نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

آزمون فاز اکتشافی جهت کشف خطاهای نرم‌افزاری

منیره قدیریان[۱]، بهروز ترک لادانی[۲]، بهمن زمانی[۳]

[۱] گروه مهندسی سیستم‌های نرم‌افزاری، دانشگاه اصفهان
ghadirian@ymail.com

[۲] دانشیار، گروه مهندسی سیستم‌های نرم‌افزاری، دانشگاه اصفهان
ladani@eng.ui.ac.ir

[۳] استادیار، گروه مهندسی سیستم‌های نرم‌افزاری، دانشگاه اصفهان
zamani@eng.ui.ac.ir

چکیده

آزمون نرم‌افزار فرآیندی وقت‌گیر و خسته کننده است. آزمون فاز در کنار خودکار بودن می‌تواند در صورت رسیدن به پوشش کد، خطاها و آسیب‌پذیری‌های زیادی را کشف کند. چالش اصلی در تمام آزمون‌های کد مانند این آزمون، رسیدن به پوشش کد و طی مناطق عمیق کد است تا احتمال یافتن خطا و آسیب‌پذیری بیشتر شود. بدین منظور استفاده از آزمون واقعی-نمادین در صورت داشتن حلال قیود مناسب و یا قیود به شکل درست می‌تواند بسیار امیدبخش باشد؛ اما به دلیل نقش گلوگاهی حلال قیود و شکل قیود ممکن است برخی از مسیرها، جوابی مناسب از حلال قیود دریافت نکرده و دچار انحراف شده و این مسیرها و مسیرهای حاشیه‌ای آن‌ها هرگز پیموده نشوند. در این مقاله، روشی برای بهبود نحوه عملکرد و ارتقاء پوشش آزمون در آزمون فاز ارائه شده است. برای این منظور در کنار استفاده از روش آزمون واقعی-نمادین، اکتشافاتی بر روی قیود شرایط مسیر با کمک الگوریتم ژنتیک صورت گرفته و شرایط مسیر بهتری تولید می‌شود به صورتی که توسط حلال قیود قابل حل بوده و طی کردن داده متناظر با آن، به پوشش کد بالاتر می‌انجامد. نتایج تجربی حاصل از پیاده سازی و اعمال روش پیشنهادی روی موارد کاربردی مختلف در مقایسه با روش مشابه مؤید این مطلب است.

کلمات کلیدی

آزمون فاز، آزمون واقعی-نمادین، اجرای واقعی-نمادین، الگوریتم ژنتیک، روش‌های اکتشافی، آزمون نرم‌افزار

۱- مقدمه

گزارش‌های آسیب‌پذیری و خطاهای موجود در نرم‌افزارها که هر روزه منتشر می‌شود و تبعات مالی و حیثیتی فراوانی که به همراه دارند دلالت بر اهمیت آزمون نرم‌افزار دارند. تولید داده‌های آزمونی که بتواند حالت‌های مختلف برنامه را در نظر گرفته و مسیرهای گوناگون موجود در کد برنامه را پوشش دهد یکی از چالش‌های اساسی آزمون است. در واقع، این امر در دنیای آزمون نرم‌افزار پذیرفته شده است که هیچ آزمونی نمی‌تواند عدم وجود خطا یا آسیب‌پذیری را به صورت کامل تضمین کند، اما هرچه آزمون انجام‌شده دارای معیارهای پوشش کد[۱] بیشتری باشد قابلیت اطمینان و اعتماد بیشتری به گروه نرم‌افزاری می‌دهد. لذا کشف خطا و آسیب‌پذیری به عنوان یک هدف غایی و پوشش کد به عنوان هدفی دیگر جهت اطمینان از آزمون مطرح است. از طرف دیگر به دلیل اینکه تولید داده‌های آزمون به روش دستی خسته‌کننده، وقت‌گیر و نیازمند هزینه مالی و انسانی زیادی است، تمایل آزمون‌گران و نیز نفوذگران امنیتی به سمت روش‌های خودکار یا نیمه خودکار آزمون بیشتر شده است.

یکی از آزمون‌های خودکار مطرح در دنیای نرم‌افزار، آزمون فاز[۲] [۱] است که روشی کارا و خودکار برای کشف آسیب‌پذیری‌های موجود در نرم‌افزار است. آزمون فاز با ارسال داده‌های زیادی به صورت خودکار به برنامه و رصد برنامه کار می‌کند و در صورتی که در یکی از این اجراهای برنامه خطا و یا رفتار غیرعادی مانند شکست سیستم رخ دهد آن را ثبت می‌کند. همان طور که مشخص است این آزمون به دلیل اجرای برنامه هدف و نه صرفاً تحلیل برنامه هدف، از رده آزمون‌های پویا است. اجرای برنامه هدف و گزارش تنها آسیب‌پذیری‌ها و خطاهایی که واقعاً در عمل اتفاق افتاده‌اند حسن این آزمون را نسبت به خیلی از آزمون‌های دیگر نشان می‌دهد که ممکن است به تولید موارد آزمون کاذب بپردازند؛ مواردی که به عنوان خطا ثبت می‌شوند اما در عمل آشکارکننده هیچ خطایی نیستند [۲، ۳]. در سال‌های اخیر، آزمون فاز به دلیل خودکار بودن و صرفه‌جویی در زمان و هزینه مورد توجه آزمون‌گرها و همچنین نفوذگران امنیتی قرار گرفته است [۳].