Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный

университет информатики и радиоэлектроники»

Институт информационных технологий

УТВЕРЖДАЮ

Директор института информационных технологий БГУИР

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Охрименко

« \_\_\_ »\_\_\_\_\_\_\_\_\_\_\_2020 г.

**УЧЕБНАЯ ПРОГРАММА**

|  |  |
| --- | --- |
| по дисциплине | Тестирование безопасности программного обеспечения |
|  | (название дисциплины) |
| для специальности | *1-40 01 75 «Тестирование программного обеспечения»* |
|  | (№ и название специальности) |
|  | вечерней и заочной формы обучения |
|  |  |

Минск, 2020

Разработчик программы:

Моженкова Е.В., ст. преподаватель

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Рекомендована к утверждению: | | | | | | | |
| кафедрой микропроцессорных систем сетей | | | | | | | |
| протокол № |  | от | " |  | " |  | 2020 г. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Утверждена | | | | | | | |
| Советом Института информационных технологий БГУИР | | | | | | | |
| протокол № |  | от | " |  | " |  | 2020 г. |

ВВЕДЕНИЕ

Учебная программа по дисциплине «Тестирование безопасности программного обеспечения» разработана для слушателей специальности 1- 40 01 75 «Тестирование программного обеспечения».

Программа предусматривает требования к содержанию лекционного материала, перечню тем лабораторных занятий, вопросам для итогового контроля по дисциплине. Дисциплина «Тестирование безопасности программного обеспечения» является дисциплиной специализации.

Цель изучения данной дисциплины — овладение знаниями в области безопасности программного обеспечения, и навыками тестирования защищенности программного обеспечения.

Основными задачами дисциплины являются:

* овладение теоретическими основами в области безопасности программного обеспечения;
* изучение основных уязвимостей веб-приложений, а также базовых методов тестирования веб-приложений на наличие этих уязвимостей;
* получение слушателями практических навыков в области тестирования безопасности программного обеспечения;
* получение практических навыков по работе с инструментами анализа защищенности веб-приложений.

В результате освоения дисциплины «Тестирование безопасности программного обеспечения» слушатель должен:

**знать:**

* классификацию угроз безопасности информационных систем и ПО;
* основные методы поиска уязвимостей в программном обеспечении;
* основные методы поиска и оценки уязвимостей информационных систем;
* основные фазы тестирования на проникновение;
* основные методы защиты от атак.

**уметь:**

* разрабатывать Security Test Plan;
* работать с локальными НТТР-прокси-серверами;
* работать с инструментами анализа защищенности веб-приложений;
* производить тестирование защищенности веб-приложений;
* работать с инструментами поиска и анализа уязвимостей в информационных системах.

Используемые методы - методы проблемного обучения, проектной деятельности, компьютерного моделирования.

Используемые средства - интерактивная доска.

### Программа дисциплины рассчитана на объем 58 учебных часов, из них – 36 аудиторных. Распределение аудиторных часов по видам занятий следующее: лекций – 16 часов, лабораторных занятий – 16 часов.

Форма аттестации - зачет.

1 СОДЕРЖАНИЕ

**1. Общие сведения о тестировании безопасности**

1.1. Процесс тестирования защищенности программного  
обеспечения

Основные понятия и определения (угроза/уязвимость/ недостаток/атака). Классификация угроз безопасности информационных систем и ПО. Требования к обеспечению безопасности информационных систем и ПО. Подходы к поиску уязвимостей (черный, серый, белый ящик). Методологии тестирования безопасности ПО. Security Test Plan, основные разделы.

1.2. Тестирование на проникновение

Общие сведения о тестировании на проникновение. Основные фазы тестирования на проникновение. Анализ и сбор информации. Проведение тестирования на проникновения. Оценка рисков и подготовка отчета.

**2. Основные типы атак на веб-приложения**

2.1. Межсайтовое выполнение сценариев

Введение в WEB технологии. Протокол HTTP/HTTPS (запросы/ ответы/заголовки). Кодирование данных (URL/HTML/Base64/Hex). Same Origin Policy. Понятие cookies и веб-сессии. Понятие локального НТТР- прокси-сервера. Анатомия атак "Межсайтового выполнения сценариев". Типы атак "Межсайтового выполнения сценариев". Методика поиска уязвимостей. Эксплуатация уязвимостей "Межсайтового выполнения сценариев". Защитные меры.

2.2. Внедрение SQL кода

Общие сведения об SQL инъекциях. Типы SQL инъекций. Методика поиска уязвимостей. Эксплуатация уязвимостей "SQL инъекции". Инструменты для поиска и эксплуатации уязвимостей типа "SQL инъекции". Защитные меры.

2.3. Атаки на аутентификацию и авторизацию пользователей

Понятия аутентификации и авторизации. Типы аутентификации. Основные атаки на аутентификацию пользователей. Методы обхода авторизации. Методы защиты от атак на аутентификацию и авторизацию пользователей.

2.4. Управление сессиями

Анализ сессионного идентификатора. Методы перехвата сессии. Атаки типа "Фиксация сессии". Атаки типа "Межсайтовая подделка запроса". Методы защиты от атак на сессии пользователя.

2.5. Атаки на файлы и ресурсы веб-приложений

Атаки на веб приложения с помощью "Выхода за пределы назначенной директории" (path traversal). Атаки типа "Включение локальных файлов". Загрузка произвольных файлов. Методы защиты от атак на файлы и ресурсы веб-приложений.

**3. Автоматические средства сканирования и аудита веб-  
приложений и информационных систем**

3.1. Общие сведения о средствах сканирования и аудита веб-  
приложений

Преимущества и недостатки средств сканирования веб-приложений. Настройка и запуск инструментов комплексной проверки веб-сайтов на уязвимости О WASP ZAP и OpenVAS. Понятие сетевых анализаторов трафика (на примере Wireshark).

1. **ТЕМАТИКА лабораторных ЗАНЯТИЙ**
2. Поиск и анализ уязвимостей на стороне клиента (XSS, CSRF).
3. Поиск и анализ уязвимостей внедрения SQL-кода и внедрения команд ОС.
4. Поиск и анализ уязвимостей аутентификации и авторизации пользователей. Управление сессиями.
5. Атаки на файлы и ресурсы веб-приложений. Небезопасная загрузка файлов на веб-сервер, эксплуатация и обход фильтров.
6. Использование автоматических средств сканирования и аудита безопасности ПО и информационных систем.

# **САМОСТОЯТЕЛЬНАЯ РАБОТА И ФОРМЫ КОНТРОЛЯ**

***Источники информации, рекомендуемые слушателям для самостоятельного изучения тем дисциплины:***

|  |  |  |
| --- | --- | --- |
| Темы дисциплины | Самостоятельная работа (количество часов) | Литература для самостоятельного изучения тем |
| Security Test Plan, основные разделы. | 4 | Электронные материалы |
| Внедрение SQL кода | 4 | Электронные материалы |
| Методы защиты от атак на аутентификацию и авторизацию пользователей. | 4 | Электронные материалы |
| Понятие сетевых анализаторов трафика (на примере Wireshark) | 6 | Электронные материалы |
| Всего | 22 |  |

1. **МАТЕРИАЛЫ ТЕКУЩЕЙ АТТЕСТАЦИИ**
2. Понятие тестирования безопасности программного обеспечения.
3. Понятия угрозы, уязвимости, атаки.
4. Классификация угроз безопасности информационных систем и ПО.
5. Требования к обеспечению безопасности информационных систем и ПО
6. Подходы к поиску уязвимостей (методы черного, серого, белого ящика)
7. Методологии тестирования безопасности ПО.
8. Security Test Plan, назначение, структура.
9. Понятие тестирования на проникновение.
10. Основные фазы тестирования на проникновение.
11. Типы кодирование данных (URL/HTML/BAse64/Hex).
12. Протокол HTTP/HTTPS (основные заголовки запросов и ответов).
13. Понятие Same Origin Policy.
14. Понятие cookies и веб-сессии.
15. Понятие веб-прокси.
16. Понятие и анатомия атаки "Межсайтового выполнения сценариев".
17. Методика поиска и эксплуатация уязвимостей "Межсайтового выполнения сценариев". Методы защиты от атак "Межсайтового выполнения сценариев"
18. Общие сведения об SQL инъекциях. Типы SQL инъекций.
19. Методика поиска уязвимостей "SQL инъекции". Эксплуатация уязвимостей "SQL инъекции". Методы защиты от уязвимостей "SQL инъекций".
20. Понятия аутентификации и авторизации.
21. Типы аутентификации.
22. Основные атаки на аутентификацию пользователей.
23. Методы обхода авторизации.
24. Методы защиты от атак на аутентификацию и авторизацию пользователей.
25. Понятие и анализ сессионного идентификатора.
26. Методы перехвата сессии.
27. Понятие атаки фиксации сессии.
28. Понятие атаки типа "Межсайтовая подделка запроса"
29. Методы защиты от атак на сессии пользователя
30. Понятие атаки атака на веб приложения с помощью "Выхода за пределы назначенной директории" (path traversal)
31. Включение локальных файлов
32. Загрузка произвольных файлов
33. Методы защиты от атак на файлы и ресурсы пользователей.
34. Средства сканирования и аудита веб-приложений
35. Преимущества и недостатки средств сканирования веб-приложений.
36. Понятие сетевых анализаторов трафика.
37. **ЛИТЕРАТУРА**

**Основная**

1. Список Топ-10 уязвимостей от OWASP - [https://www.owasp.Org/images/7/72/OWASP\_Top\_l 0-2017\_%28en%29.pdf.pdf](https://www.owasp.Org/images/7/72/OWASP_Top_l_0-2017_%28en%29.pdf.pdf)
2. Тестирование защищенности Web -приложений по методологии OWASP https ://www. owasp. org/index.php/Web Application Penetration Testing
3. OWASP Testing Guide v4 (сборник статей от множества авторов, включающий «лучшие практики» тестирования и техники тестирования веб­приложений и веб-сервисов с точки зрения безопасности) <https://wvvw.owasp.Org/images/l/19/OTGv4.pdf>
4. Penetration Testing Execution Standard (PTES) [http://www.pentest- standard.org/index.php/Main\_Page](http://www.pentest-standard.org/index.php/Main_Page)

**Дополнительная**

1. D. Stuttard M. Pinto The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition-Wiley. 2011, - 912 c
2. G. Weidman Penetration Testing: A Hands-On Introduction to Hacking (Практическое руководство по тестированию на проникновение) - 2014, - 528 с.
3. J. Faircloth Penetration Tester's Open Source Toolkit 4th Edition - Syngress, 2016-458 c.

**6 УЧЕБНАЯ КАРТА ПО ДИСЦИПЛИНЕ ПЕРЕПОДГОТОВКИ**

**Специальность**: «Тестирование программного обеспечения»

**Форма получения образования**: заочная

**Дисциплина:** «Основы организации систем непрерывного выполнения и тестирования программного обеспечения».

**Этап обучения:** 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  занятия  п/п | Вид занятия | Кол-во часов | Тема занятия | Обеспеченность\* |
|  | л | 2 | Процесс тестирования защищенности программного обеспечения | презентация |
|  | л | 2 | Тестирование на проникновение | презентация |
|  | л | 2 | Межсайтовое выполнение сценариев | презентация |
|  | л | 2 | Внедрение SQL кода | компьютерный класс |
|  | лз | 4 | Поиск и анализ уязвимостей на стороне клиента (XSS, CSRF). | компьютерный класс |
|  | л | 2 | Атаки на аутентификацию и авторизацию пользователей | презентация |
|  | л | 2 | Управление сессиями | презентация |
|  | лз | 4 | Поиск и анализ уязвимостей внедрения SQL-кода и внедрения команд ОС. | компьютерный класс |
|  | лз | 4 | Поиск и анализ уязвимостей аутентификации и авторизации пользователей. Управление сессиями. | компьютерный класс |
|  | л | 2 | Атаки на файлы и ресурсы веб-приложений | презентация |
|  | л | 2 | Общие сведения о средствах сканирования и аудита веб- приложений | презентация |
|  | лз | 4 | Атаки на файлы и ресурсы веб-приложений. Небезопасная загрузка файлов на веб-сервер, эксплуатация и обход фильтров. | компьютерный класс |
|  | лз | 4 | Использование автоматических средств сканирования и аудита безопасности ПО и информационных систем. | компьютерный класс |
| **Итого** | 16 ч.л., 20 ч. лз | |  |  |

\* презентация, компьютерный класс, задания для письменного опрос, перечень вопросов для устного опроса и т.д.