ЛАБОРАТОРИЯ СЕРТИФИКАЦИИ МОУ «ИИФ» ИСПОЛЬЗУЕТ PT APPLICATION INSPECTOR ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ИСХОДНОГО КОДА ПРИ АНАЛИЗЕ НДВ

«Наши специалисты искали отечественный инструмент для обнаружения уязвимостей в исходном коде, но с принципиально новыми технологиями, которые, в отличие от простого поиска по шаблонам, позволяют вычислять уязвимости, уникальные для сертифицируемого средства защиты. Именно таким инструментом оказался продукт компании Positive Technologies».

Валерий Маслов,
начальник комплексного испытательного управления
МОУ «ИИФ»

ПРОФИЛЬ КОМПАНИИ

- **Организация:** Комплексное испытательное управление Межрегионального общественного учреждения «Институт инженерной физики» (МОУ «ИИФ»)
- **Профиль деятельности управления:** Испытания средств защиты информации, проектирование и создание систем в защищенном исполнении, предназначенных для обработки информации ограниченного доступа.
- **География сотрудничества:** более 80 предприятий в 24 городах
- **Лицензии:** аккредитация в качестве испытательной лаборатории ФСБ, ФСТЭК, Минобороны РФ. Лицензии Минобороны, Минпромторга, МЧС, Росатома, Роскомнадзора, Роспотребнадзора, Рособоронзаказа, ФСБ, ФСТЭК и др.

ЗАДАЧА

Испытательная лаборатория межрегионального общественного учреждения «Институт инженерной физики» — одна из крупнейших испытательных лабораторий в России. В задачи лаборатории входит проведение сертификационных испытаний специального программного обеспечения, автоматизированных систем и средств вычислительной техники и др.

Согласно последним нормативным требованиям ФСТЭК России, при сертификации программного обеспечения испытательные лаборатории должны контролировать отсутствие недекларированных возможностей (НДВ) — функциональных возможностей, не описанных или не соответствующих описанным в документации, при использовании которых возможно нарушение конфиденциальности, целостности и доступности обрабатываемой информации, — а также выполнять работы по анализу угроз безопасности информации.

Необходимость поиска всех угроз безопасности информации, а не только НДВ, связана с тем, что незамеченные ошибки кода и конфигурации, слабые механизмы аутентификации и другие внутренние недостатки системы также могут приводить к нарушению конфиденциальности, целостности и доступности. С развитием целенаправленных атак даже небольшая уязвимость может стать частью многоступенчатой схемы промышленного шпионажа или саботажа.

Анализ отсутствия НДВ сертифицируемых систем, помимо прочего, включает и сигнатурный анализ программного обеспечения.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Анализатор исходного кода PT Application Inspector для тестирования и сертификации средств защиты информации:

- Минимум ложных срабатываний
- Простота и безопасность тестирования
- Ясное представление рисков
- Адаптация к логике приложения для выявления уникальных НДВ
- Выполнение требований регуляторов

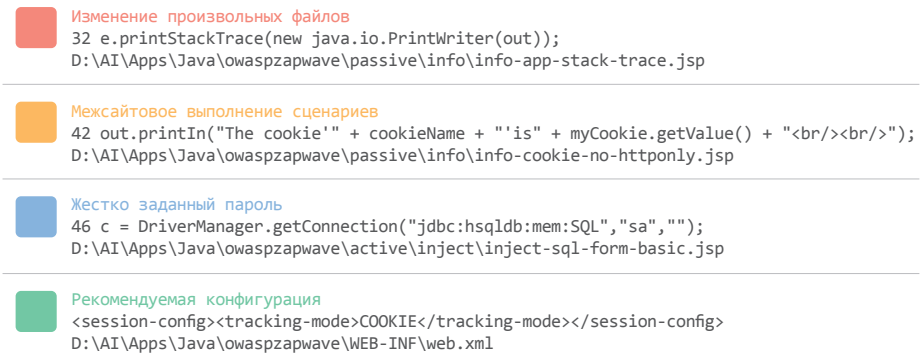
«Высокая точность обнаружения уязвимостей с использованием PT Application Inspector позволила институту вывести контроль НДВ при испытательных работах по сертификации средств защиты на новый качественный уровень».

Владимир Потапов,
начальник группы анализа недекларированных возможностей МОУ «ИИФ»

РЕШЕНИЕ

Сигнатурный анализ программного обеспечения является одним из важнейших этапов сертификации, так как именно он обычно помогает выявлять НДВ. Однако большинство анализаторов кода, используемых при сертификации, проводят подобный анализ самым простым методом поиска по шаблону (pattern matching), что в совокупности с астрономическим количеством ложных срабатываний сильно снижает практическую ценность работы анализатора и требует ручной проверки результатов специалистами.

Для более качественного выявления уязвимостей специалисты испытательной лаборатории МОУ «ИИФ» выбрали систему анализа исходного кода PT Application Inspector (PT AI). Данная система использует гибридный подход, сочетающий методы статического (SAST), динамического (DAST) и интерактивного анализа, что радикально снижает количество ложных срабатываний. Кроме того, PT AI дает возможность анализа как частичного исходного кода, так и полностью собранного приложения, а механизм генерации эксплойтов позволяет наглядно продемонстрировать найденные уязвимости.



РЕЗУЛЬТАТ

Анализатор исходного кода PT Application Inspector успешно интегрирован в инструментальную базу испытательной лаборатории МОУ «ИИФ». Продукт компании Positive Technologies помог автоматизировать процесс выявления уязвимостей в соответствии с новыми требованиями и рекомендациями ФСТЭК.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.ru
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays