

Intern Requirement

No. of students required	1
Preferred Discipline	<ul style="list-style-type: none">• Computing
Prerequisites/ Skills Required	<ul style="list-style-type: none">• Interest in security and testing• Programming and scripting skills (C/C++, Python)• Knowledge of the following would be an advantage<ul style="list-style-type: none">- Assembly language (x86)- Constraint solving

Project Details

Title	Security Assessment of Software by Dynamic Test Case Generation
Overview/Background	<p>Attackers exploit insecure software to gain unauthorised access to machines. Such access allows them to steal confidential information and bring down critical infrastructures. Many formal program analysis and testing methodologies exist to help uncover vulnerabilities in applications during development.</p> <p>A newer methodology is Whitebox Fuzzing, or Dynamic Test Case Generation, which is able to discover vulnerabilities that usually cannot be found by other methods.</p>
Objectives/Scope/ Deliverables	<p>The objective of the project is to automate the dynamic testing processes and improve existing Whitebox Fuzzing techniques.</p> <p>The scope of the project will cover:</p> <ul style="list-style-type: none">• understanding Whitebox Fuzzing and analysing existing techniques• proposing and implementing an automated solution• proposing and implementing improvements to the different techniques employed by Whitebox Fuzzing such as<ul style="list-style-type: none">- better algorithms to rank files in a corpus according to how different they are from a reference test file- adding support for indirect tainting in the dynamic taint analysis techniques- better algorithms that can identify potential vulnerabilities in a run trace and model them using constraints <p>The deliverables will include :</p> <ul style="list-style-type: none">• fully annotated source code (written using the language of choice) and compiled binaries if applicable, that implement the proposed automation and improvements• documentation of the research and development process, the rationale behind the design, and the time savings and increased effectiveness as a result of automation and better techniques• a summary presentation and a proof-of-concept demonstration of the above
Project Duration	6 months