Solertia
STUDHACK.RU

# СЕМИНАР «УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

В рамках студенческой исследовательской группы «Солерция» на базе «Института математики, механики и компьютерных наук» ЮФУ планируется организация **постоянно действующего семинара по теме «Уязвимости программного обеспечения».** Целью семинара является создание и поддержание сообщества людей, увлеченных тематикой современной информационной безопасности. Работа группы будет включать в себя лекции, семинары и практические занятия в группах с привлечением ведущих специалистов в области информационной безопасности.

Занятия будут организованы при участии ведущих специалистов ФГАНУ НИИ «Спецвузавтоматика» (Минобрнауки РФ, г.Ростов-на-Дону).

В ходе семинарских занятий студенты смогут получить необходимый **багаж знаний, практический опыт и навыки исследовательской работы** в сфере информационных технологий, которые они смогут использовать в практической работе после окончания университета. Заинтересовавшиеся тематикой информационной безопасности студенты могут быть трудоустроены в ФГАНУ НИИ «Спецвузавтоматика», где смогут продолжить работу по данному направлению.

## ТЕМЫ СЕМИНАРА

В ходе семинара планируется освещение целого ряда направлений современной информационной безопасности:

- Современные хакерские атаки. Арсенал средств и техника работы злоумышленника. «Anonymus», «White Hats» и «Black Hats»: кто они?
- Причины возникновения уязвимостей прикладных программ и эксплуатация уязвимостей
- Методы обнаружения уязвимостей прикладных программ. Автоматизированное тестирование методами «белого» и «черного ящика».
- Поиск уязвимостей в смартфонах, «умных домах» и различных гаджетах

и другие темы, непосредственно посвященные уязвимостям программ.

Ряд занятий будет посвящен общим тенденциям в IT-индустрии:

- Современные средства разработки
- Методологии разработки IT-проектов (Agile)

а также планируется несколько лекций по смежным IT-тематикам.

studhack.ru
тел./факс: 8 (863) 201-28-17
344010, г.Ростов-на-Дону, ул.Греческого города Волос, д.6

Solertia
STUDHACK.RU

# СЕМИНАР «УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

## ПЛАН СЕМИНАРСКИХ ЗАНЯТИЙ НА 2014-2015 УЧЕБНЫЙ ГОД

### ОКТЯБРЬ

Вводные лекции по тематике «уязвимости программного обеспечения», докладчики: К.Ю. Гуфан, В.Н. Шаповалов.

Формирование группы для семинарских занятий

### НОЯБРЬ – ДЕКАБРЬ

Доклады приглашенных лекторов-специалистов в области информационной безопасности и современных IT-технологий.

Еженедельные семинарские занятия под руководством Шаповалова В.Н.:

- ◊ Анализ существующих направлений исследований в области поиска уязвимостей прикладных программ
- ◊ Работа с существующими решениями в области фаззинга форматов файлов
- ◊ Первые эксперименты по поиску уязвимостей в популярном ПО с помощью фаззинга популярных форматов: doc, rtf, pdf и т.д.
- ◊ Постановка задач для исследовательских проектов

### ФЕВРАЛЬ – МАЙ

- ◊ Разработка методов и средств поиска уязвимостей прикладного ПО в рамках исследовательских проектов
- ◊ Практическая работа и экспериментальные исследования
- ◊ Оформление, публикация и внедрение результатов индивидуальных работы

Доклады участников семинара и приглашенных лекторов

## ЛЕКТОРЫ

К.Ю.Гуфан - выпускник мех-мата к. ф.-м. н., заместитель директора по научной работе ФГАНУ НИИ «Спецвузавтоматика»

В.Н.Шаповалов - выпускник мех-мата, ведущий научный сотрудник, ФГАНУ НИИ «Спецвузавтоматика», специалист в области обфускации программного кода

Информация о семинаре будет размещена на сайте studhack.ru и в группе Вконтакте (vk.com/solertia_rostov)

OWASP Open Web Application Security Project

Семинар проводится при поддержке сообщества OWASP Foundation:Rostov

studhack.ru
тел./факс: 8 (863) 201-28-17
344010, г.Ростов-на-Дону, ул.Греческого города Волос, д.6

Solertia
STUDHACK.RU

# СЕМИНАР «УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

## ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Поиск уязвимостей программного обеспечения – одна из ключевых задач современной информационной безопасности.

Эксплуатация уязвимостей программ позволяет злоумышленникам воровать деньги с банковских счетов, делать «дефейсы» веб-сайтов, блокировать работу банков и городских служб.

К уязвимостям приводят программистские ошибоки, которые есть в любом программном продукте. Уязвимости в программном обеспечении ищут разными способами: автоматическими тестировщиками, анализаторами кода, ручной проверкой. Однако, наибольшее распространение получили метод тестирования программ называемый «фаззингом».

Фаззинг (от англ. fuzz testing – тестирование на случайных данных) – методика тестирования программного обеспечения на наличие в ней уязвимости методом «черного ящика». При таком тестировании на вход программы подаются невалидные, непредусмотренные или просто случайные данные, сгенерированные автоматическим или полуавтоматическим образом, после чего анализируется результат работы программы. При этом аналитику не нужен доступ к исходному коду программы, чем и пользуются злоумышленники и так называемые «white hats» (независимые эксперты по компьютерной безопасности).

Современный фаззинг, как и любой другой метод «грубой силы», реализуется с помощью сложного эвристического подхода, нетривиальных алгоритмических конструкций и тщательного предварительного анализа. Исследования в этой области активно ведутся во всех ведущих научных IT-институтах Мира, например, в MIT (США) и ИСП РАН (Россия). Однако, на текущий момент не существует готовых ответов на вопрос - «как проверить готовую программу на отсутствие в ней уязвимостей?»

Таким образом, задача поиска уязвимости в программном обеспечении, является многогранной, неоспоримо актуальной и имеющей конкретное практическое значение для исследователей, работающих в области информационной безопасности.

studhack.ru
тел./факс: 8 (863) 201-28-17
344010, г.Ростов-на-Дону, ул.Греческого города Волос, д.6