GTTA 2.0 New Features

Table of Contents

TABLE OF CONTENTS 1

TIME TRACKER 2

CHECKLIST TEMPLATES 5

CHECK RELATIONS 8

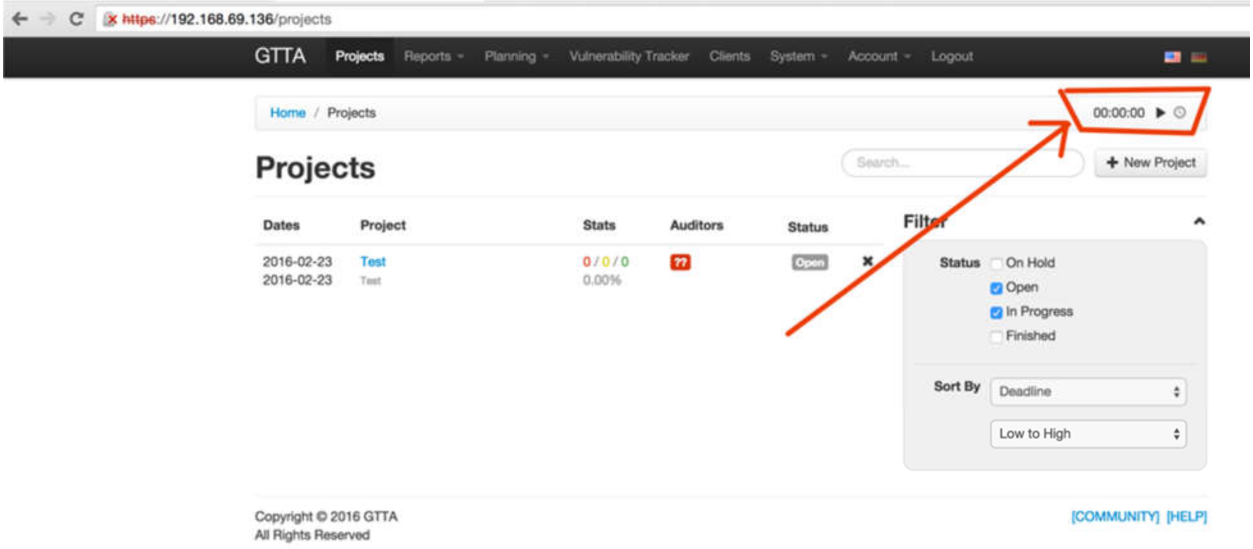
INFORMATION GATHERING 15

PACKAGE SYNCHRONIZATION OVER GIT 17

Time Tracker

Time tracker is used to track how much time user has spent on certain project. We already had time management in previous versions, this version extends this feature.

Figure 1 - Time Tracker Block



https://192.168.69.136/projects

Dates	Project	Stats	Auditors	Status
2016-02-23 2016-02-23	Test Test	0 / 0 / 0 0.00%	??	Open

Filter

Status: □ On Hold ☑ Open ☑ In Progress □ Finished

Sort By: Deadline; Low to High

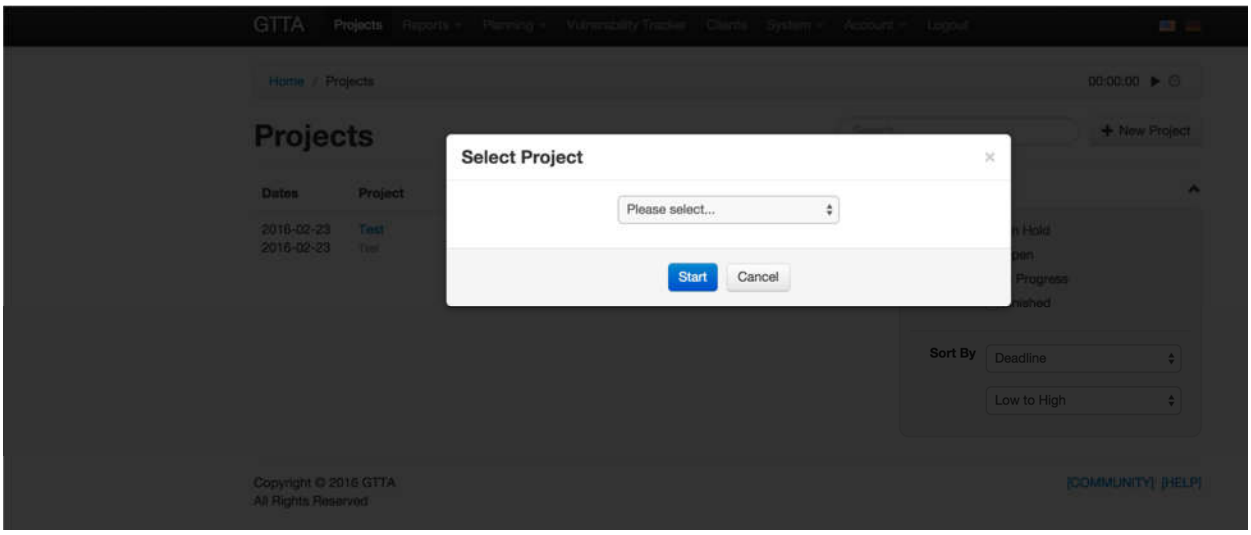
Copyright © 2016 GTTA
All Rights Reserved

On Figure 1 you see the time tracker block that appears on all pages of GTTA. It contains 3 items:

- Timer – shows amount of time spent on a project within current session. When there is no active session, shows “00:00:00”
- Play/Stop icon – starts/stops the session
- Clock icon – shows several latest time tracking sessions (see Figure 6)

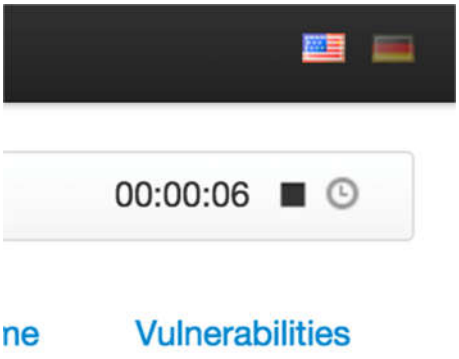
If you press “play” button when outside of the project, the system shows you a pop-up window, where you can select a project, for which the time will be calculated (see below). If you are within some project pages, the timer will start for that project automatically.

Figure 2 - Time Tracker - Select Project



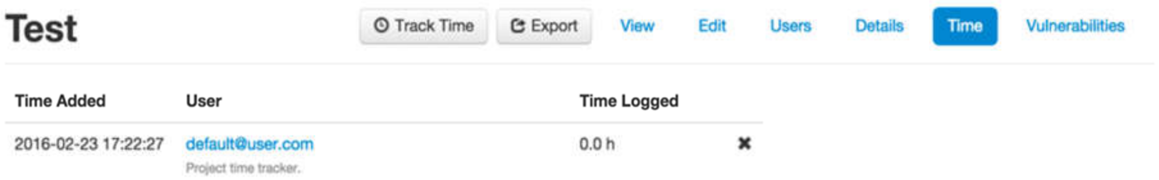
When the timer is launched, you will see the seconds running on the timer (as on picture below). The timer is able to display hours, minutes and seconds. You are able to stop the timer anytime by pressing the stop button. If you close the page (and all other GTTA pages) the timer will stop automatically as well.

Figure 3 - Running Time Tracker Block



In project you can click on "Time" submenu and see previous/current time tracker entries logged for this project. You will see the current session as well – its time will increase while you continue working on it.

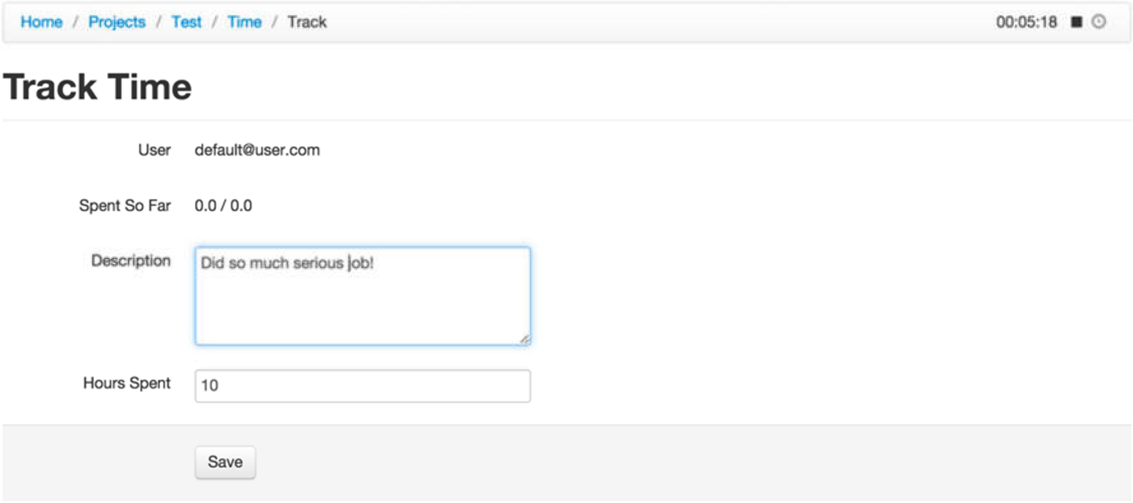
Figure 4 - Time Tracker History



Time Added	User	Time Logged	
2016-02-23 17:22:27	default@user.com Project time tracker.	0.0 h	✖

You can also track time manually (as in previous GTTA versions) by clicking "Track Time" button in project. There you will be able to write a description of the work done and the time spent on it.

Figure 5 - Time Tracker New Entry



Track Time

User default@user.com

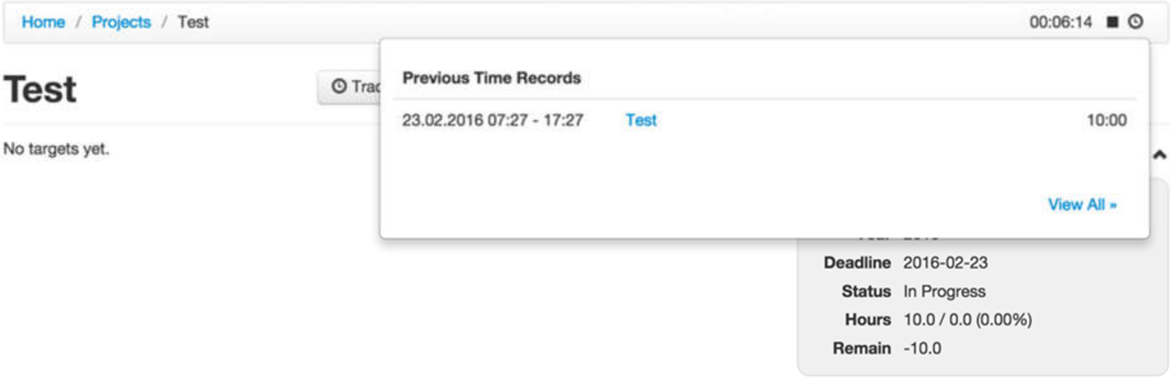
Spent So Far 0.0 / 0.0

Description Did so much serious job!

Hours Spent 10

As was told above, you can view recent time tracker entries by clicking on the clock icon in time tracker block. It shows when the work was started, the name of the project and the time spent on it.

Figure 6 - Time Tracker Recent Entries



No targets yet.

Previous Time Records

23.02.2016 07:27 - 17:27 Test 10:00

Deadline 2016-02-23

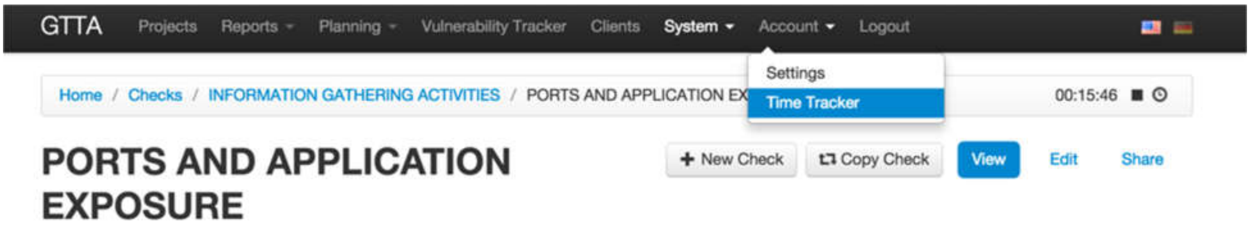
Status In Progress

Hours 10.0 / 0.0 (0.00%)

Remain -10.0

You are also able to view your account’s time records across all project on Account’s “Time Tracker” page.

Figure 7 - Time Tracker Account Access

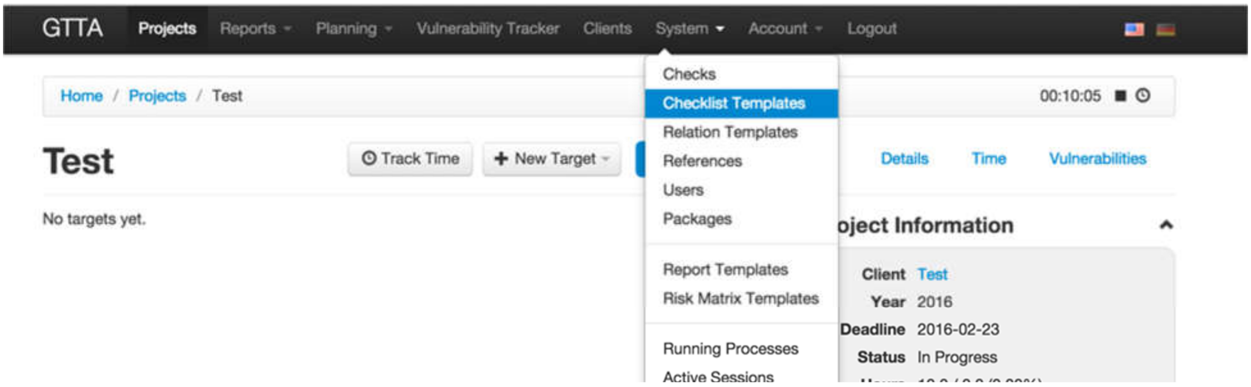


Checklist Templates

Since GTTA 2.0 you can create Checklist Templates – a reduced lists of checks from different categories. For example, you can create “Most Used Tests” template and include 5-10 most used checks in there and assign that template to a target, so only those checks will be visible in that target.

Click on “System” -> “Checklist Templates”.

Figure 8 - Checklist Templates Menu Entry



Test

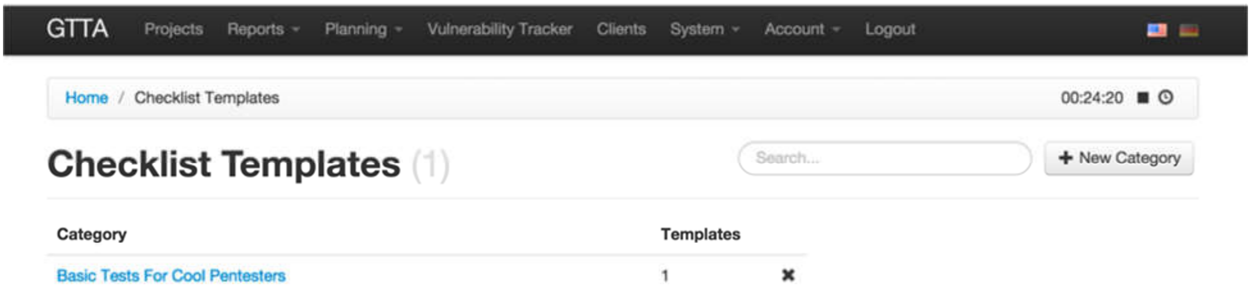
No targets yet.

oject Information

Client Test
Year 2016
Deadline 2016-02-23
Status In Progress

On “Checklist Templates” page you see a list of categories – each checklist template belongs to some category.

Figure 9 - List of Checklist Template Categories

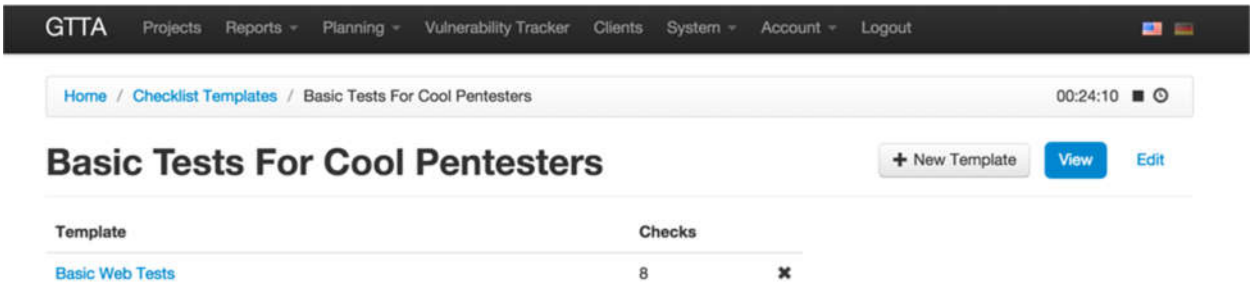


Checklist Templates (1)

Category	Templates	
Basic Tests For Cool Pentesters	1	✖

If you click on category, you will see a list of Checklist Templates in it.

Figure 10 - List of Checklist Templates

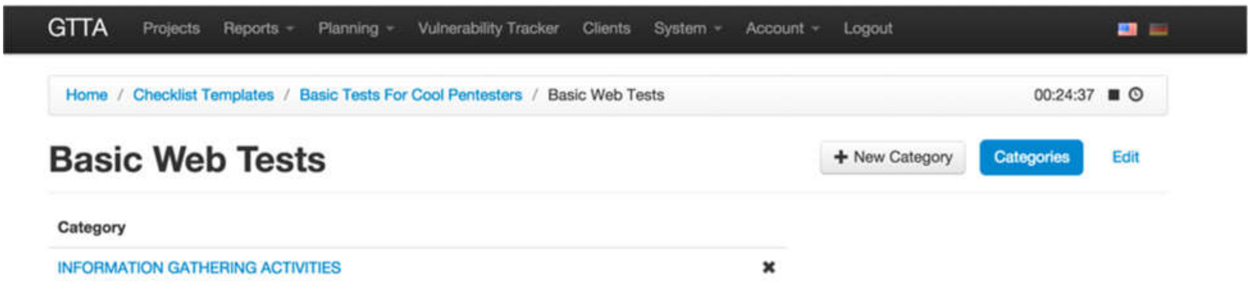


Basic Tests For Cool Pentesters

Template	Checks	
Basic Web Tests	8	✖

Clicking on Checklist Template will show you a list of categories used in that Checklist Template.

Figure 11 - List of Categories in Checklist Template



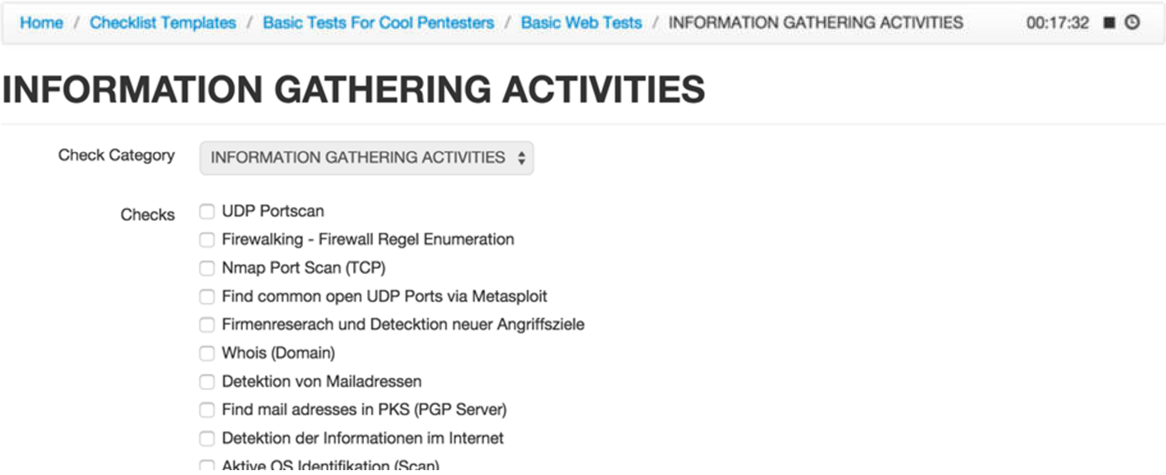
Home / Checklist Templates / Basic Tests For Cool Pentesters / Basic Web Tests 00:24:37

Basic Web Tests

Category	
INFORMATION GATHERING ACTIVITIES	✖

Click on existing category or press “New Category” to add a new category to the Checklist Template. There you will see all checks in the category – select those, which should be tied to this checklist template. You should select at least 1.

Figure 12 - Checks Selection for Category



Home / Checklist Templates / Basic Tests For Cool Pentesters / Basic Web Tests / INFORMATION GATHERING ACTIVITIES 00:17:32

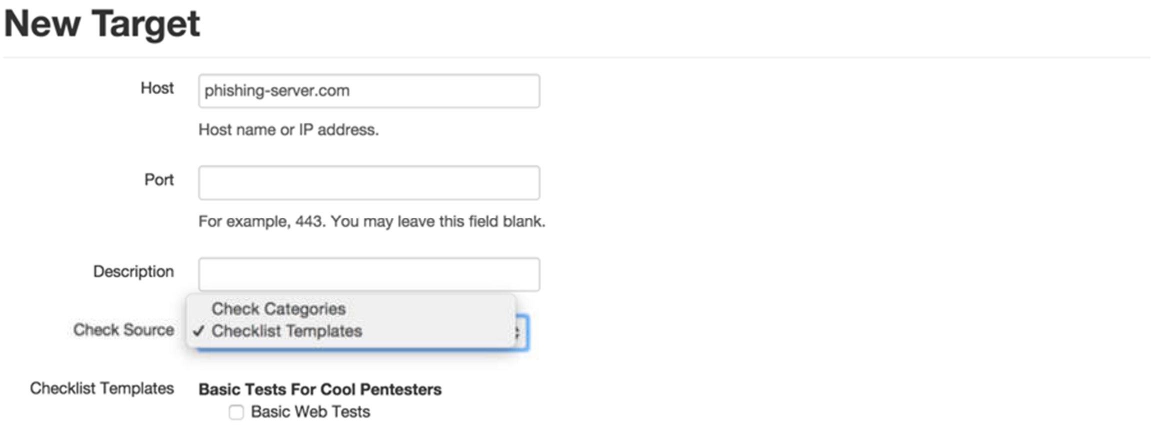
INFORMATION GATHERING ACTIVITIES

Check Category: INFORMATION GATHERING ACTIVITIES

Checks
- □ UDP Portscan
- □ Firewalking - Firewall Regel Enumeration
- □ Nmap Port Scan (TCP)
- □ Find common open UDP Ports via Metasploit
- □ Firmenreserach und Detecktion neuer Angriffsziele
- □ Whois (Domain)
- □ Detektion von Mailadressen
- □ Find mail adresses in PKS (PGP Server)
- □ Detektion der Informationen im Internet
- □ Aktive OS Identifikation (Scan)

After you set up all required checklist templates, you can use them in targets. Just choose “Checklist Templates” as the “Check Source” and check the required Checklist Templates you want to use for this target.

Figure 13 - Use Checklist Templates in Target



New Target

Host: phishing-server.com

Host name or IP address.

Port:

For example, 443. You may leave this field blank.

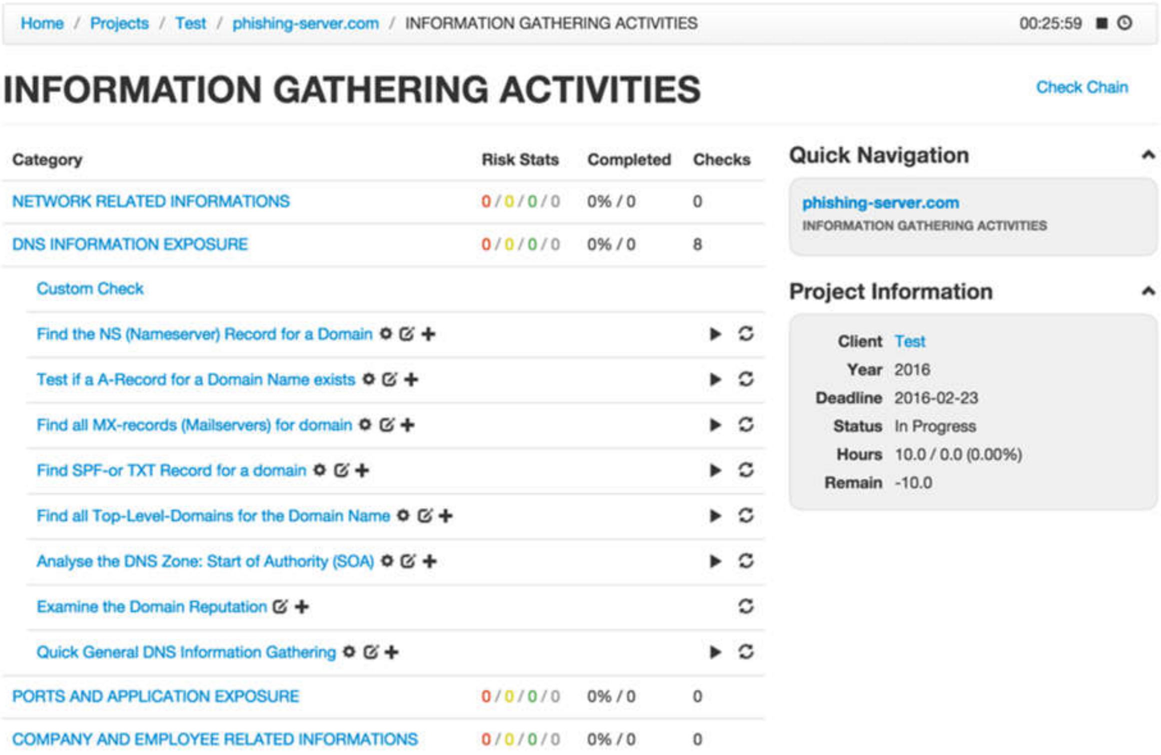
Description:

Check Source:
Check Categories
✓ Checklist Templates

Checklist Templates: **Basic Tests For Cool Pentesters**
- □ Basic Web Tests

After you save the target, you can go to the checklist – only checks that are present in the selected Checklist Template will appear in the checklist.

Figure 14 - Checklist Template in a Project Checklist



Home / Projects / Test / phishing-server.com / INFORMATION GATHERING ACTIVITIES 00:25:59 ■ ⏲

INFORMATION GATHERING ACTIVITIES

Category	Risk Stats	Completed	Checks	
NETWORK RELATED INFORMATIONS	0 / 0 / 0 / 0	0% / 0	0	
DNS INFORMATION EXPOSURE	0 / 0 / 0 / 0	0% / 0	8	
Custom Check				
Find the NS (Nameserver) Record for a Domain				▶ ⟳
Test if a A-Record for a Domain Name exists				▶ ⟳
Find all MX-records (Mailservers) for domain				▶ ⟳
Find SPF-or TXT Record for a domain				▶ ⟳
Find all Top-Level-Domains for the Domain Name				▶ ⟳
Analyse the DNS Zone: Start of Authority (SOA)				▶ ⟳
Examine the Domain Reputation				⟳
Quick General DNS Information Gathering				▶ ⟳
PORTS AND APPLICATION EXPOSURE	0 / 0 / 0 / 0	0% / 0	0	
COMPANY AND EMPLOYEE RELATED INFORMATIONS	0 / 0 / 0 / 0	0% / 0	0	

Quick Navigation

phishing-server.com
INFORMATION GATHERING ACTIVITIES

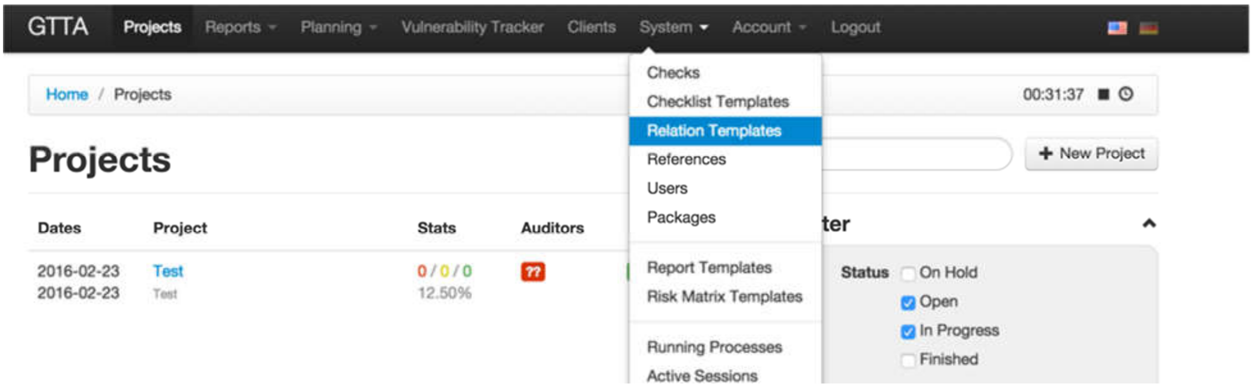
Project Information

Client	Test
Year	2016
Deadline	2016-02-23
Status	In Progress
Hours	10.0 / 0.0 (0.00%)
Remain	-10.0

Check Relations

Check relations are used to connect one's check output with other check's input and autonomously run multiple automated checks without user interaction. You can set up check relations individually for each target or by using a Relation Template. In order to create a Relation Template, go to corresponding menu in System.

Figure 15 - Check Relations Menu Entry



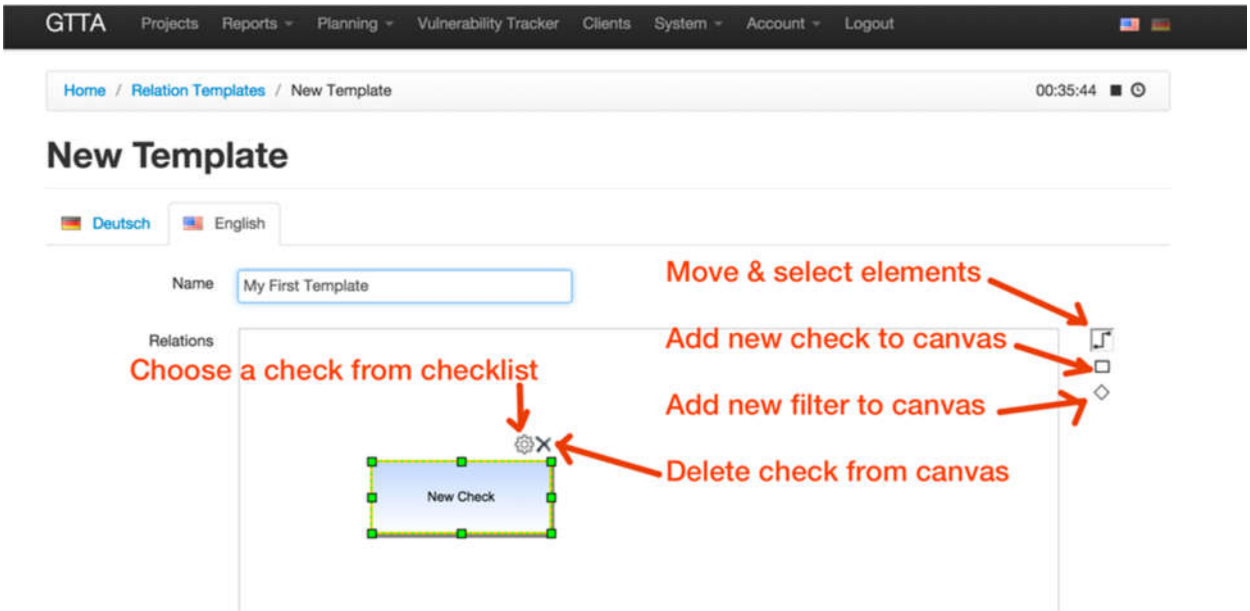
Projects

Dates	Project	Stats	Auditors
2016-02-23 2016-02-23	Test Test	0 / 0 / 0 12.50%	??

Status □ On Hold ☑ Open ☑ In Progress □ Finished

In Relation Templates you either need to click on the existing template, or create a new one. On the template edit page you can see a canvas, where you can add checks and draw relations (connections) between them.

Figure 16 - Check Relations UI



New Template

Name: My First Template

Move & select elements

Add new check to canvas

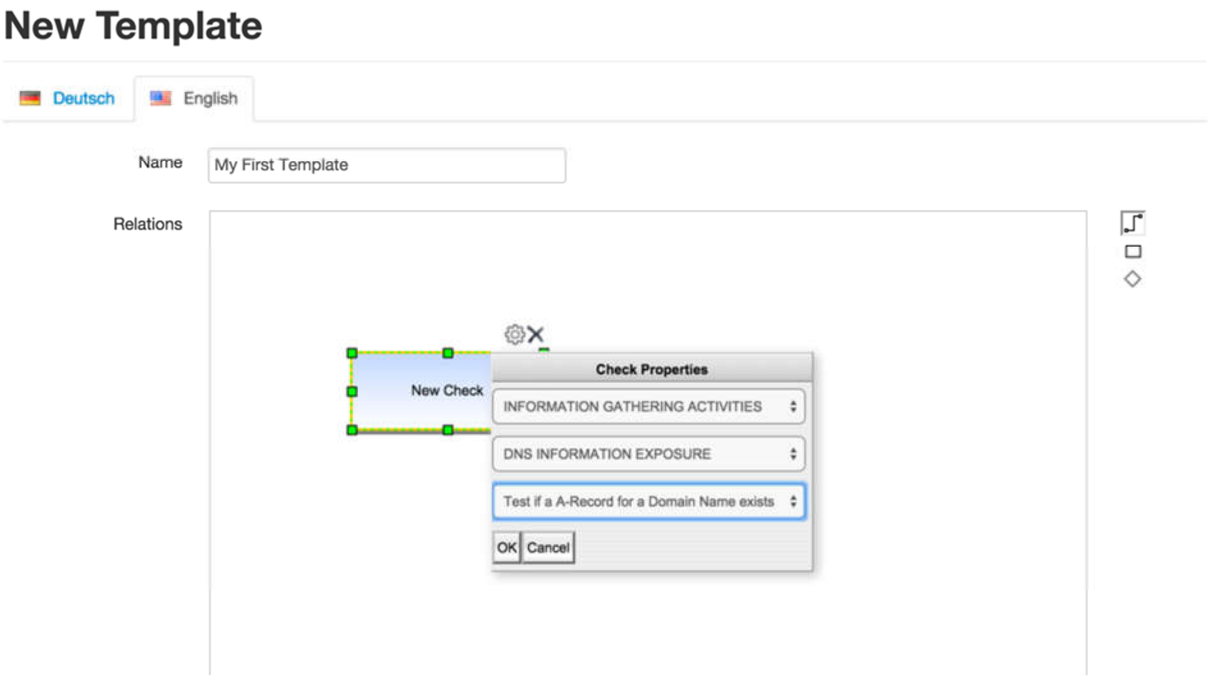
Add new filter to canvas

Choose a check from checklist

Delete check from canvas

Adding checks. In order to add a check, press square button on the right and click somewhere on canvas. After check is added, you should press on "cog" icon above it and the check selector window will appear (see Figure 17 below). There you should select a check, that will be tied to this block.

Figure 17 - Insert Check into Relation Scheme


New Template

Deutsch English

Name My First Template

Relations

New Check

Check Properties

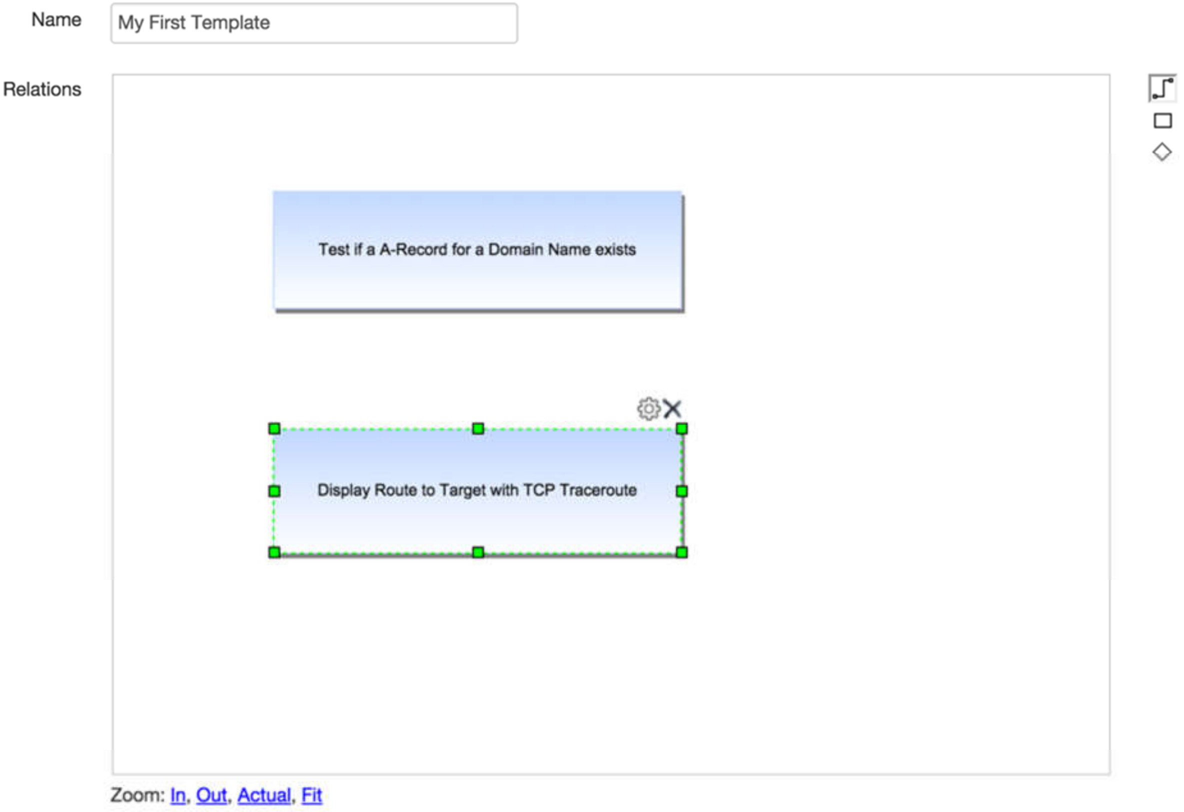
INFORMATION GATHERING ACTIVITIES

DNS INFORMATION EXPOSURE

Test if a A-Record for a Domain Name exists

Add as many checks as you need. You can resize check blocks to fit the text into them. You can add checks from various categories.

Figure 18 - Add As Many Checks As You Need


Name My First Template

Relations

Test if a A-Record for a Domain Name exists

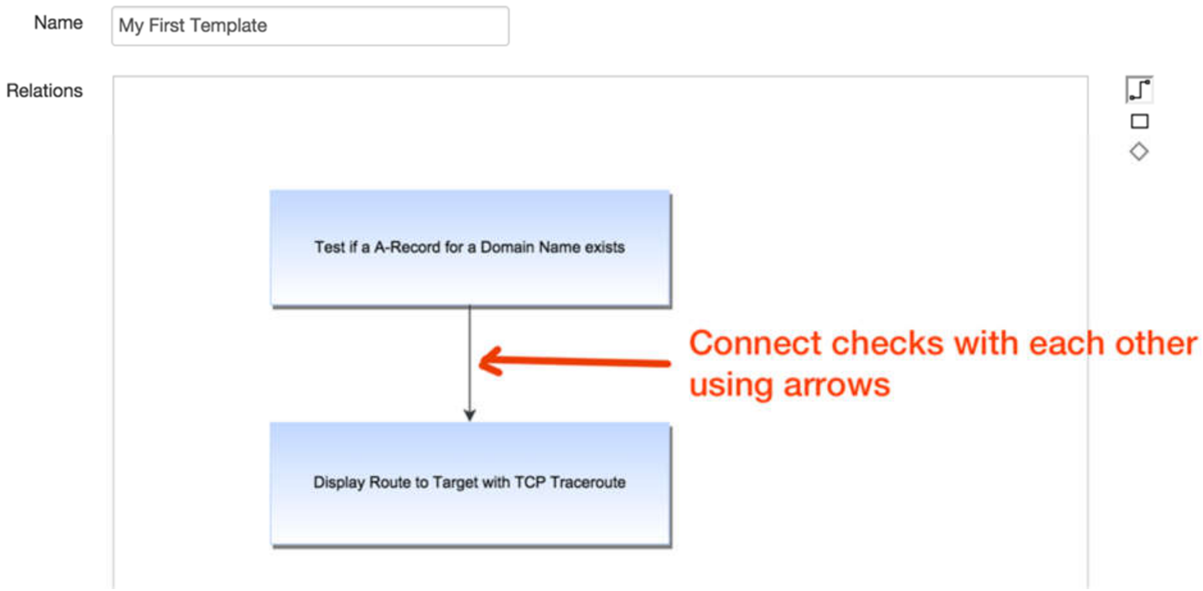
Display Route to Target with TCP Traceroute

Adding connections. After you add checks, you should connect them using arrows. Select some check, which will provide results for the other check. You will see an arrow icon in the middle of the check. Click on it and drag mouse to the check you want to connect to. You will that these checks will be connected with an arrow. That means that the source check will provide some results and send them as input ("override target") for the destination check and the destination check will run automatically.

You can connect as many checks as you need. You can connect one check to multiple checks – and that should work too. The only limitation is to have all checks on canvas connected – there can be no checks without connections.

If you wouldn't like to run the next check automatically and want to pause the chain and see the results produced with previous check, then just click on the check with right mouse button and select "Stop Here" menu item. That means that the after the check receives input from previous check, the chain will stop and wait until you review the results and press the "Start" button again. That can help to avoid various situations when your chain is using inconsistent data for checks.

Figure 19 - Connect Checks Using Arrows



Name: My First Template

Relations
Test if a A-Record for a Domain Name exists
Display Route to Target with TCP Traceroute
Connect checks with each other using arrows

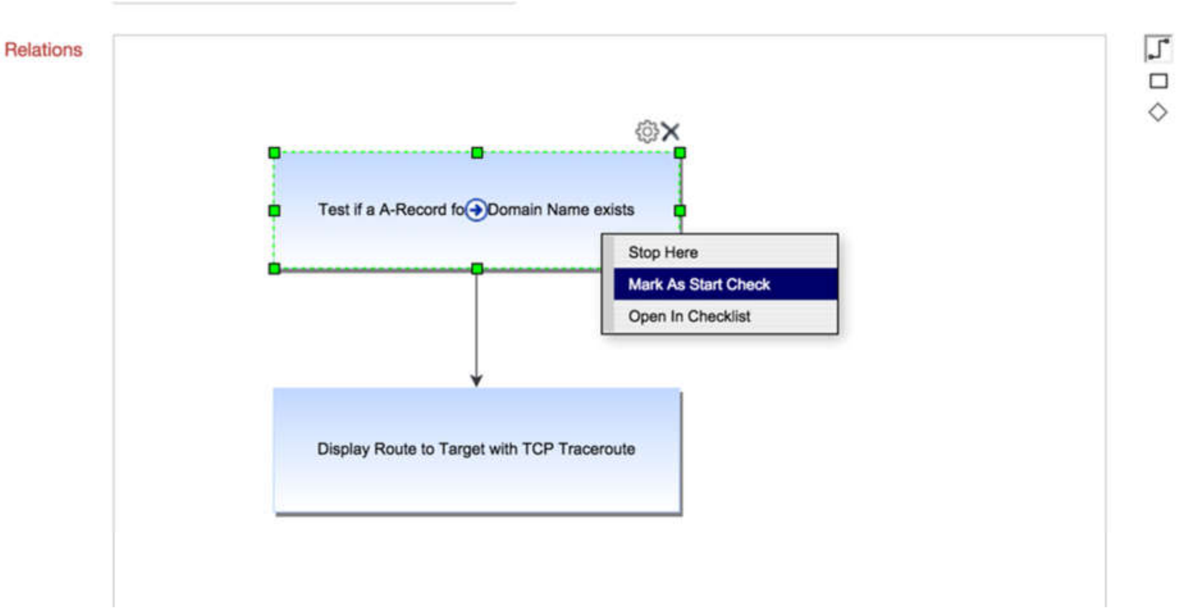
Adding filters. It is possible to "filter" results from one check before sending them to the next check. Currently GTTA supports only "port" filter – it selects only those results, that have the selected ports specified. For example, you specify it to filter ports "80,443". It will get results from the incoming check and see all results ending with ":80" and ":443" and pass them to the next check, other results will be dropped. In order to add a filter to canvas, press a "rhombus" icon on the right and click somewhere on canvas.

Then press the "cog" icon to show filter settings. There you can choose the type of the filter (as I said before, currently we support only Port Filter) and the filtering values. For the Port Filter you can specify ports separated by comma (ex: "80,443,8080"). Then connect this filter with checks, just like you connect other checks. You can connect multiple filters with each other, making the filtering process very complex.

After you add enough checks, filters and connections please select the first check, right click on it and press “Mark As Start Check”. That means that now GTTA knows which check to use as a starting point of this chain. This starting check should have input data (target or “override target”) defined before running the chain.

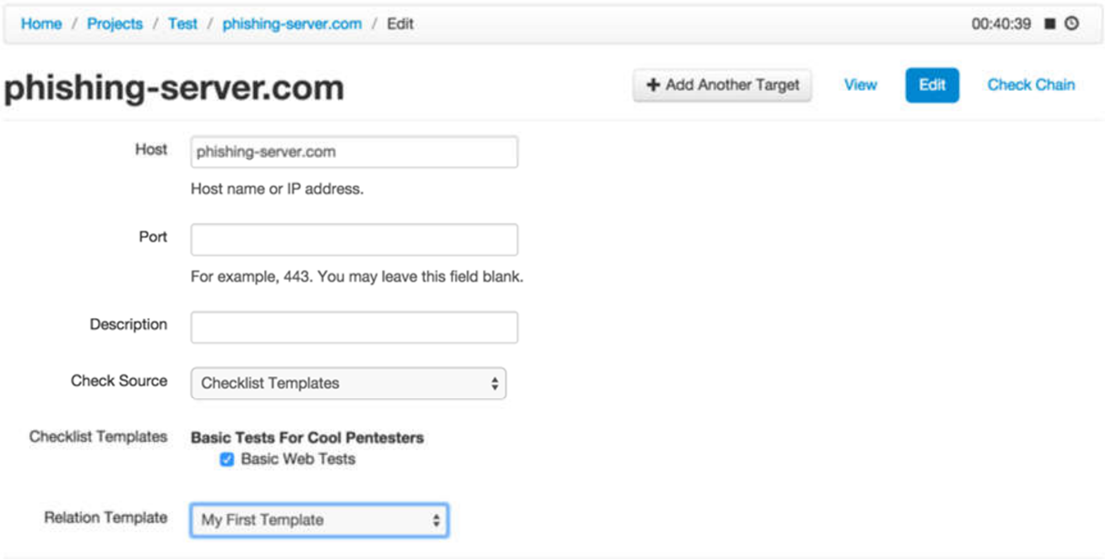
The example chain you see below will get IP address for targets provided and automatically do a traceroute to each IP discovered. The results of this chain will be placed into “traceroute” check result field.

Figure 20 - Add a Start Check


Relations
Test if a A-Record for Domain Name exists
Stop Here
Mark As Start Check
Open In Checklist
Display Route to Target with TCP Traceroute

Ok, now your Relation Template is ready – don’t forget to hit “Save” button below. Now go to project’s target edit page – there you will see a “Relation Template” input. You can either select some existing template, or leave it as “N/A” and add a custom relations scheme to this particular target. In this example we choose “My First Template”.

Figure 21 - Use Relation Template in Target



Home / Projects / Test / phishing-server.com / Edit 00:40:39

phishing-server.com

+ Add Another Target View Edit Check Chain

Host: phishing-server.com
Host name or IP address.

Port:
For example, 443. You may leave this field blank.

Description:

Check Source: Checklist Templates

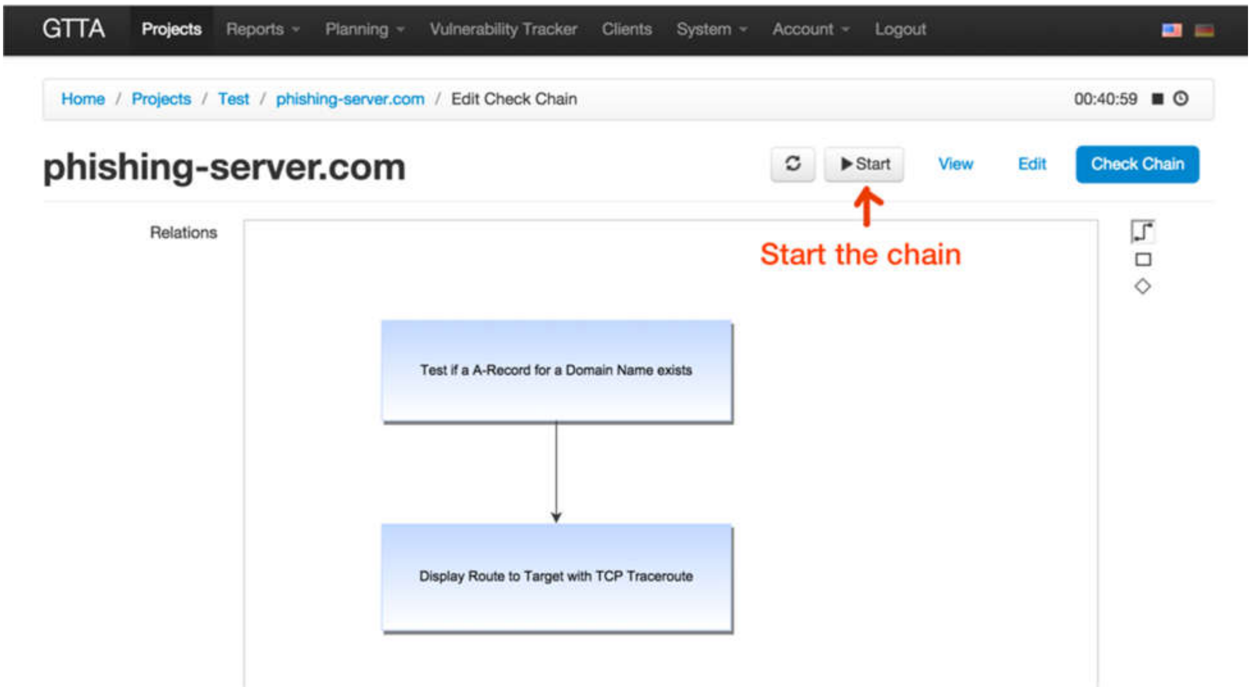
Checklist Templates: **Basic Tests For Cool Pentesters**
☑ Basic Web Tests

Relation Template: My First Template

When you are done with Relation Template selection, press “Check Chain” in target’s menu. If you selected some chain, you will see it on the screen, otherwise you will see a blank canvas, where you can add some checks from start. Even if you have used some Relation Template, you can adjust the chain for this particular target – that won’t affect the initial Relation Template.

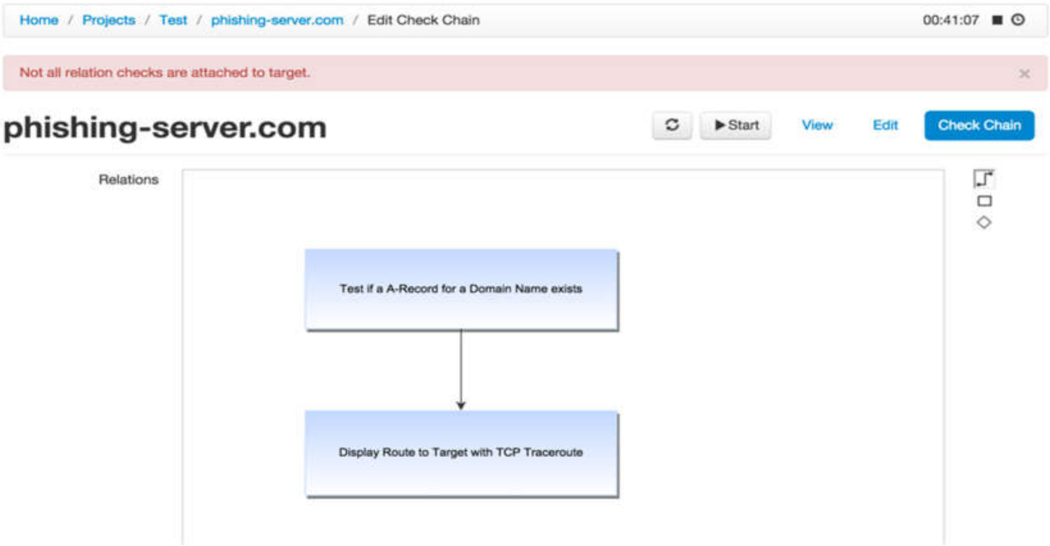
If you feel that you are ready with the chain, just hit “Start” button up top to start the automated chain.

Figure 22 - Start the Chain



After you hit “Start” you can see the error like on the picture below. That means that your chain has some checks, which are not present in categories (or checklist templates) attached to the target. If that happened, make sure you have all required checks attached to the target, then try to run the chain again.

Figure 23 - Not All Relation Checks Are Present

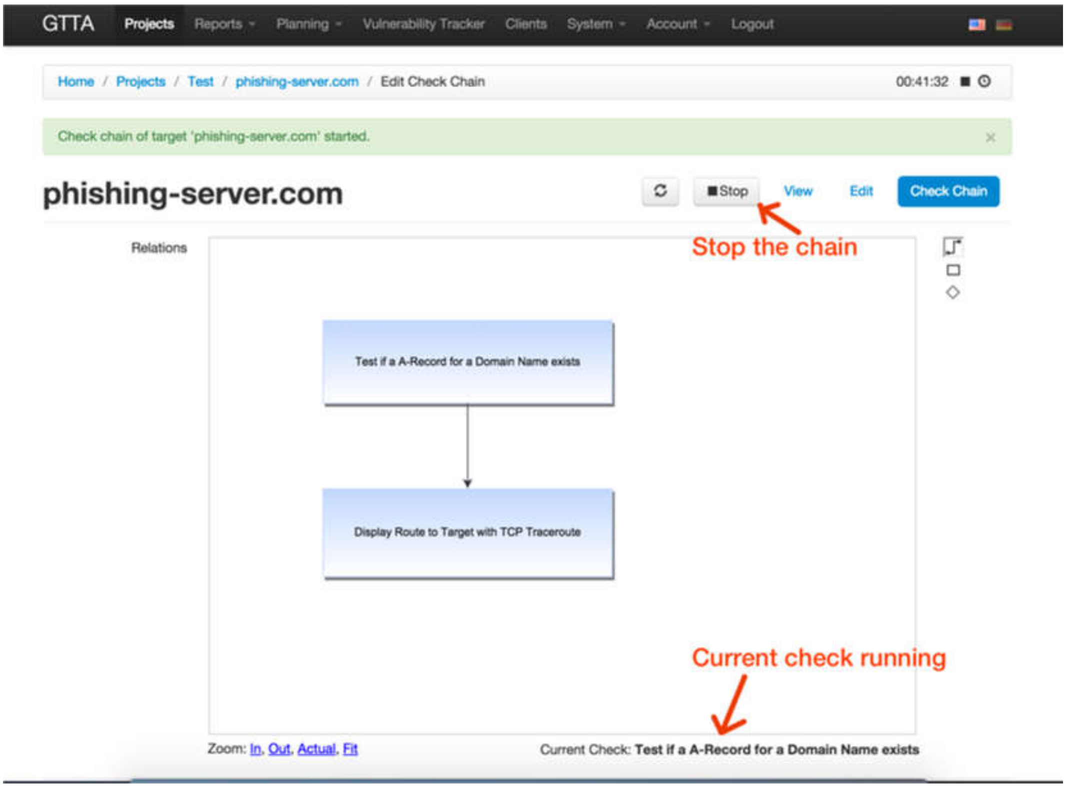


Not all relation checks are attached to target.

Home / Projects / Test / phishing-server.com / Edit Check Chain
00:41:07
phishing-server.com
▶ Start
View
Edit
Check Chain
Relations
Test if a A-Record for a Domain Name exists
Display Route to Target with TCP Traceroute

After the chain has been started, you can stop it anytime and see the current running check name under the canvas (see picture below). The system will walk all checks on the diagram one by one and run them automatically, providing previous check results as an input for the next check (unless you have marked some check as “Stop Here”).

Figure 24 - Chain Started



Check chain of target 'phishing-server.com' started.

Stop the chain

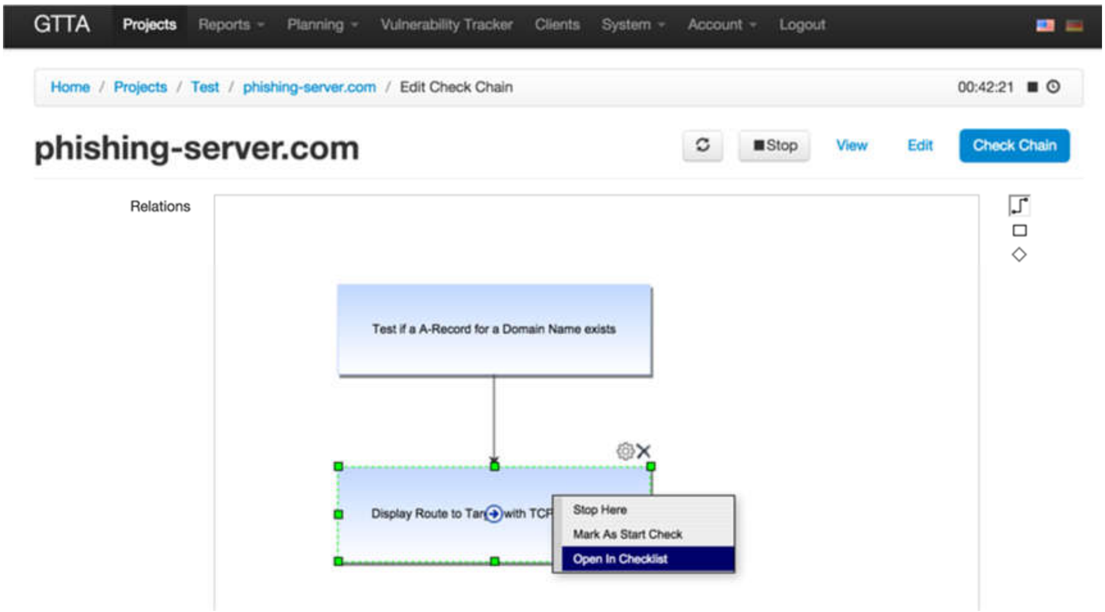
Current check running

Current Check: **Test if a A-Record for a Domain Name exists**

GTTA
Projects
Reports
Planning
Vulnerability Tracker
Clients
System
Account
Logout
Home / Projects / Test / phishing-server.com / Edit Check Chain
00:41:32
phishing-server.com
Stop
View
Edit
Check Chain
Relations
Test if a A-Record for a Domain Name exists
Display Route to Target with TCP Traceroute
Zoom: In, Out, Actual, Fit

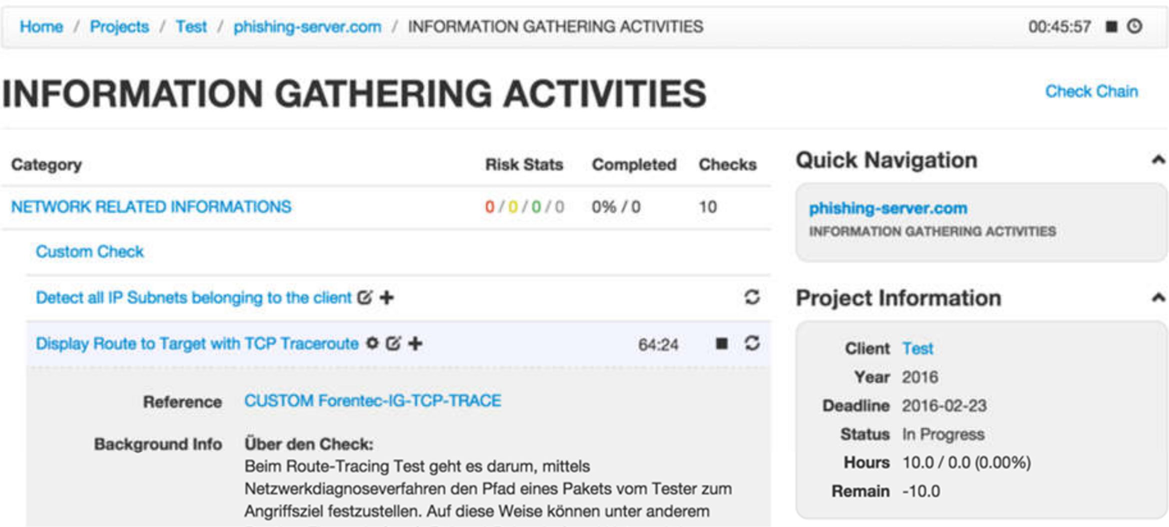
You can click on any check with right mouse button and select “Open in Checklist” menu item – that will open you a traditional checklist, where you can see check’s status, inputs and results.

Figure 25 - Open Particular Check in Checklist



The classical checklist view is the same, as before – you just running the same checks using a diagram. You can stop the check the same way as before, if needed.

Figure 26 - Running Check in Checklist



Home / Projects / Test / phishing-server.com / INFORMATION GATHERING ACTIVITIES 00:45:57 ■

INFORMATION GATHERING ACTIVITIES

Check Chain

Category	Risk Stats	Completed	Checks
NETWORK RELATED INFORMATIONS	0 / 0 / 0 / 0	0% / 0	10

Custom Check

Detect all IP Subnets belonging to the client

Display Route to Target with TCP Traceroute 64:24 ■

Reference CUSTOM Forentec-IG-TCP-TRACE

Background Info Über den Check:
Beim Route-Tracing Test geht es darum, mittels Netzwerkdiagnoseverfahren den Pfad eines Pakets vom Tester zum Angriffsziel festzustellen. Auf diese Weise können unter anderem

Quick Navigation

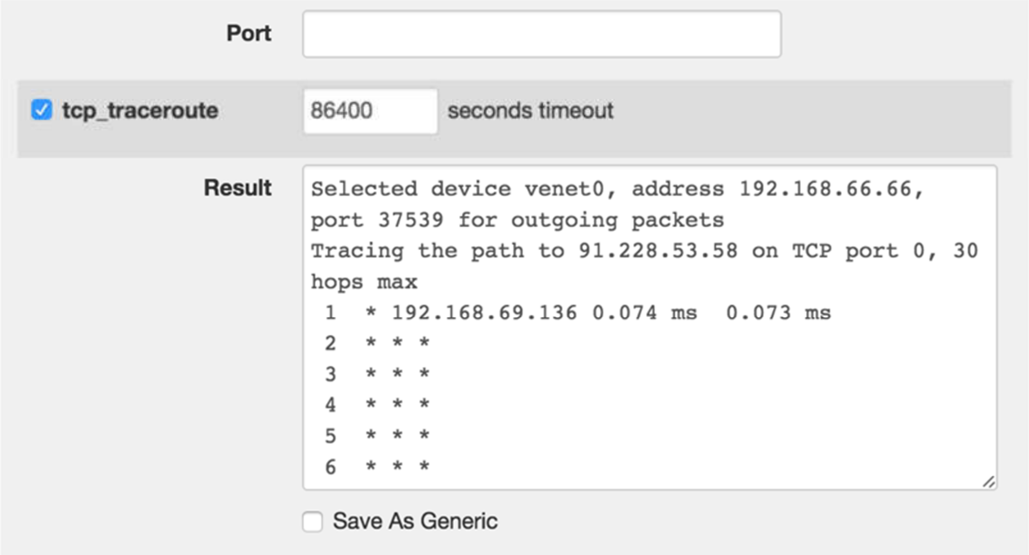
phishing-server.com
INFORMATION GATHERING ACTIVITIES

Project Information

Client	Test
Year	2016
Deadline	2016-02-23
Status	In Progress
Hours	10.0 / 0.0 (0.00%)
Remain	-10.0

After the chain finishes, you see a notification. And when you go to the last check in chain (or to the check, where the chain has stopped), you will see the final results of the chain run in the "Result" field of the final check.

Figure 27 - Chain Result



Port

☑ tcp_traceroute 86400 seconds timeout

Result

```
Selected device venet0, address 192.168.66.66,
port 37539 for outgoing packets
Tracing the path to 91.228.53.58 on TCP port 0, 30
hops max
 1   * 192.168.69.136 0.074 ms  0.073 ms
 2   * * *
 3   * * *
 4   * * *
 5   * * *
 6   * * *
```

□ Save As Generic

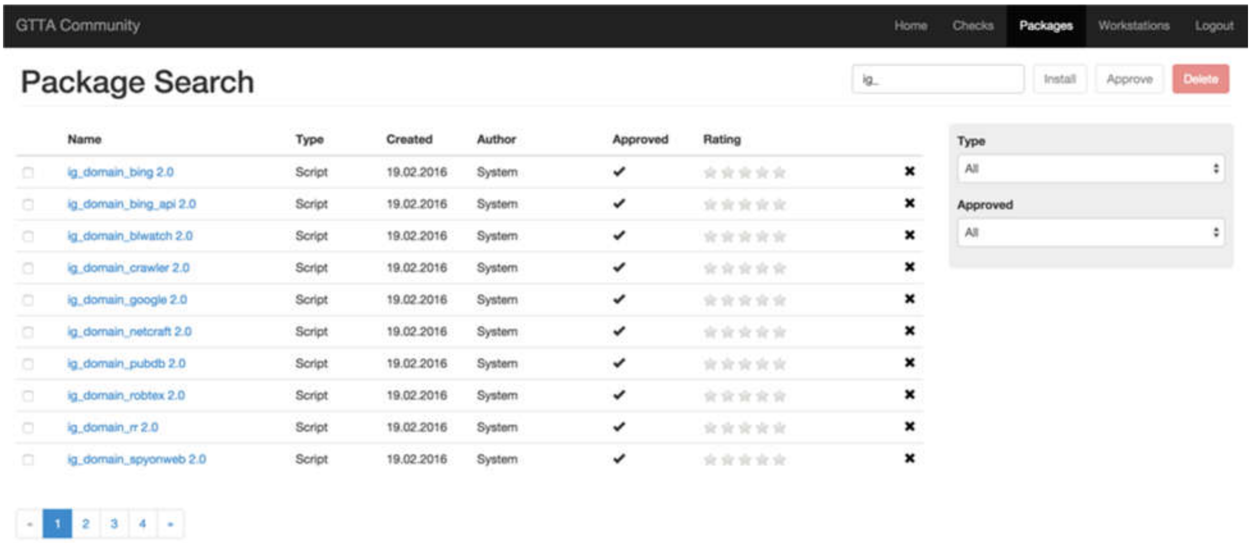
Information Gathering

Check relations function described in previous paragraph are useful for information gathering process. There are some new information gathering scripts – for domain, subdomain, network and email discovery. For example, you can use chained script running for the following scenarios:

- connect network discovery with nmap check to discover company's networks and hosts/ports within those networks automatically
- connect domain discovery with email lookup scripts to get all possible emails on various company's domains
- connect subdomain discovery with nmap, port filter (ports 80, 443 and 8080) and with some web checks – to be able to find web applications on subdomains and test their vulnerabilities automatically
- etc

You can obtain the Information Gathering scripts on Community, as seen on the screenshot below. Unfortunately, there are no checks for these scripts currently, so you should create some checks for them and add scripts to newly created checks to be able to use them in checklist.

Figure 28 - Information Gathering Scripts in Community



Package Search

	Name	Type	Created	Author	Approved	Rating	
□	ig_domain_bing 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_bing_api 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_blwatch 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_crawler 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_google 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_netcraft 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_pubdb 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_robtex 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_rr 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖
□	ig_domain_spyonweb 2.0	Script	19.02.2016	System	✓	☆☆☆☆☆	✖

Type: All

Approved: All

Here is a brief description of all available IG scripts:

- ig_domain_bing – search domains using http://bing.com HTML scraper and domaintools.
- ig_domain_bing_api – search domains using Bing API and domaintools. Bing API key is required.
- ig_domain_blwatch – search domains using http://www.backlinkwatch.com HTML scraper.
- ig_domain_crawler – search domains using website crawler – walk all pages and find all external domains. Manual result review is recommended, as many websites have external links to domains that belong to other companies.
- ig_domain_google – search domains using http://google.com HTML scraper and domaintools.

- ig_domain_netcraft – search domains using http://searchdns.netcraft.com HTML scraper.
- ig_domain_pubdb – search domains using http://pub-db.com HTML scraper.
- ig_domain_robtex – search domains using http://robtex.com HTML scraper.
- ig_domain_rr – search domains using reverseraider software - http://complemento.sourceforge.net/
- ig_domain_spyonweb – search domains using Spyonweb API. Spyonweb API key required.
- ig_domain_yahoo – search domains using http://yahoo.com HTML scraper and domaintools.
- ig_domain_yahoo_api – search domains using Yahoo Search API and domaintools. Yahoo API key required.
- ig_email_bing – search emails using http://bing.com HTML scraper.
- ig_email_bing_api – search emails using Bing API. Bing API key required.
- ig_email_crawler – search emails by walking website links.
- ig_email_dogpile – search emails using http://dogpile.com HTML scraper.
- ig_email_duckduckgo – search emails using http://duckduckgo.com HTML scraper.
- ig_email_exalead – search emails using https://www.exalead.com/search/ HTML scraper.
- ig_email_google – search emails using http://google.com HTML scraper.
- ig_email_hotbot – search emails using http://hotbot.com HTML scraper.
- ig_email_lixam – search emails using http://lixam.de HTML scraper.
- ig_email_omgili – search emails using http://omgili.com HTML scraper.
- ig_email_wotbox – search emails using http://wotbox.com HTML scraper.
- ig_email_yahoo – search emails using http://yahoo.com HTML scraper.
- ig_email_yahoo_api – search emails using Yahoo API. Yahoo API key required.
- ig_email_yandex – search emails using http://yandex.com HTML scraper.
- ig_network_arin – search networks using http://whois.arin.net HTML scraper.
- ig_network_ripe – search networks using https://apps.db.ripe.net HTML scraper.
- ig_subdomain_axfr – search subdomains using AXFR request to NS server
- ig_subdomain_bruteforce – search subdomains using bruteforce
- ig_subdomain_fierce – search subdomains using Fierce tool (http://ha.ckers.org/fierce/)

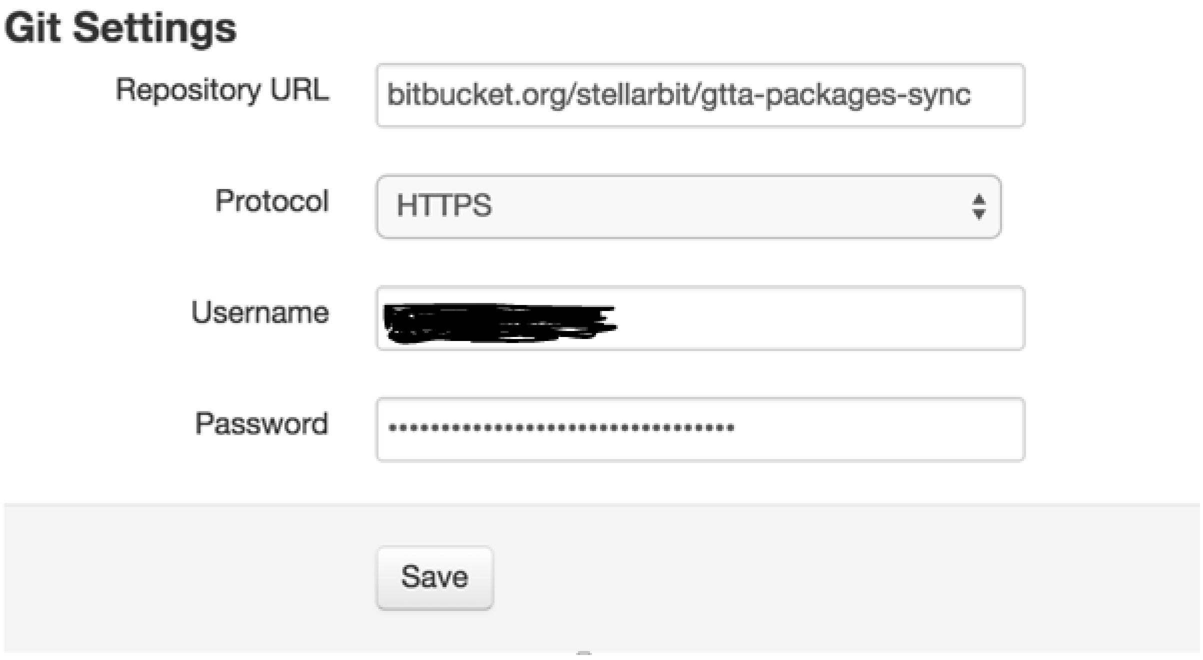
HTML scraper tools use current website HTML output to parse information and if site owners will change the HTML format, the scripts may stop working.

Also some websites (like google.com) ban automated tools from scanning their output, so these tools may eventually stop working.

Package Synchronization over Git

Git synchronization is used to synchronize packages across different workstations using a git repository. In order to setup it, create a git repository on some host, which is accessible from all GTTA workstations. Then go to “System” -> “Settings” and scroll down to “Git Settings” fields. Here you can enter Git Repository URL, the protocol that will be used for connecting to the repository and the login details.

Figure 29 - Git Settings



Git Settings

Repository URL: bitbucket.org/stellarbit/gtta-packages-sync

Protocol: HTTPS

Username: [redacted]

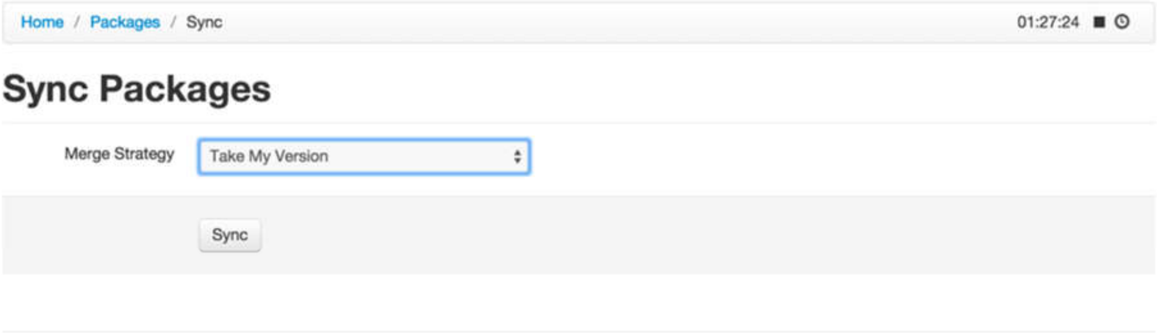
Password: ••••••••••••••••••••••••••••••••••

Go to “System” -> “Packages” and press “Sync” button on the top. You will get to Packages Sync page. There you can select which strategy to use on conflicts (for example, when you and your colleague change the same lines of the same script):

- Take My Version – means that if the remote repository contains changes in the same package lines where you have changes, then the system will keep your version and remote changes will be lost.
- Take Remote Version – means that if the remote repository contains changes in the same lines where you have changed something, then the system will prefer remote changes over yours and you changes will be lost.

Choose the merge strategy which fits your situation and hit the “Sync” button to start the process.

Figure 30 - Syncrhonize Packages

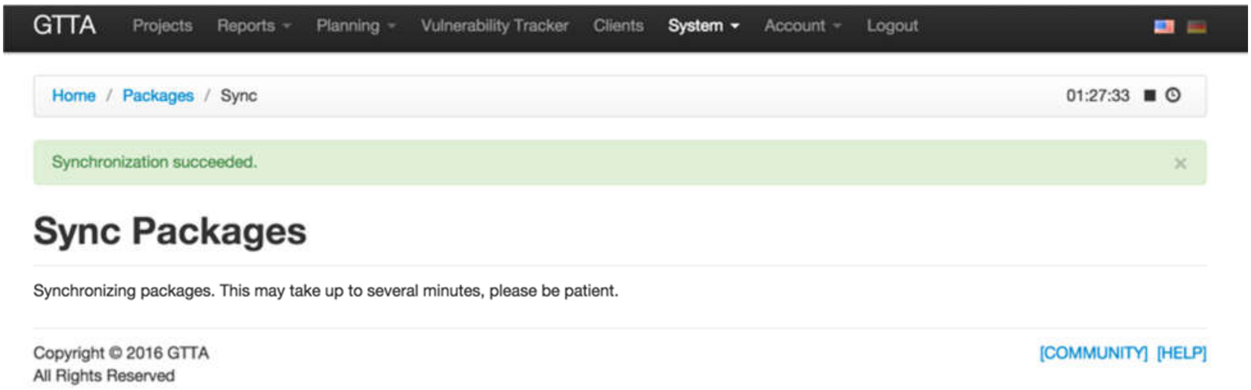


Sync Packages

Merge Strategy: Take My Version

The system will work for a while and show you a success message after the synchronization is completed.

Figure 31 - Well Done



Synchronization succeeded.

Sync Packages

Synchronizing packages. This may take up to several minutes, please be patient.

Copyright © 2016 GTTA
All Rights Reserved