Time and Attack Mapper (TA-Mapper)
Beta Release 0.1

1st Jan, 2009

Author: Debasis Mohanty
www.coffeeandsecurity.com
www.hackingspirits.com

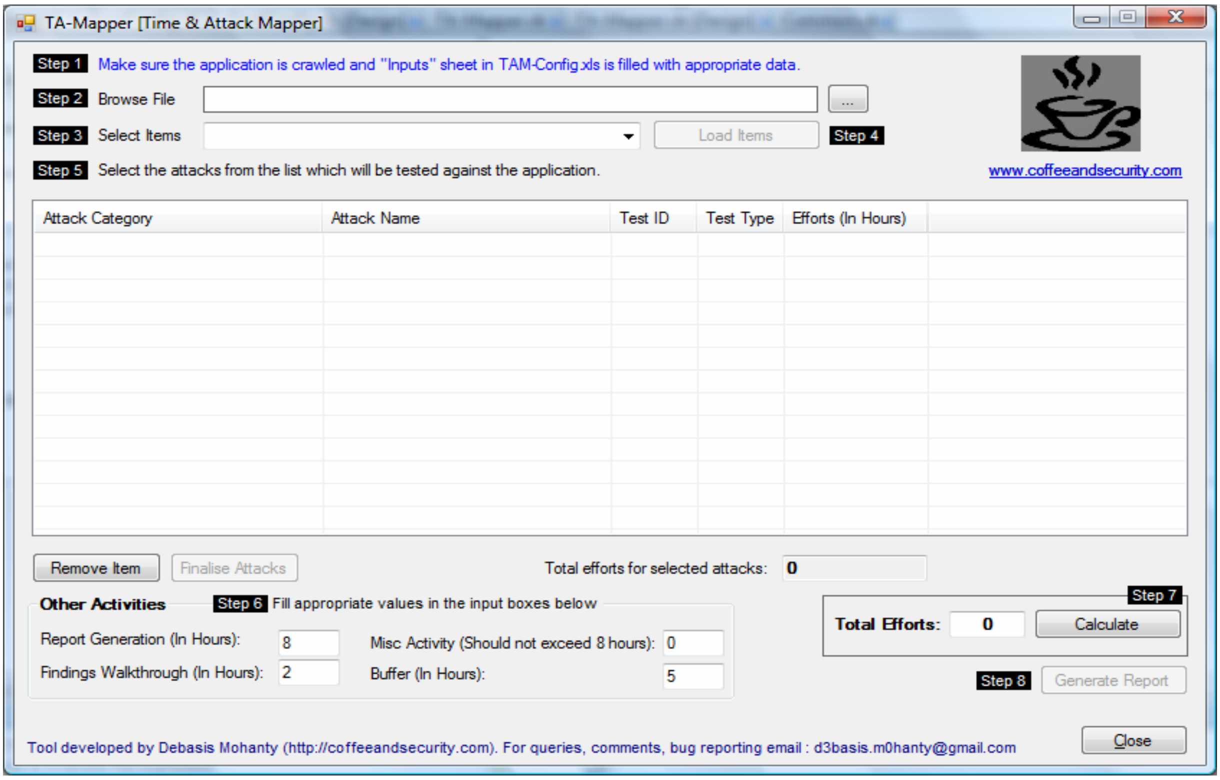
OVERVIEW

Time and Attack Mapper (alternatively known as TA-Mapper) is an effort estimator tool for blackbox security assessment (or Penetration Testing) of applications. This tool provides more accurate estimation when compared to rough estimation. Penetration testers who always has hard time explaining/justifying the efforts charged (or quoted) to their customers can find this tool handy by able to calculate efforts with greater accuracy required for application penetration testing.

In addition, this tool helps application pen-testers in itemizing their penetration testing efforts into micro-level and provides more clarity of their pen-testing activities. In future I have plans to extend this tool ability to generate test cases.

I wrote this tool back in 2004 to support some of my freelancing assessment. I was intrigued to write this tool when I was asked by one of my Fortune 100 customer to justify efforts quoted against the activities for a penetration testing assignment. It not just helped me win the project but also help me educate the customer in knowing the activities involved at the micro-level. After making few changes in the tool I thought I have kept it private too long and its right time to share it with the world.

Read further to learn more about the tool.



TA-Mapper [Time & Attack Mapper]

Step 1 Make sure the application is crawled and "Inputs" sheet in TAM-Config.xls is filled with appropriate data.

Step 2 Browse File

Step 3 Select Items

Step 4

Step 5 Select the attacks from the list which will be tested against the application.

www.coffeeandsecurity.com

Attack Category	Attack Name	Test ID	Test Type	Efforts (In Hours)

Total efforts for selected attacks: 0

Other Activities

Step 6 Fill appropriate values in the input boxes below

Report Generation (In Hours): 8

Findings Walkthrough (In Hours): 2

Misc Activity (Should not exceed 8 hours): 0

Buffer (In Hours): 5

Step 7

Total Efforts: 0

Step 8

Tool developed by Debasis Mohanty (http://coffeeandsecurity.com). For queries, comments, bug reporting email : d3basis.m0hanty@gmail.com

TOOL INTERNALS

The strength of this tool lies in the background factors that were taken into consideration which helps in making an accurate estimation.

The tool makes it calculation based on various test types set against individual attacks. Almost all attacks performed against an application involve different factors in the way it is tested. Hence those different factors make it more complex to make a generic calculation of efforts. Around seven different test types were identified where different complex factors were mapped and grouped to come up with a mathematical formula for calculating efforts against individual attacks.

Different test types (T1 – T7) are listed below

T1 - Calculated based on total no. of get/post parameter
T2 - No. of instances cannot be determined without a thorough scan
T3 - Can be calculated based on URLs
T4 - Occurrences uncertain (Estimation based on probability of occurrences of potential area of threats)
T5 - Assumed time derived from T1 (Errors can be generated by fault injection via parameters)
T6 - No. of privilege functions
T7 - Small test time required (Test that required time less than 5 mins)

More details about the mathematical formula used for different test types can be found in the “Formula” sheet in TAM-Config.xls.

Lot more details needs to be updated here which I will update in my next release of this tool. Right now I feel tool lazy to update this manual but I am sure this tool is self explanatory and you will not find much difficulty in understanding it.

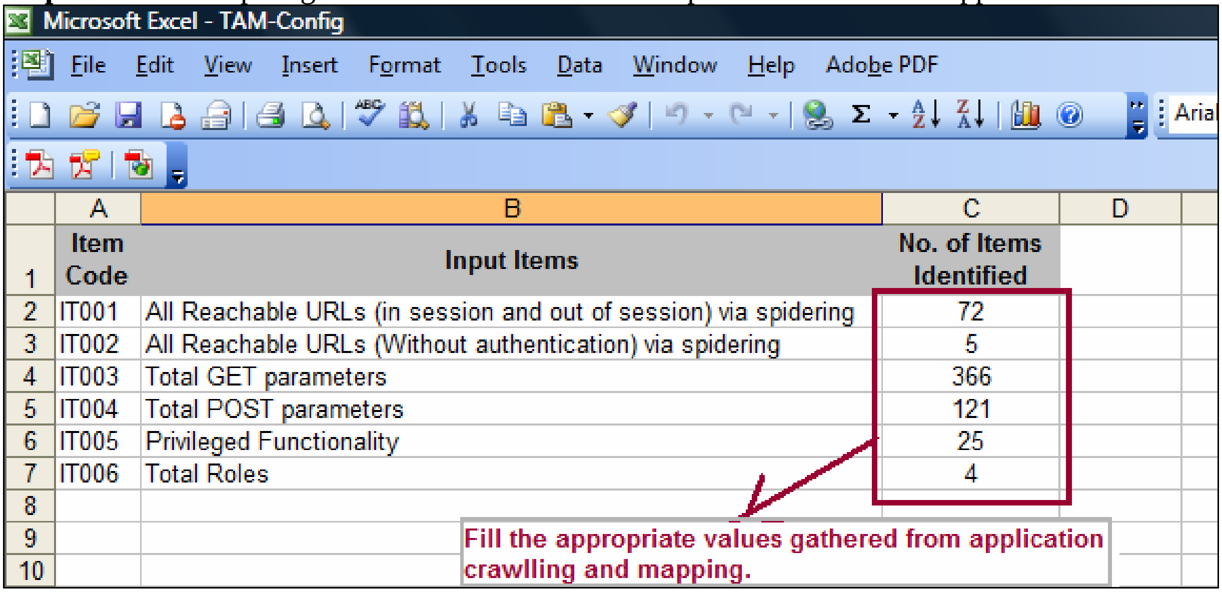
USAGE INSTRUCTIONS

Phase I: Application crawling and Inputs Gathering – The application needs to be crawled to gather inputs that can be feed into to tool to get an accurate estimation of efforts required to perform a BlackBox security assessment against the application.

For application crawling any standard intercepting proxy (like Paros) or any other web application crawler that has support for both HTTP/HTTPS crawling and have provision to count details like number of URLs crawled, number of GET/POST parameters etc can be used here.

Phase II: Effort Estimation

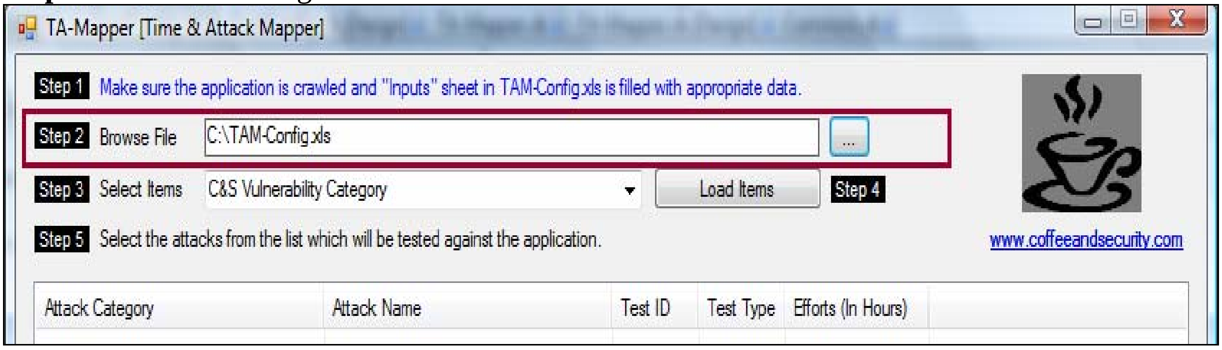
Step 1: Feed the inputs gathered in Phase I into the “Inputs” sheet of TA-Mapper.xls.



	A	B	C	D
1	Item Code	Input Items	No. of Items Identified	
2	IT001	All Reachable URLs (in session and out of session) via spidering	72	
3	IT002	All Reachable URLs (Without authentication) via spidering	5	
4	IT003	Total GET parameters	366	
5	IT004	Total POST parameters	121	
6	IT005	Privileged Functionality	25	
7	IT006	Total Roles	4	
8				
9				
10				

Fill the appropriate values gathered from application crawlling and mapping.

Step 2: Load TA-Config.xls in the tool.



Step 1 Make sure the application is crawled and "Inputs" sheet in TAM-Config.xls is filled with appropriate data.

Step 2 Browse File C:\TAM-Config.xls

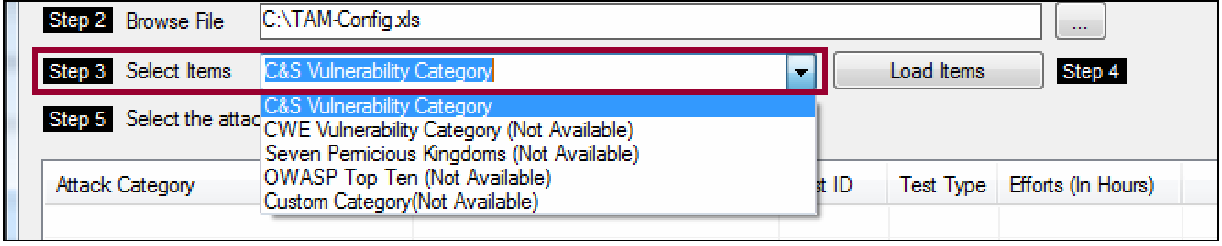
Step 3 Select Items C&S Vulnerability Category

Step 4

Step 5 Select the attacks from the list which will be tested against the application.

Attack Category	Attack Name	Test ID	Test Type	Efforts (In Hours)

Step 3: Select the appropriate vulnerability category
Step 4: Click on the "Load Items" button

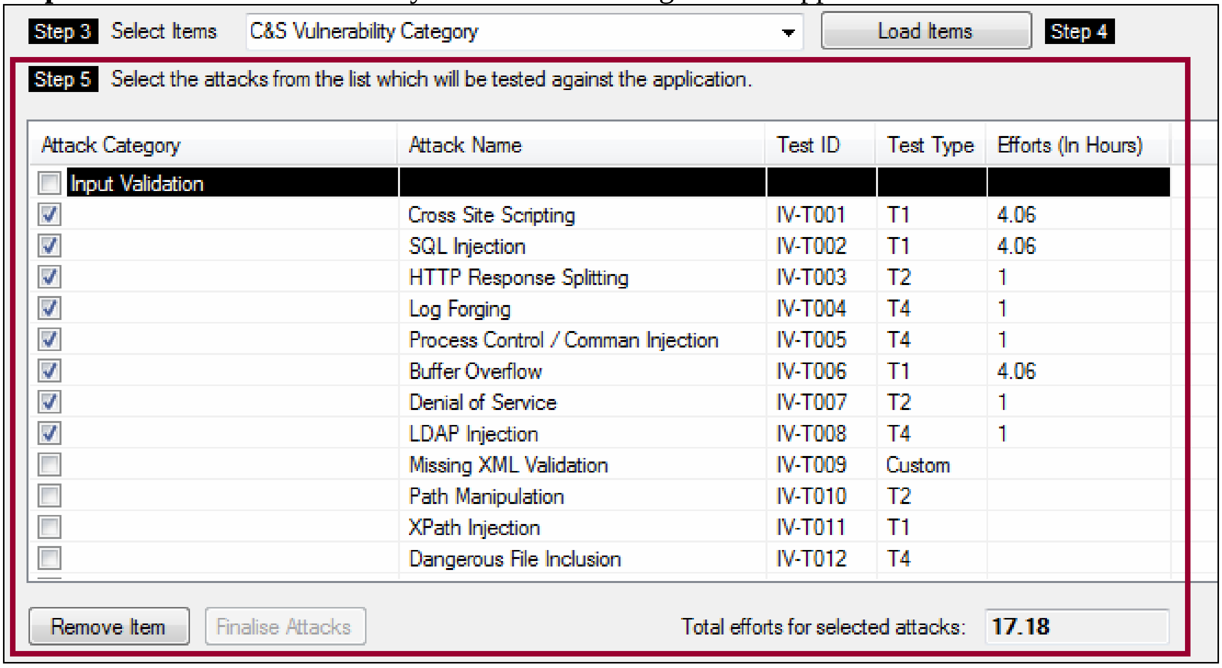


Step 2
Browse File
...
Step 3
Select Items
Load Items
Step 4
Step 5
Select the attac
C&S Vulnerability Category
CWE Vulnerability Category (Not Available)
Seven Pernicious Kingdoms (Not Available)
OWASP Top Ten (Not Available)
Custom Category(Not Available)
Attack Category
t ID
Test Type
Efforts (In Hours)

Browse File: C:\TAM-Config.xls

Select Items: C&S Vulnerability Category

Step 5: Select the attacks which you want to check against the application



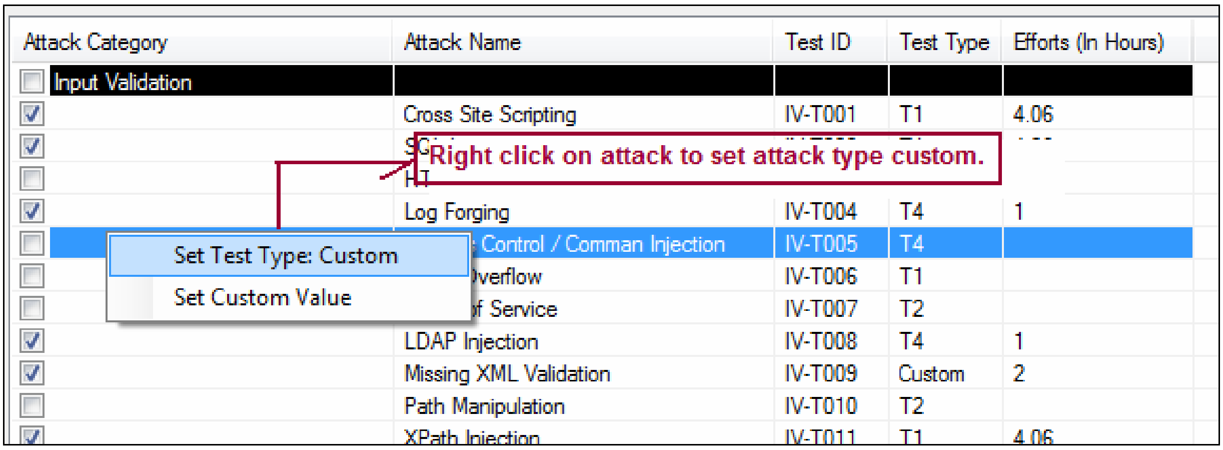
Select Items: C&S Vulnerability Category

Select the attacks from the list which will be tested against the application.

Attack Category	Attack Name	Test ID	Test Type	Efforts (In Hours)
☐ Input Validation				
☑	Cross Site Scripting	IV-T001	T1	4.06
☑	SQL Injection	IV-T002	T1	4.06
☑	HTTP Response Splitting	IV-T003	T2	1
☑	Log Forging	IV-T004	T4	1
☑	Process Control / Comman Injection	IV-T005	T4	1
☑	Buffer Overflow	IV-T006	T1	4.06
☑	Denial of Service	IV-T007	T2	1
☑	LDAP Injection	IV-T008	T4	1
☐	Missing XML Validation	IV-T009	Custom	
☐	Path Manipulation	IV-T010	T2	
☐	XPath Injection	IV-T011	T1	
☐	Dangerous File Inclusion	IV-T012	T4	

Total efforts for selected attacks: **17.18**

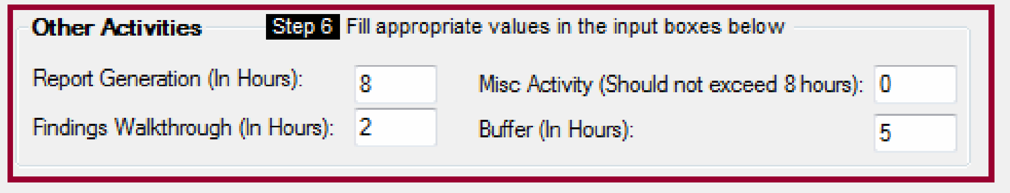
To set test type as custom for an attack right click mouse and select the appropriate option from the context menu.



Attack Category	Attack Name	Test ID	Test Type	Efforts (In Hours)
☐ Input Validation				
☑	Cross Site Scripting	IV-T001	T1	4.06
☑	S			
☐	HT			
☑	Log Forging	IV-T004	T4	1
☐	Control / Comman Injection	IV-T005	T4	
☐	verflow	IV-T006	T1	
☐	f Service	IV-T007	T2	
☑	LDAP Injection	IV-T008	T4	1
☑	Missing XML Validation	IV-T009	Custom	2
☐	Path Manipulation	IV-T010	T2	
☑	XPath Injection	IV-T011	T1	4.06

To set custom value, select "set custom value" option in the context menu.

Step 6: Set the values for other activities



Other Activities

Step 6 Fill appropriate values in the input boxes below

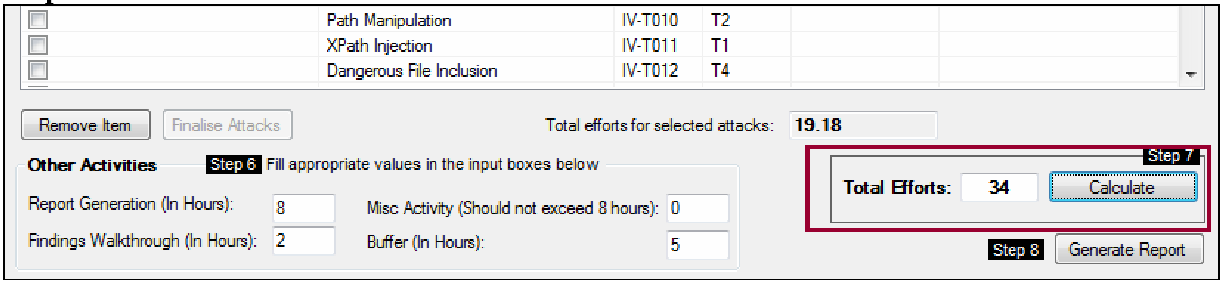
Report Generation (In Hours): 8

Findings Walkthrough (In Hours): 2

Misc Activity (Should not exceed 8 hours): 0

Buffer (In Hours): 5

Step 7: Set the values for other activities



☐	Path Manipulation	IV-T010	T2
☐	XPath Injection	IV-T011	T1
☐	Dangerous File Inclusion	IV-T012	T4

Total efforts for selected attacks: 19.18

Other Activities

Step 6 Fill appropriate values in the input boxes below

Report Generation (In Hours): 8

Findings Walkthrough (In Hours): 2

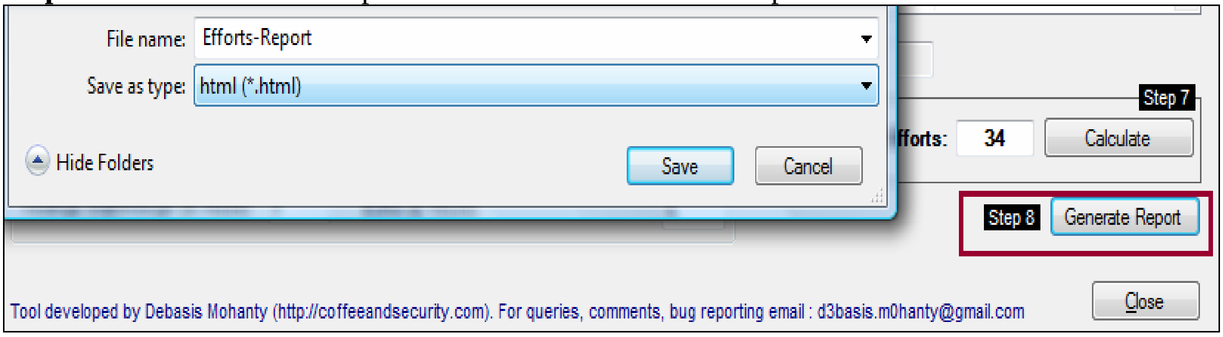
Misc Activity (Should not exceed 8 hours): 0

Buffer (In Hours): 5

Step 7 **Total Efforts:** 34

Step 8

Step 8: Generate itemized report – Click on the “Generate Report” button



File name: Efforts-Report

Save as type: html (*.html)

Step 7 **fforts:** 34

Step 8

Tool developed by Debasis Mohanty (http://coffeeandsecurity.com). For queries, comments, bug reporting email : d3basis.m0hanty@gmail.com

WISH LIST

Below are the lists of items that will be included in the future releases

- Include advance user estimation option
- Platform specific calculation
- Architecture/design specific calculation
- Include Effort Optimization Option: Which will make estimation based on no. of resources / automated - manual test / parallel activities / activity ordering based on its effectiveness of test

ABOUT AUTHOR

Debasis Mohanty
Email: d3basis.m0hanty@gmail.com
To know more about me and my work visit
www.hackingspirits.com and www.coffeeandsecurity.com

Feel free to email me your comments, suggestions, bug reports in the above email id. In case you would like to support my work by your donation then visit http://coffeeandsecurity.com/donate.aspx