КОНКУРСНОЕ ЗАДАНИЕ

КОМПЕТЕНЦИЯ «Информационная безопасность»

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Модули задания и необходимое время
4. Критерии оценки

Количество часов на выполнение задания: 8ч.

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания является применение на практике систем информационной безопасности.

Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Конкурс включает анализ защищенности веб-приложений и шифрование базы данных под управлением Firebird 3.0.

Окончательные аспекты критериев оценки уточняются членами жюри. Оценка производится как в отношении работы модулей, так и в отношении процесса выполнения конкурсной работы. Если участник конкурса не выполняет требования техники безопасности, конфликтен, не владеет техниками управления стрессом и разрешения конфликтных ситуаций, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри.

Конкурсное задание должно выполняться по модульно. Оценка также происходит от модуля к модулю.

Если участник закончил выполнение модуля досрочно, он должен расписаться в ведомости времени напротив соответствующей информационной записи «Участник №__ закончил выполнение модуля __».

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время сведены в таблице 1

Таблица 1.

№ п/п	Наименование модуля	Рабочее время	Время на задание
1	Модуль 1: Анализ защищенности веб-приложений	С1 10.00-14.00	4 часа
2	Модуль 2: Шифрование БД под управлением Firebird 3.0	С1 15.00-19.00	4 часа
	Итого		8 часов

Модуль 1: Анализ защищенности веб-приложений

Участники должны владеть навыками:

- тестирование защищенности механизма управления сессиями исследуемого веб-приложения;
- тестирование веб-приложений на устойчивость к атакам отказа в обслуживании (DoS-атакам) на уровне протокола HTTP;
- идентификации уязвимостей веб-приложений к атакам CSRF;
- выявление уязвимостей веб-приложений к атакам XSS;
- идентификации и эксплуатации уязвимостей к атакам SQL-injection;

Участники должны уметь работать с программами такие как:

Для обеспечения условий выполнения работ используются следующие программные обеспечения:

- среда виртуализации VMWare Player;
- дистрибутивы Backtrack Linux или Kali Linux;
- среда выявления и эксплуатации уязвимостей Metasploit Framework;
- среда тестирования защищенности веб-приложений Burp Suite;
- среда эксплуатации уязвимостей веб-приложений BeEF;
- небезопасные веб-приложения проекта Web Goat;
- образы небезопасных веб-приложений проекта PentesterLab;
- современные веб-браузеры (Internet Explorer, Google Chrome, Mozilla Firefox);
- программные средства инструментального анализа защищенности XSpider, а также специализированные сканеры уязвимостей веб-приложений (например, Acunetix, AppScan, Burp Suite Pro, W3AF).

Модуль 2: Шифрование БД под управлением Firebird 3.0.
Участники должны обладать знаниями касательно следующих пунктов:
- СУБД Firebird.
Участники должны владеть навыками:
- программирование на языке программирования C++;
- работы с программой IDE Embarcadero RAD Studio.

4. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 100.

Таблица 2.

Раздел	Критерий	Оценки	
		Объективная	Общая
A	Анализ защищенности веб-приложений	55,00	55,00
B	Шифрование БД под управлением Firebird 3.0.	45,00	45,00

Субъективные оценки - Не применимо.