**Fuzz Testing**

**1 Суть метода**

Fuzz Testing(fuzzing, фаззинг) – методика тестирования, при которой на вход программы подаются невалидные, непредусмотренные или случайные данные. Это своего рода стрессовое тестирование программы.

Смысл такой проверки сводится к тому, что программист не знает, какие данные будут переданы приложению/протоколу/функции, поэтому его задача предусмотреть и проверить как можно больше вариантов. Если происходит зависание, крах, утечка памяти или другое ненормальное поведение, то можно говорить об обнаружении проблемы, и высока вероятность, что это проблема в безопасности.

По способу манипуляции с данными фаззинг распределяется на генерацию и мутацю.

1. Генерация — это случайным образом придуманный набор байтов, который подсовывается, например, программе для просмотра картинок со словами: "Это на  
   самом деле JPEG-файл, читай его".
2. Мутация — прием намного более изящный и подразумевает внесение изменений в "хороший", то есть вполне корректный файл.

Все фаззеры(программы, осуществляющие фазинг) работают примерно одинаковым образом, позволяя задавать некоторые ограничения на мутирование входных данных определенными байтами или последовательностью байтов.

**2 Решаемые задачи**

Фазинг обычно предназначен для проверки проблем безопасности в программных системах, так как данный метод позволяет выявлять ошибки в процессе функционирования ПО. Ошибки, найденные фазером, могли бы быть использованы злоумышленниками, если их вовремя не исправить

Метод позволяет обнаружить аварийные ситуации, ошибки, сбои и утечки памяти. Он может быть пригоден для тестирования больших приложений, где любая ошибка памяти может привести к серьёзной уязвимости.

Fuzz Testing также позволяет найти непредусмотренные различия между двумя версиями программы или между двумя реализациями из одной и той же спецификации.

Обычно данный метод применяется для тестирования программ, для которых работоспособность и безопасность при любых входных данных являются наиважнейшими приоритетами/ веб-сервер, клиент/сервер SSH, sandboxing, сетевые протоколы.

Сам по себе Fuzz Testing является простым методом и дает возможность проведения тестирования в автоматическом режиме.

**3 Недостатки метода**

Fuzz Testing проверяет устойчивость программы на поступление некорректных входных данных, однако не проверяет правильность обработки верных, что требует дополнительных тестов.

Используя фаззинг, генерируются случайные данные, а значит нельзя точно быть уверенным, что будут протестированы граничные значения.

Сам фазер ничего не знает о внутреннем состоянии программы, что может затруднить проведение автоматического тестирования. Также он вынужден перебирать огромное количество вариантов, которые растет экспоненциально в зависимости от входных данных. Помимо всего этого, простой фазер может очень плохо покрыть код программы.