

# Payment Village

Попробуйте себя во взломе банковских систем!

В этом году посетителей ждут конкурсы по взлому онлайн-банка, банкоматов, смарт-терминалов и платежных карт. Участие в конкурсе доступно всем гостям конференции. Доступ к онлайн банку и виртуальным банкоматам доступен из сети интернет.

Связь с организаторами конкурсов в Telegram-канале <https://t.me/paymentvillage>.

Призовой фонд - 10000 Offcoin.

## Призовые места по конкурсам

### Смарт-терминалы

1-е место - 1000 Offcoin

2-е место - 500 Offcoin

### АТМ

1-е место - 2000 Offcoin

2-е место - 1000 Offcoin

### Онлайн-банк

1-е место - 2000 Offcoin

2-е место - 1000 Offcoin

3-е место - 500 Offcoin

### Кредитные карты

1-е место - 1500 Offcoin

Объявление победителей на второй день Offzone по результатам отправленных отчетов.

## Взлом онлайн-банка

Регистрируйтесь, ищите уязвимости в веб-приложении онлайн-банка и публикуйте их в разделе "Репорт" в личном кабинете!

Конкурс доступен для онлайн-прохождения.

## Взлом смарт-терминалов от Эвотор

Обходите экран блокировки и получайте максимальные привилегии на устройствах. В этом году ИТ-компания "Эвотор" специально для OFFZONE подготовила несколько своих смарт-терминалов с отключенными системами безопасности.

### Внимание

Количество доступных смарт-терминалов ограничено.

## Взлом виртуальных банкоматов

Получите доступ к системе, обойдя защитные механизмы, и получите максимальный уровень привилегий.

### **Внимание**

Для участия необходимо будет загрузить образы виртуальных машин формата OVA (VirtualBox).

### **Взлом кредитных карт.**

Обойдите защитные механизмы платежной системы и совершайте произвольные переводы.

### **Внимание**

1. Количество участников на данный конкурс строго ограничено. Успей поучаствовать!
2. Для участия необходим ноутбук или VM с ОС Windows.

## **Инструкция**

### **Онлайн-банк**

#### **Описание**

Для участия в конкурсе необходимо зарегистрировать аккаунт по [ссылке](http://bank.paymentvillage.org:8081) (<http://bank.paymentvillage.org:8081>).

Для регистрации бага необходимо кликнуть по иконке с жуком, после чего заполнить необходимые поля, либо приложить файл с описанием. Чем качественнее представленный отчет, тем больше награда! Небольшая подсказка: искать нужно не только веб-уязвимости, но и уязвимости связанные с логикой приложения.

Кстати, если вы хотите показать другим участникам, как много вам удалось заработать на банке - делайте переводы в благотворительный фонд для котиков.

Не забудьте указать данные о себе в Personal Дата в ЛК, чтобы организаторы могли связаться с вами.

#### **Задачи**

1. Найти как можно больше уязвимостей.
2. Отправить репорт по каждой найденной уязвимости, используя ЛК онлайн-банка.

### **Смарт-терминал**

#### **Описание**

Для участия в конкурсе необходимо подойти к организатору для получения смарт-терминала.

#### **Внимание**

Количество доступных смарт-терминалов ограничено.

При получении смарт-терминала, необходимо предоставить свои данные организатору.

При завершении участия в конкурсе, устройство необходимо вернуть организатору.

Для отправки результатов, необходимо заполнить форму по следующей [ссылке \(https://forms.gle/4eT5XXwSkdb6rj1f8\)](https://forms.gle/4eT5XXwSkdb6rj1f8).

Задачи:

1. Обойти экран блокировки (2 уровня сложности на выбор).

## **Виртуальные банкоматы**

### **Описание**

Для участия в конкурсе необходимо скачать образы виртуальных машин ATM1 и ATM2 формата .OVA (необходимо использовать VirtualBox для запуска виртуальных машин).

Виртуальные машины имеют одинаковые задания, но имеют разную сложность. Пароль от исходной учетной записи (АТМ) является пустым.

Для отправки результатов, необходимо заполнить форму по следующей [ссылке \(https://forms.gle/4eT5XXwSkdb6rj1f8\)](https://forms.gle/4eT5XXwSkdb6rj1f8).

Задания нужно проходить в указанном порядке. Обход AppLocker с при помощи повышения привелегий будет давать меньшее количество баллов.

### **Внимание**

При выполнении задания, установленный АТМ в зоне Payment Village на конференции Offzone выдает купюры. Дополнительную награду в 500 Offcoin получает участник, собравший наибольшее количество бумажных купюр.

### **Задачи:**

1. Обойти киоск и запустить C:\task\_kiosk.exe.
2. Обойти апплокер и запустить C:\task\_applocker.exe
3. Повысить привилегии до администратора и запустить C:\task\_escalation.exe
4. Проэксплуатировать веб=-уязвимости.

### **Ресурсы**

#### **АТМ1**

Сложность: Medium

Ссылка: <https://drive.google.com/file/d/10wDbWri0wfjH8Azy5FH-dNo6NPd8UkDg/view?usp=sharing>

#### **АТМ2**

Сложность: Hard

Ссылка: <https://drive.google.com/file/d/1ILV5t5nmL9dHcieEgLjJovbH1N1SS7uS/view?usp=sharing>

### **Ограничения**

Запрещается использовать загрузочную флешку и безопасный режим.

## **Карты**

### **Описание**

Для участия в данном конкурсе, необходимо подойти к организатору и получить кредитную карту, а так же устройство для чтения смарт-карт. Также необходимо загрузить ПО для работы с ними.

Для отправки результатов, необходимо заполнить форму по следующей [ссылке \(https://forms.gle/4eT5XXwSkdb6rj1f8\)](https://forms.gle/4eT5XXwSkdb6rj1f8).

### **Внимание**

1. При получении устройства для чтения смарт-карт, необходимо предоставить свои данные организатору.
2. При завершении участия в конкурсе, устройство необходимо вернуть организатору.

### **Задачи**

1. Обойти лимит в \$10 для чиповых платежей.
2. По одной карте сделать платежи на общую сумму эквивалентную 500 USD. Описать каждую из совершенных мошеннических транзакций, чем подробнее тем лучше.

### **Ресурсы**

#### **ПО для работы с картами**

Ссылка: [https://drive.google.com/file/d/1\\_UD3Rk3psP5ZXdtrs6YBsjb-43HEXQXu/view?usp=sharing](https://drive.google.com/file/d/1_UD3Rk3psP5ZXdtrs6YBsjb-43HEXQXu/view?usp=sharing)