Бауманский учебный центр «Специалист»

Программа курса Уязвимости программного обеспечения

Код курса: **УПО**

Тема	Ак. часов
Модуль 1. Системные уязвимости. Организация памяти процесса в архитектуре x86 • Структура виртуальной памяти, выделяемой процессу. • Основные регистры процессора. • Вызов и возврат из функции. Соглашение о вызовах __stdcall.	**2**
Модуль 2. Системные уязвимости. Переполнение на стеке (stack smash). Иные уязвимости (heap overflow, integer overflow, read overflow, уязвимости форматной строки) • Понятие системного буфера. • Этапы эксплуатации stack smash. • Переполнение в куче (heap overflow). • Переполнении при операциях с целыми (integer overflow). • Чтение за пределами буфера (read overflow). • Уязвимости форматной строки. • Висячие указатели (dangling pointers). • **Лабораторная работа:** Эксплуатация переполнения буфера в стеке (stack-smash). • **Лабораторная работа:** Эксплуатация иных системных уязвимостей.	**4**
Модуль 3. Системные уязвимости. Механизмы защиты. Техники преодоления защитных механизмов • Безопасность типов и безопасность работы с памятью (type safety и memory safety). • Стековая канарейка. • Запрет выполнения из области данных (DEP). • Рандомизация смещений динамических областей памяти (ASLR). • Контроль целостности потока управления (CFI). • Обход защитных механизмов: использование libc, прямой перебор памяти, обход stack canary, возвратное программирование (ROP). • Правила и принципы безопасного программирования. • **Лабораторная работа:** Обход механизмов ASLR, DEP, stack canary на примере проекта с открытым исходным кодом.	**4**
Модуль 4. Уязвимости Web-приложений. Архитектура Web-приложений • Принципы работы веб-серверов и веб-приложений. • Обзор классификации OWASP Top 10. • **Лабораторная работа:** Настройка учебного стенда.	**2**

Модуль 5. Уязвимости Web-приложений. Инъекции. Межсайтовый скриптинг (XSS). Внешние XML-объекты • Общие сведения об инъекциях. • HTML инъекции. • iFrame инъекции . • LDAP инъекции. • Инъекции в почтовых заголовках. • Инъекции команд операционной системы . • Инъекции PHP кода. • Простые SQL инъекции. • SQL инъекции в AJAX/JSON/jQuery. • Примеры SQL инъекции в Drupal и SQLite. • Хранимые SQL инъекции. • Хранимые SQL инъекции в XML. • SQL инъекции в поле User-Agent. • Слепые SQL инъекции на логической основе. • Слепые SQL инъекции на временной основе. • XML/XPath инъекции. • Отраженные XSS. • Отраженная XSS в JSON. • Отраженная XSS в AJAX. • Отраженная XSS в XML. • Отраженная XSS в кнопке возврата. • Отраженная XSS в функции Eval. • Отраженная XSS в атрибуте HREF. • Отраженная XSS в форме входа. • Пример отраженной XSS в phpMyAdmin. • Отраженная XSS в переменной PHP_SELF. • Отраженная XSS в заголовках HTTP. • Хранимые XSS в записях блогов. • Хранимые XSS при смене пользовательских данных. • Хранимые XSS в Cookies. • Хранимые XSS в заголовках HTTP. • Атаки на внешние XML объекты. • Атака на отказ в обслуживании типа XML Bomb. • **Лабораторная работа:** Эксплуатация уязвимостей типа: injection, xss.	**6**
Модуль 6. Уязвимости Web-приложений. Уязвимости аутентификации и управления сеансом • Обход CAPTCHA. • Атака на функционал восстановления паролей. • Атака на формы входа. • Атака на управление выходом. • Атаки на пароли. • Атаки на административные порталы. • Атаки на Cookies. • Атаки на передачу идентификатора сеанса в URL. • Фиксация сеанса. • **Лабораторная работа:** Эксплуатация уязвимостей аутентификации и управления сеансом.	**2**

Модуль 7. Уязвимости Web-приложений. Небезопасное хранение и передача чувствительных данных • Использование кодировки Base64. • Открытая передача чувствительных данных по HTTP. • Атаки SSL BEAST/CRIME/BREACH. • Атака на уязвимость Heartbleed. • Уязвимость POODLE. • Хранение данных в веб-хранилище HTML5. • Использование устаревших версий SSL. • Хранение данных в текстовых файлах. • **Лабораторная работа:** Эксплуатация уязвимостей, связанных с небезопасным хранением и передачей данных.	**2**
Модуль 8. Уязвимости Web-приложений. Уязвимости механизма управления доступом • Пример атаки на небезопасную прямую ссылку при смене пароля пользователя. • Пример атаки на небезопасную прямую ссылку при сбросе пароля пользователя. • Пример атаки на небезопасную прямую ссылку при заказе билетов в интернет-магазине. • Принципы атак на функциональный уровень. • Что такое обход каталога. • Обход каталога в каталогах. • Обход каталога в файлах. • Атака на заголовок Host, приводящая к сбросу пароля. • Концепции подключения локального или удаленного файла. • Включение локального файла в SQLiteManager. • Включение локального или удаленного файла (RFI/LFI). • Атака на ограничение доступа устройств. • Атака на ограничение доступа к каталогам. • Атака SSRF. • Атака на XXE. • **Лабораторная работа:** Эксплуатация уязвимостей механизма управления доступом.	**2**
Модуль 9. Уязвимости Web-приложений. Небезопасная десериализация • Демонстрация инъекции PHP объекта. • Инъекция бэкдора при десериализации. • Небезопасная десериализация в JavaScript. • **Лабораторная работа:** Эксплуатация уязвимостей, связанных с небезопасной десериализацией.	**2**
Модуль 10. Уязвимости Web-приложений. Небезопасная конфигурация • Произвольный доступ к файлам в Samba. • Общие ресурсы в AJAX. • Межсайтовая трассировка (XST). • Отказ в обслуживании (Large Chunk Size). • Отказ в обслуживании (Slow HTTP DoS). • Отказ в обслуживании (SSL-Exhaustion). • Небезопасная конфигурация FTP. • Небезопасная конфигурация NTP. • Небезопасная конфигурация SNMP. • Небезопасная конфигурация VNC . • Небезопасная конфигурация WebDAV . • Атака «Человек посередине» в HTTP. • Атака «Человек посередине» в SMTP. • Небезопасное хранение архивных файлов. • Файл robots. • **Лабораторная работа:** Эксплуатация уязвимостей, связанных с небезопасной конфигурацией.	**2**

Модуль 11. Уязвимости Web-приложений. Использование небезопасных компонент, уязвимости системы логирования, иные уязвимости • Локальные атаки на переполнение буфера. • Удаленные атаки на переполнение буфера. • Удаленное исполнение кода в PHP CGI. • Уязвимость в phpMyAdmin BBCode Tag XSS. • Уязвимость Shellshock. • Подключение локального файла в SQLiteManager.	**2**
Модуль 12. Уязвимости Android-приложений. Архитектура и компоненты Android-приложений. Сбор данных об Android-приложении • Архитектура мобильных приложений для ОС Android. • Компоненты приложения. • Файл AndroidManifest.xml • Файл classes.dex. • Инструментарий для анализа Android приложения. • **Лабораторная работа:** Настройка учебного стенда. Сбор данных об учебном приложении.	**2**
Модуль 13. Уязвимости Android-приложений. Уязвимости компонент • Несанкционированный активация операций. • Утечка данных через широковещательные сообщения. • Активация операций через широковещательные сообщения. • **Лабораторная работа:** Реализация атак на компоненты приложений.	**2**
Модуль 14. Уязвимости Android-приложений. Небезопасное хранение чувствительных данных • Общие сведения о хранении данных в Android-приложении. • Использование внутренней памяти. • Использование внешнего хранения. • Использование поставщиков контента. • **Лабораторная работа:** Эксплуатация уязвимостей, связанных с небезопасным хранением данных.	**2**
Модуль 15. Уязвимости Android-приложений. Перехват и модификация трафика. Преодоление механизма SSL-pinning • Общие сведения о методах перехвата и модификации трафика. • SSL pinning. • **Лабораторная работа:** Перехват и модификация трафика. Преодоление механизма SSL-pinning.	**4**
Модуль 16. Дополнительные материалы • Не cookies единым. Так ли опасен XSS сегодня?	
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru