



CTF в Банке. Взломай систему, получи са\$h

Клендар Николай

Начальник Управления ИБ

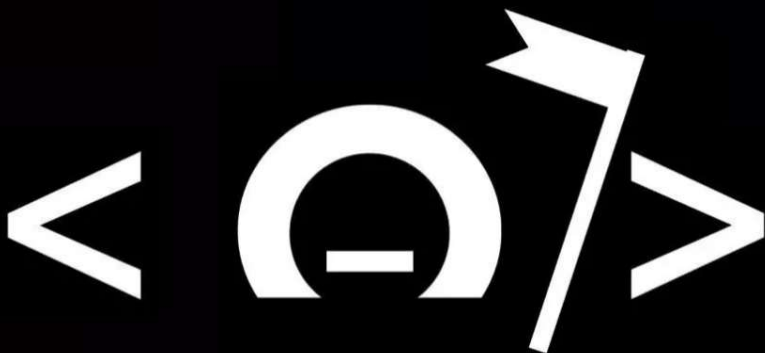
Home Credit Bank

bsploit@gmail.com

Москва, 25.08.2022



Цели CTF



Знакомство участников с уязвимостями

Элемент программы security awareness

Выявление security champions

Установка неформальных контактов между
безопасностью и ИТ

Весело провести время!

Бюджет, призы



1 место: 25 000 ₽

2 место: 15 000 ₽

3 место: 10 000 ₽

поощрительные призы футболки, худи: 79 500 ₽

разработка: 0 ₽ (for fun)

Итого: 129 500 ₽

Сроки

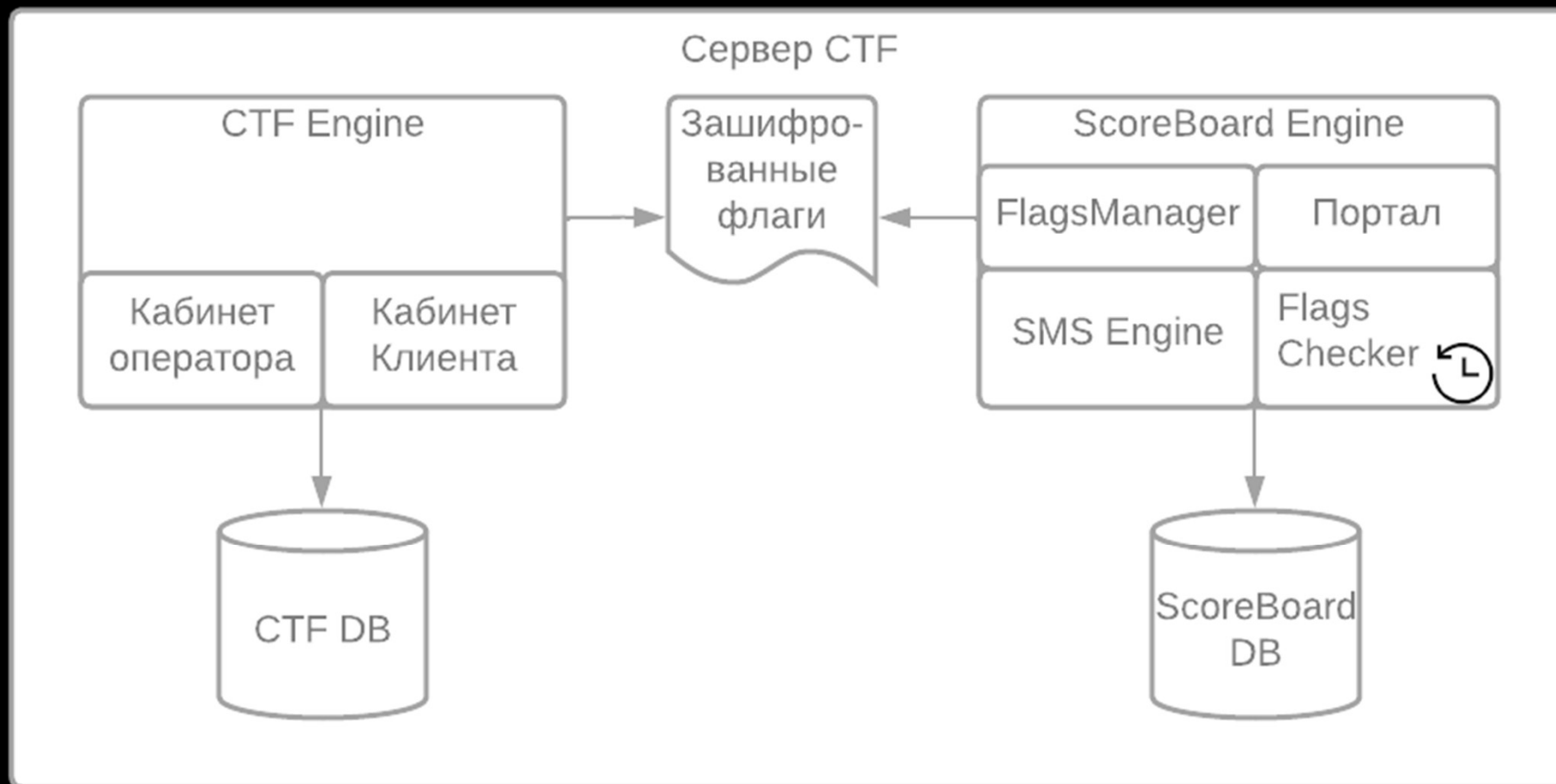


Разработка: ноябрь-декабрь 2019

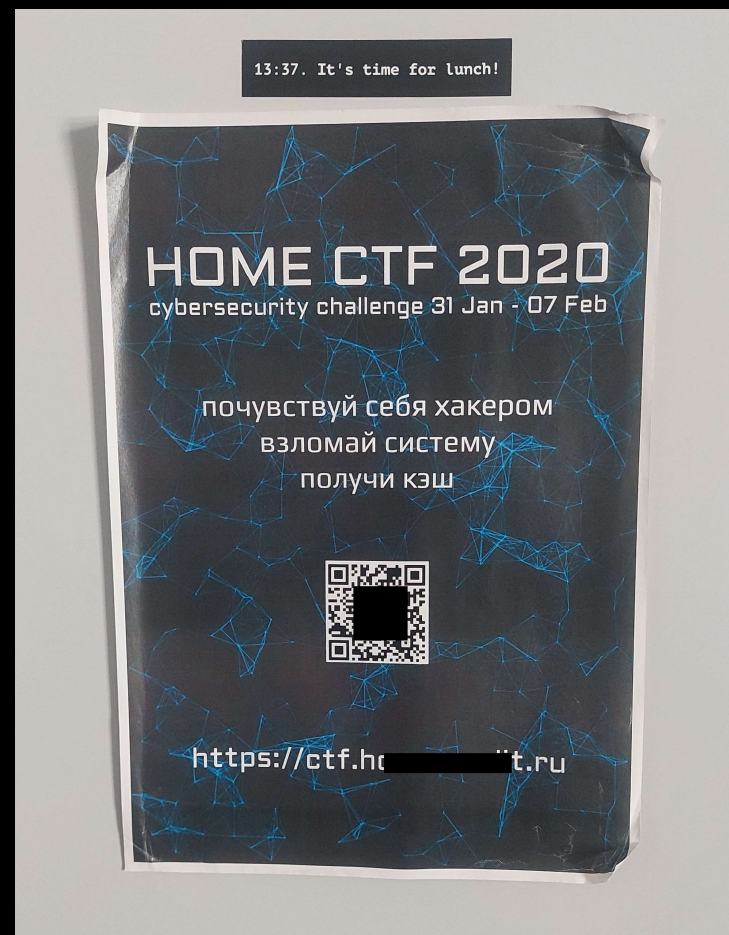
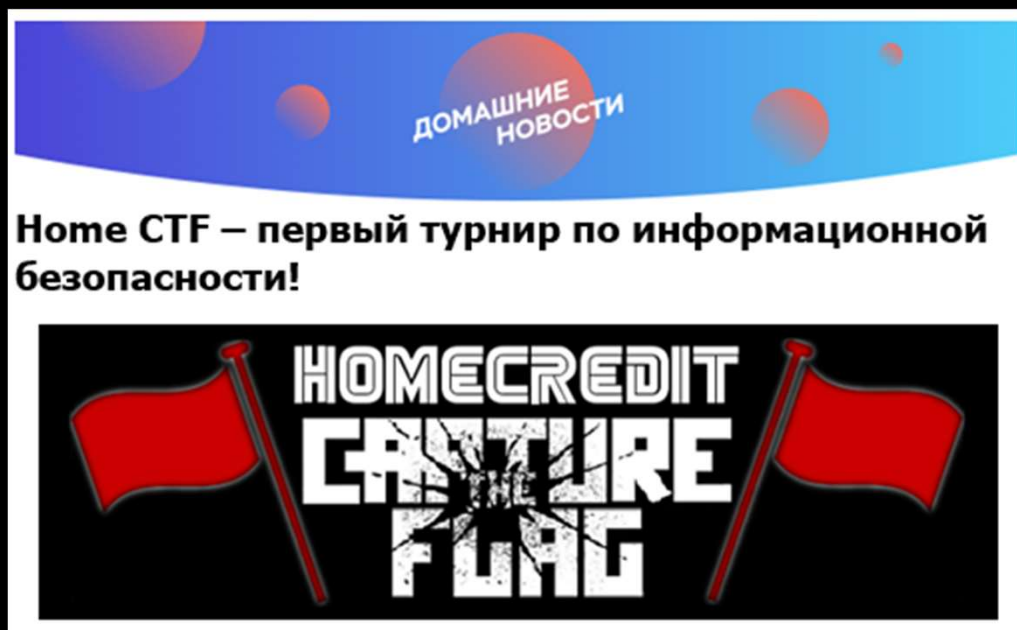
Разворачивание стенда, настройка МЭ: ½ января 2020

Турнир: 31 января – 07 февраля 2020 (Пт 11:00 – Пт 15:00)

Архитектура



Коммуникации



VulnCredit – уязвимое ДБО



VulnCredit

₽ Кабинет оператора

Личный кабинет

+7 () - - -

Дата рождения

Введите код

RXRB



Продолжить

Интерфейс Клиента

VulnCredit - OTP



VulnCredit

Подтверждение входа

SMS код

Продолжить

HomeCTF

Турнирная таблица

Обратная связь

Мои SMS

07.04.2022 21:33:40

Код для входа. Никому не сообщайте, даже сотрудникам Банка

8470

VulnCredit – Кабинет клиента



VulnCredit

Мои счета

9111111111

Мои счета

445433*****4494

1000

445433*****5630

990

О счете

Номер счета: 40817810570009057591

Номер карты: 445433*****5630

Баланс: 990 руб

Создать перевод

Последние операции

04.07.2022 21:41:19

Перевод на счет

40817810570009057591

Сумма: 10 руб.

Операции

Счет списания

40817810570009057591

Счет получателя

40817810570006205082

Сумма (минимум 1р)

50

SMS код

Отправить

VulnCredit – Профиль Клиента

VulnCredit

₽ Мои счета

9111111111

Профиль пользователя

Логин:

9111111111

Аватар



Заменить аватар

Перетащите jpg файл (300x300)

Выберите файл с аватаром

Выберите файл

Файл не выбран

Интерфейс оператора

VulnCredit

₽ Кабинет оператора

Ошибка Доступ к интерфейсу оператора
разрешен только из сети 10.200.0.0/24

Панель оператора

Логин

operator

Пароль

.....

Войти

Интерфейс оператора. Обход ограничений



VulnCredit

Кабинет оператора

Флаг1: {hcfctf}43140fdcfd077b37cfae3722b4810ddf

Флаг2: {hcfctf}85786c39f7c58ee4030ce8c713074d37

Transactions

Search filter...

Timestamp	Пользователь	Счет списания	Счет назначения	Сумма
2022-07-03 23:01:36	7070000000	40817810570004853529	40817810570002368159	841
2022-07-03 23:01:36	7070000006	40817810570007145911	40817810570007445636	832
2022-07-04 21:41:19	9111111111	40817810570009057591	40817810570007920551	10

First Previous **1** Next Last

Total count: 3

⌚ Last 24 hours



2022-07-03 22 : 11

2022-07-04 22 : 11

Пользователь

Счет списания

Счет назначения

Сумма

Search

Кабинет участника

[HomeCTF](#)[Турнирная таблица](#)[Обратная связь](#)

9111111111

Мои SMS

07.04.2022 21:34:02

Код для перевода на счет
40817810570005422659 сумма: 10.0



07.04.2022 21:33:40

Код для входа. Никому не сообщайте, даже
сотрудникам Банка



07.04.2022 21:32:41

Код для перевода на счет
40817810570009057591 сумма: 10.0



Мои флаги 1 из 14

PAN

{hcfctf}26b487bb30e30de6e41f60d77e0e3fd3

Инструменты

Обменять PAN на флаг

PAN

Обменять

Флаг

Мои флаги 1 из 14

Флаг

Отправить флаг

Футболка

	S	M	L	XL	XXL	
	69,5/48	71,5/51	73,7/54	75,5/57	77,5/60	
	XS	S	M	L	XL	XXL
	62/49	69/50	72/53	74/56	76/58	78/62

Размер футболки:

Сохранить размер

Задания – 14 флагов

- Выполнение произвольного кода
- Увеличение средств на своем счете (3 разных способа)
- Чтение произвольных файлов
- Доступ в интерфейс оператора (2 флага: обход ограничения по IP и аутентификации)
- Получение полного номера карты
- Доступ к перс данным других клиентов
- Доступ к транзакциям других клиентов
- Хищение средств с чужого счета
- «Затерянные» флаги (3 шт)

15

Создание транзакции

```
if (srcAccount.balance >= transModel.amount) {
    transModel.ts_committed = Instant.now().toEpochMilli();
    if (AntiFraudManager.checkTransaction(user.getLogin(), transModel.src, transModel.dst,
        transModel.creator.getLogin(), transModel.amount)) {
        AccountModel dstAccount = (AccountModel)
            DBManager.findOne(AccountModel.class, "accountno", transModel.dst);
        srcAccount.balance -= transModel.amount;
        dstAccount.balance += transModel.amount;
        transModel.is_committed = true;
        DBManager.getDao(AccountModel.class).update(srcAccount);
        DBManager.getDao(AccountModel.class).update(dstAccount);
        transModel.flag = flag;
        DBManager.getDao(TransactionModel.class).update(transModel);
    } else {
        throw new Exception("Подозрительная транзакция, обратитесь в Банк");
    }
}
```

```
public static boolean checkTransaction(s
    try {
        Thread.sleep(750);
    } catch (InterruptedException e) {
        return true;
    }
```


Подсчет баллов

Первый нашедший получает все баллы за флаг

У остальных вычитаем штраф: (ранг флага-1)/число флагов

score –

```
((rank() over (PARTITION BY
    flag ORDER BY score DESC, ts_created ASC) ) -1)/c.cnt
```

Подводные камни

Некорректная настройка СУБД, позволяла читать файлы ☺

Scoreboard и CTF располагались на одном сервере => миграция в контейнеры

Допущено несколько багов, несвязанных с
уязвимостям => оперативный фикс



ИТОГИ

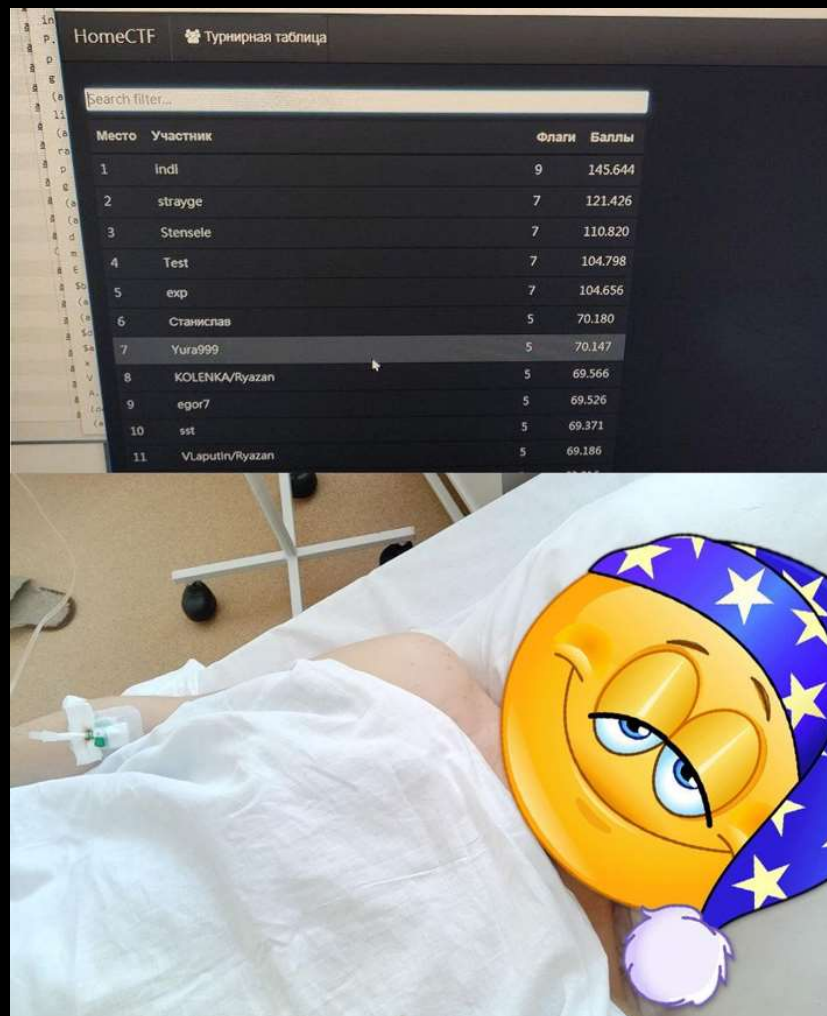
Количество участников: 129

Нашли флаги: 41

Удаление аппендицита не помешало участнику

Максимальный баланс счета:
10 000 000 000 000 000₽

Один из участников сообщил о критичном баге
на **тесте**, который влиял на прод



Спасибо за внимание!



Вопросы?