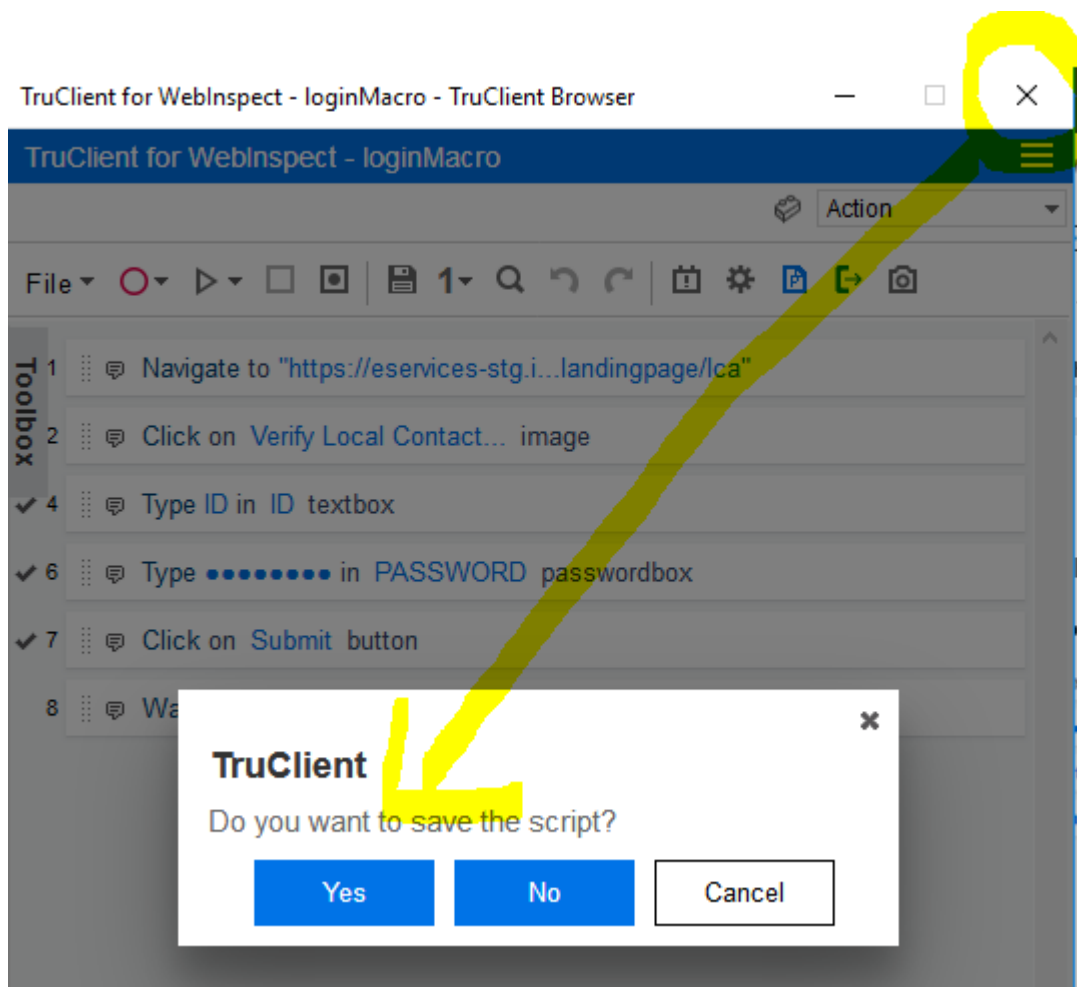
13. Logout Condition

after step 11, it will try to create a logout condition automatically and show u the result.

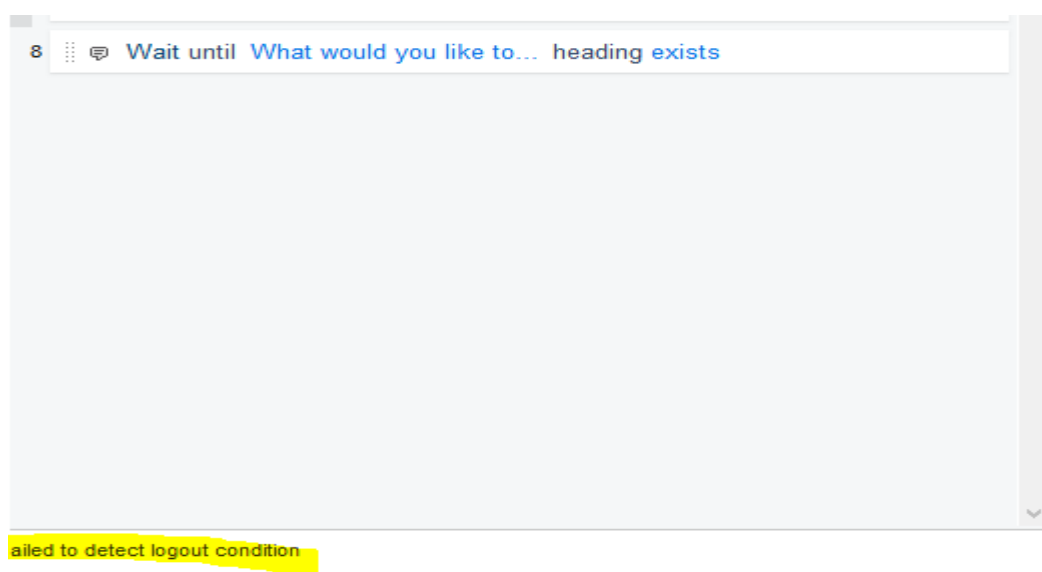
Result 1 – succeed as below



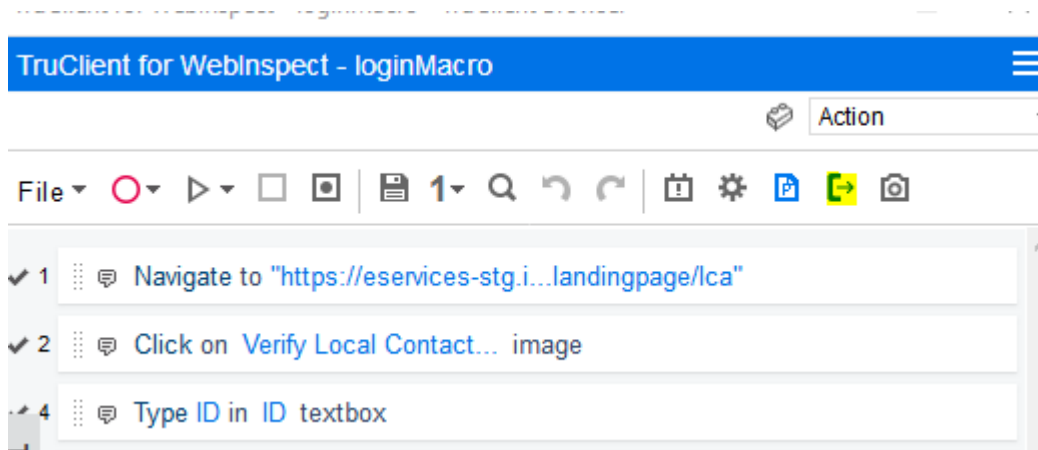
Then close the page with save to completed the macro creation.



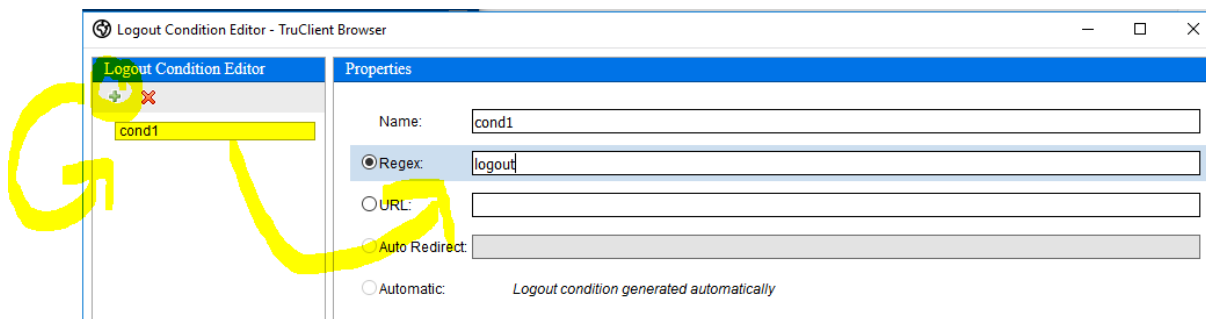
Result 2 - Failed as below



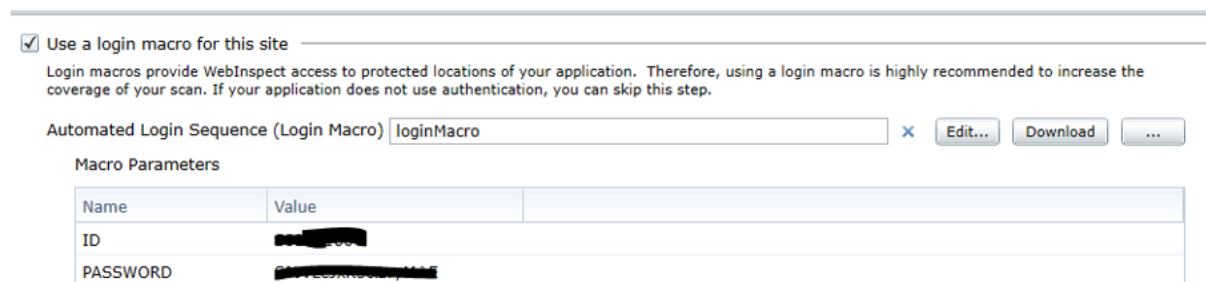
Then click Edit icon



Add a condition and fill in 'logout'

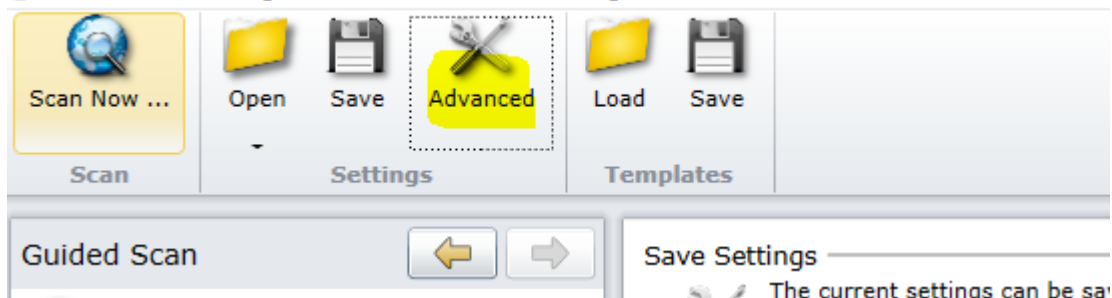


Final, Do the reply and close with save, u will see

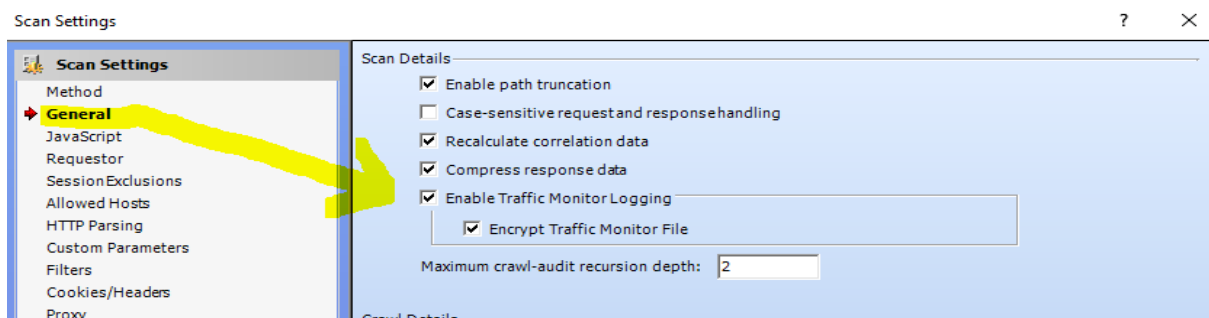


Add Advanced setting for scan

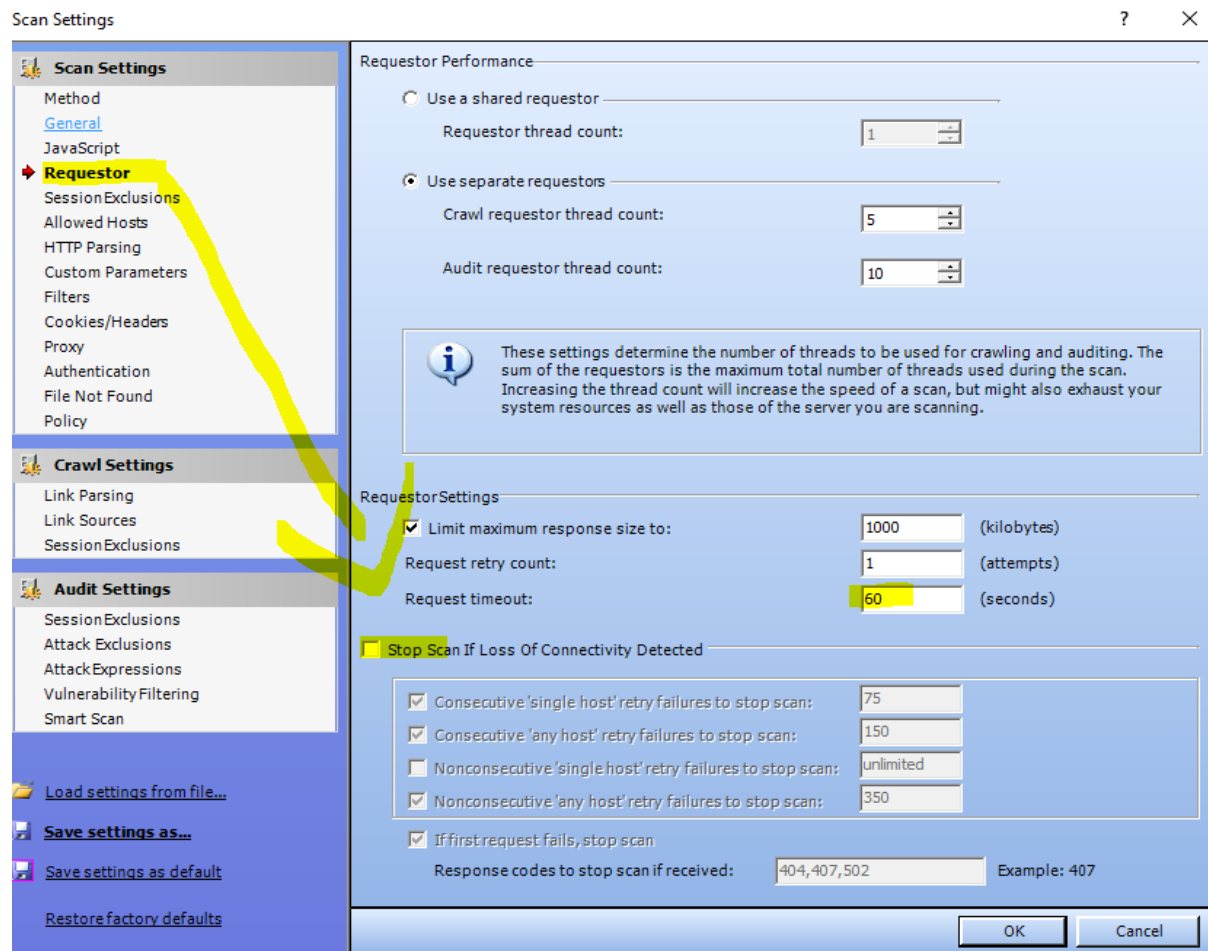
Guided Scan - Settings - Final Review - Validate Settings and Start Scan



Enable traffic

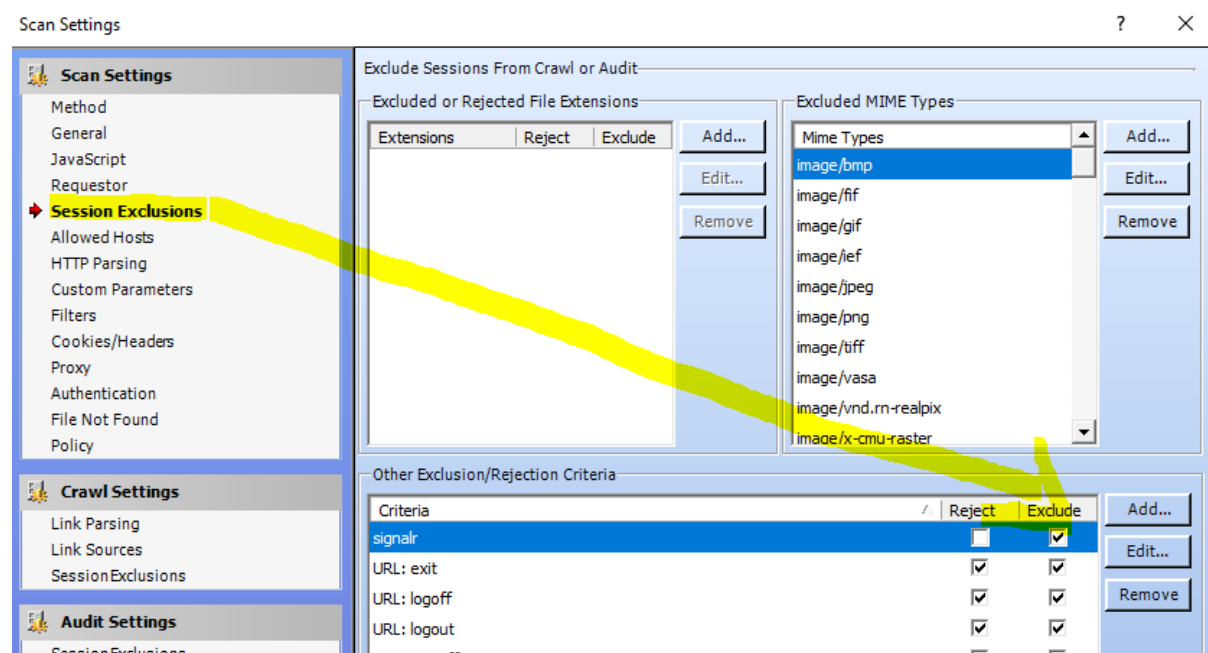


Cancel stop scan



Add regex to specify ur scan context path of url

\\.sg(\\:443)?\\(?![a-z]*(common|assets|dashboard| |landingpage\\save|webseviceapi\\esvc\\[a-z]+\\save|^\\)+\\.js|css|html|)[a-z]*\\w+





Fill in match string and click 'add' icon


Create Exclusion ? X

Improved Exclusions



To create an exclusion, you must specify the Target, Target Type (if necessary), Match Type, and Match. For example, Query parameter 'username' contains 'userone'. Once you have finished creating your exclusion, you can click the 'Test' button (if in Current Scan Settings) to test your exclusion.

Exclusion Name:

Target	Target Name	Match Type	Match String	
URL		matches regex	<code>css html a-z*\w+</code>	 



14. Optimization Task


Guided Scan  

- Site
- Start Parameters
- Login
- Network Authentication
- Application Authentication
- Active Learning
- Optimization Tasks**
- Profile site for optimal settings
- Settings
- Final Review



Guided Scan will now enter the Active Learning phase. During this step, all visited pages will be analyzed. WebInspect will show recommended settings for the scan, which can provide better coverage and assessment of the target site.

Profiler

Please press the button below to begin profiling your site.



Settings

- ☒ **Disable case sensitivity for crawling**
 WebInspect detected a server type (e.g. IIS) that does not depend on case sensitive URLs. Disabling case sensitivity should improve crawler accuracy.
IIS 7.0 was detected which is case insensitive by default.
- ☒ **Maximum response size recommendation**
 WebInspect limits the sizes of responses by design. If your site has a large number of pages that exceed the limit then you may be missing important content while performing the scan. The Profiler can detect if pages during the pre-scan exceed the limit. Raising this limit will result in a more complete and accurate scan that includes all the site's page content.
Current max response size is 1000 KB but one or more pages were encountered with sizes as high as 5 KB

15. Go to Final view, and select the fortify app id and version

Guided Scan

Site

Start Parameters

Login

Network Authentication

Application Authentication

Active Learning

Optimization Tasks

Settings

Final Review

Validate Settings and Start Scan

Save Settings

The current settings can be saved to an external file for later use.
[Click here to save settings.](#)

Save Template

The current settings can be saved to an external file for later use.
[Click here to save template.](#)

WebInspect Enterprise

Choose a location for the scan to be located when it has completed running on the sensor.

Application: [REDACTED] RNET

Application Version: 1.0

Sensor: [Run on Any Available Sensor]

Priority: ☐ 1 (highest) ☐ 2 ☒ 3 ☐ 4 ☐ 5 (lowest)

Scan Now

Here is a summary of the scan that you are about to start.

16. Save template for setup

Save settings to Scan Template

Save these settings to WebInspect Enterprise as a scan template.

Application: [REDACTED]

Application Version: 1.0

Template Name: [REDACTED]

☐ Global Template

Save the scan template at the security group level. This template will then be available for all applications in the security group. Otherwise, the template will only be available for the selected project version.


Save

Cancel

Then you can go to console to get the template id

Click the Name, now u can copy the template id and set in Bamboo pipeline

← → ↻ wie.hats[REDACTED] WebConsole/ConfigureScanTemplate.aspx?ScanTemplateID=[REDACTED]ad3fe22f-d91c-4344-a723-e[REDACTED]mand=Update

 **WebInspect Enterprise**

UPDATE SCAN TEMPLATE

GENERAL

OVERRIDES

Application

Global Template: ☐

Application [REDACTED] ▼

Version: 1.0 ▼

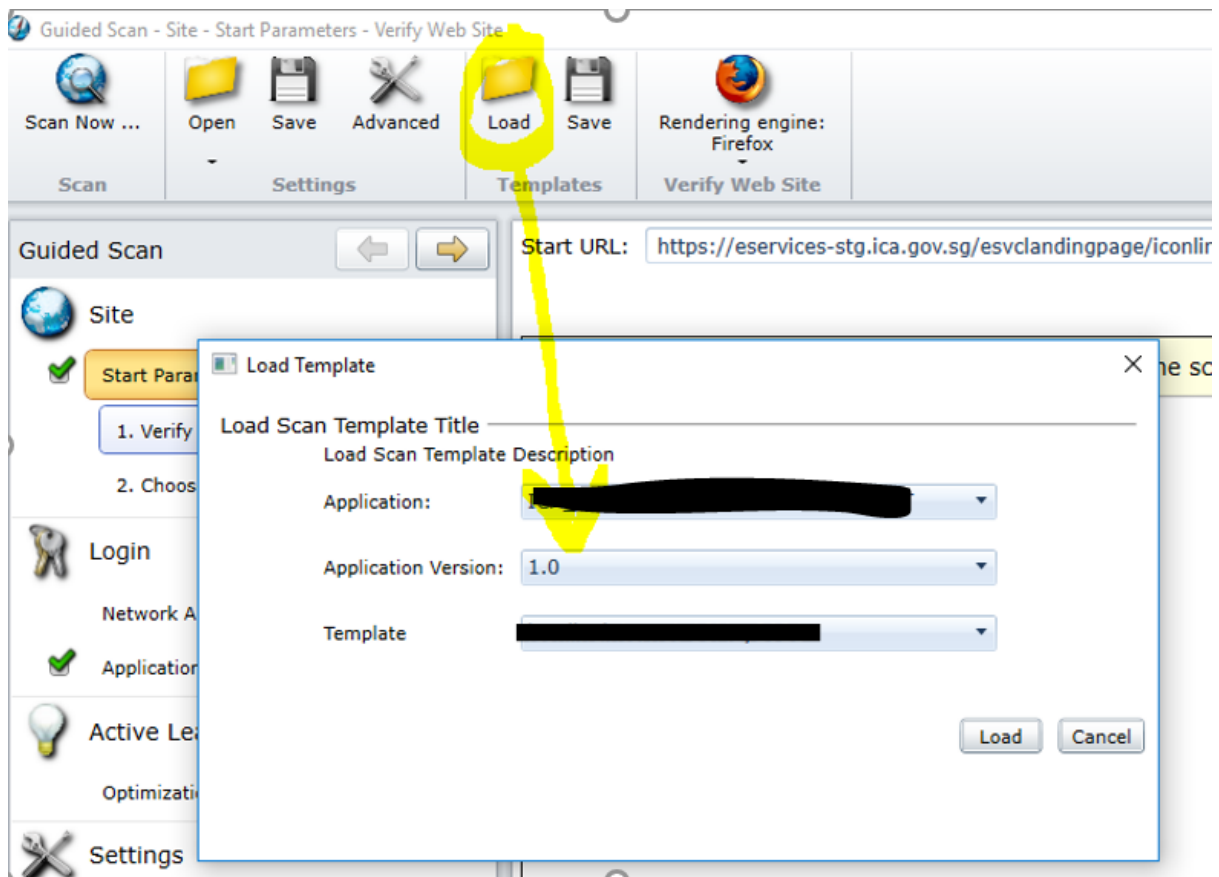
Template Name

[REDACTED]21

Update ID and PASSWORD

Click GUIDE SCAN

Load Template



Change value and save template

