ПОСТМОРТЕМ QCTF STARTER 2018.2

«Единственная моя ошибка: три четверти жизни я думала, что всё ещё впереди»
Алиса Фрейндлих

9 декабря 2018 года прошёл QCTF Starter 2018.2. Более 500 команд пришло на 50 площадок в трёх часовых поясах, чтобы принять участие в соревнованиях по информационной безопасности для новичков. Однако вместо качественной игры участники столкнулись с множеством проблем: задержка запуска, неработающие и нерешаемые задания, постоянные ошибки на сайте проверяющей системы.

Этот документ — восстановление части тех событий, попытка понять ошибки команды разработки, которые привели к запуску неработающего контеста и тому факту, что почти две тысячи человек потратили 8 часов своего времени на чтение «500 Internal Server Error» в воскресенье 9 декабря.

Постмортем состоит из трёх частей: краткого содержания, полной хронологии событий и анализа возникших проблем. Последняя часть будет полезна тем, кто собирается организовать своё соревнование и не повторить ошибок QCTF.

TL;DR

- Разработка была начата почти за полгода до соревнования, однако правильно рассчитать ресурсы и заранее реализовать все планы не удалось.
- Подготовкой тасков к деплою, запуском проверяющей системы и интеграцией Defense-сервиса разработчики начинают заниматься только в последнюю неделю.
- Большая часть задач была завязана на двух разработчиках, которые не смогли правильно доделать всё необходимое.
- Несмотря на неполную готовность накануне дня соревнования, разработчики были уверены, что успеют всё закончить за оставшееся время.
- Из-за проблем с проверяющей системой начало сдвигается на 1.5 часа, контест запускается с неполным набором тасков.
- Проверяющая система не выдерживает нагрузки и постоянно выдаёт ошибки.
- Из-за нехватки сна большую часть возникающих проблем не удаётся решить до конца соревнования.
- Оставшееся время разработчики пытаются помогать участникам через Telegram.

Полная хронология событий

8 августа

- Выдвигается предложение провести второй QCTF Starter в году.
- Создаётся чат разработки в Telegram, в чат приглашаются разработчики.

11 августа — Первая очная встреча разработчиков

- Выбирается тимлид.
- Обсуждаются дизайн и легенда соревнования, идеи для тасков.
- Возникает идея сделать Defense-таск в стиле классического CTF.
- Планируются задачи по доработке проверяющей системы.

14 августа

- Дизайнер присылает первую версию внешнего вида проверяющей системы.
- Оформляется общая идея легенды соревнования.
- Начинается проработка интерфейса сайта.

23 августа — Вторая очная встреча разработчиков

- К этому моменту уже придумана большая часть тасков.
- Обсуждается сложность тасков, дорабатываются детали легенды.
- Тимлид сообщает о начале активной фазы разработки.
- Создаётся репозиторий, авторы тасков отправляют первые коммиты.

3 сентября

- У команды разработки сменяется дизайнер.

5 сентября — Разработчики Defense-таска встречаются с тимлидом RuCTFE

- Обсуждается архитектура сервиса, процесс выдачи серверов командам.
    1. Первоначальная идея: хостить все команды на одной мощной машине, поднимать контейнеры и выдавать командам доступ в контейнер.
    2. В процессе обсуждения решили использовать Digital Ocean и выдавать каждой команде по дроплету, используя API.
- Используется цифра 500 как верхняя граница числа команд.
  Ожидается 350-400 участников: немного больше, чем на прошлом QCTF Starter.
- Распределяются обязанности по разработке: сервис, выдача машинок, чексистема.
  Из-за недопонимания никто не взял на себя задачу деплоя сервиса на дроплет.

14 сентября

- Становится известна дата RuCTFE — 10 ноября.
- QCTF планируется на 2-3 ноября, чтобы успеть познакомить новичков с Attack-Defense и подготовить к RuCTFE.

18 сентября — Третья очная встреча разработчиков

- Оформляются идеи трёх уязвимостей Defense-таска.
- Команда беспокоится, что разработка не будет закончена за полтора месяца.

- Возникают предложения отказаться от части тасков или от сервиса.
- Тимлид ставит дедлайн разработки тасков: 20 октября.

23 сентября

- Первое предложение помощи от человека извне команды разработки.
  Было проигнорировано, поскольку команда не смогла сформировать конкретных задач. Была уверенность, что времени достаточно чтобы справиться самим.
- Начинается переписка с Digital Ocean по поводу увеличения лимита дроплетов.

26 сентября — Встреча команды разработки с командой организаторов

- Соревнование переносится на 25 ноября, то есть сдвигается почти на месяц.
  Причиной послужили проблемы с организацией двух CTF от Хакердома с разницей в неделю.
- Проявляются первые узкие места: у части разработчиков начинаются проблемы в учёбе, разработка почти написанных тасков “зависает”.

2 октября

- Переписка с Digital Ocean завершается отказом предоставить 500 дроплетов.
- Команда разработки пишет Vscale с аналогичной просьбой.
- В это же время ведётся обсуждение о возвращении к выдаче контейнеров.

5 октября

- В чате разработки целую неделю не было ни одного сообщения.
- Дизайнер забеспокоился и уточнил, продолжается ли разработка.
- Разработка проверяющей системы для Defense заморожена из-за проблем с учёбой.

10 октября

- Дизайнер присылает прототипы всех страниц сайта.
- Остаётся 10 дней до дедлайна, установленного тимлидом.
- Количество тасков в репозитории разработки — 8.

13 октября

- Дизайнер завершил работу над вёрсткой проверяющей системы.

20 октября — Дедлайн, установленный тимлидом

- Количество тасков в репозитории разработки — 9.
- Завершается переписка с Vscale, лимит серверов увеличен до 500.

28 октября

- Команда VoidHack участвует в отборочных на MIEM CTF 2018.

2 ноября — До соревнования чуть больше 20 дней

- Разработчик сервиса Defense консультируется с опытным разработчиком извне команды по поводу деплоя сервиса и написания чексистемы.
- Один из организаторов вступает в команду разработки с идеей своего таска.

4 ноября — QCTF переносится на 9 декабря

- Разгораются споры о создании чата соревнования в Telegram.
- Чат всё-таки создан, но пока не опубликован.

7 ноября

- Организатор одной из площадок просит перевести таски на английский язык.
- Команда разработки относится скептически из-за сложности встраивания перевода.

10 ноября — До QCTF Starter 2018.2 остаётся меньше месяца

- Команда VoidHack участвует в RuCTFE.

17 ноября

- Команда VoidHack летит в Москву и участвует в MIEM CTF 2018 Final.

19 ноября

- Чат соревнования публикуется и сразу же удаляется. Споры продолжаются.
- Разработчики с удивлением обнаруживают отсутствие новых тасков в репозитории.
- В обсуждении выясняется, что над некоторыми тасками работа ещё не велась.

21 ноября

- Начинается написание кода микросервиса для выдачи машинок.
- Начинается процесс соединения дизайна и проверяющей системы.

23 ноября

- Закончена вёрстка Defense сервиса.
- Команда VoidHack участвует в Kaspersky Industrial CTF 2018.

1 декабря

- Команда VoidHack летит в Москву и участвует в Кубке CTF России 2018.

3 декабря (понедельник) — Неделя до соревнования

- Часть команды собирается локально и начинает “усиленную разработку”.
- Директор спрашивает, много ли ещё осталось доделывать до воскресенья. Вопрос успешно проигнорирован.
- Паники нет: разработчики уверены, что успеют всё доделать за неделю.

4 декабря (вторник)

- Появляются подозрения, что участвовать будет больше 500 команд.
- Разработчики пытаются связаться с Vscale (Selectel) напрямую.
- Лимит машинок увеличивается до 1000.

5 декабря (среда)

- Количество участников достигло 500.
- Разработчики усиленно думают над внедрением формата шоу в QCTF.
- По инициативе координатора проводится социальная инженерия организаторов. Регистрируется команда из известных опытных игроков, запрещённых правилами.

6 декабря (четверг)

- Готов чекер и эксплоиты для Defense-таска.
- Готова первая версия микросервиса, выдающего машинки командам.
- Продолжается написание клиентского кода проверяющей системы.
- Начинается процесс докеризации всех серверных тасков.

7 декабря (пятница)

- Успешно тестируется выдача нескольких машинок с помощью микросервиса.
- Пишется скрипт для развёртывания Defense-сервиса на “чистой” машинке.

- В Defense-сервис вносятся изменения, связанные с изоляцией между командами.
- Готов базовый код чексистемы Defense, вносятся правки в работу с таймаутами.
- Разработчики беспокоятся, что не успеют интегрировать части Defense между собой.
- Предлагается перенести QCTF Starter 2018.2 на неделю, директор не соглашается.

8 декабря (суббота)

- Основная часть команды разработки и координатор собирается локально.
- Заметного ощущения проблем до сих пор нет.
- Всё скорее работает, чем не работает, но полной уверенности нет ни в чём.
- При тестировании Defense находится и решается проблема с одним из эксплоитов.

8 декабря (вечер субботы) — Последний вечер перед QCTF

~ 19:00

- Неудачные попытки связать все части контеста между собой.
- Становятся очевидными проблемы, команда разработки сдерживает панику.
- Проблемы с тасками:
    - Над несколькими тасками работа ещё не завершена.
    - Большая часть серверных тасков без докеризации.
    - Статические файлы для команд не сгенерированы ни для одного таска.
    - Ни один таск не подготовлен для встраивания в проверяющую систему.
- Проблемы с проверяющей системой:
    - Не дописан клиентский код.
    - Не дописаны компоненты API для взаимодействия с клиентской частью.
    - Работа над модулем для автоматического встраивания тасков ещё не велась.
    - Система не подготовлена к контесту (участники, сертификаты, площадки…).
- Проблемы с Defense-сервисом:
    - Микросервис по выдаче машинок и чексистема не тестировался при нагрузках.
    - Отсутствует связь между чексистемой Defense и проверяющей системой QCTF.
    - Не разработан механизм управления выдачей машинок командам.

9 декабря (воскресенье) — День проведения QCTF

~ 00:00

- Двое разработчиков дорабатывают и тестируют микросервис выдачи машинок.
- Один разработчик занимается доработкой клиентской части проверяющей системы.
- Ещё один занимается доработкой логики чексистемы Defense.
- Другой разработчик решает задания с hxp CTF 2018 от лица всей команды.

~ 01:00

- Координатор начинает придумывать описания тасков, связывать описания в одну общую легенду.

~ 01:30

- К координатору подключается один из разработчиков, который до этого момента принимал участие в hxp CTF 2018.

~ 02:00

- Разработчики обнаруживают, что у всех тасков отсутствуют сгенерированные статические файлы, предназначенные для выдачи командам.
- Начинается процесс генерации для некоторых тасков.

~ 03:00

- Defense начинает работать в связке с проверяющей системой и микросервисом.
- Разработчики исправляют баги в чексистеме Defense, настраивают коэффициенты.

~ 03:30

- Начинается процесс докеризации оставшихся тасков.
- Разработчики планируют использовать готовые скрипты с прошлых соревнований, поэтому уверены, что много времени это не займёт.
- Разработчик, который занимается докеризацией, параллельно доделывает один из своих тасков.

~ 06:55

- Разработчики выбирают и арендуют виртуальные серверы для проверяющей системы и серверной части тасков.
- Начинается сбор статики, сгенерированной разработчиками, на флешку.
- Два разработчика начинают переносить описания тасков и флаги в конфиг-файлы проверяющей системы.

~ 08:40

- До сих пор не все таски полностью готовы к деплою.
- Принимается решение запуститься с тем набором, который уже готов, а остальные добавить во время контеста.
- Пишется ключевой конфигурационный файл для запуска проверяющей системы.
- Из захардкоженного на фронтенде списка тасков удаляются ещё не готовые.

~ 09:18

- Конфигурационный файл готов, производится первая неудачная попытка запуска проверяющей системы.

~ 09:25

- Один из разработчиков находит проблему: в списке площадок есть две площадки с одинаковым названием.
- Ошибку исправляют, и проверяющая система успешно запускается.

~ 09:30

- Проверяющая система доступна, но участники не могут в неё зайти, поскольку их логины и пароли ещё не загружены.
- Начинается процесс загрузки участников в чексистему. Случайно удаляется папка с настройками деплоя, в процессе восстановления ошибочно запускается деплой прошлого соревнования. Это приводит к необходимости полного перезапуска проверяющей системы и восстановления актуальных настроек по памяти.

~ 10:25

- Проверяющая система полностью поднята. Участники заходят со своими логинами и паролями.
- Сервер с тасками пока ещё не запущен и статика не загружена. В результате, фактически для решения доступны только 2 recon-таска и Defense-сервис.
- В процессе загрузки статики на сервер проверяющей системы происходит обрыв интернета. Архив, занимающий 5Гб, загружается не полностью, в результате после распаковки не всем командам доступны файлы из тасков.

~ 10:40

- Два разработчика начинают деплоить серверную часть тасков.
- В процессе деплоя web-тасков возникают проблемы с TLS сертификатами, успешно поднимается только один таск. Разработчики решают, что дело в неправильном деплое и безуспешно пытаются запустить их заново.
- Остальные TCP таски поднимаются, но в проверяющей системе есть информация только о трёх из них.

~ 11:00

- Начинаются проблемы с ошибками и падениями проверяющей системы.
- Разработчики пытаются её перезапускать, но это не решает проблему и падения повторяются.

~ 12:00

- К этому времени большинство разработчиков больше суток без сна, некоторые из них мало спали всю неделю.
- Те, кто не занимается проверяющей системой, начинают засыпать.

~ 12:30

- Разработчики связываются с Андреем Гейном (автором проверяющей системы Drapo) и объясняют ему возникшие проблемы.
- Андрей вручную получает нужный TLS-сертификат и настраивает nginx. После этого удаётся запустить ранее не работавшие web-таски.

~ 13:00

- Андрей пытается решить проблемы с проверяющей системой: при использовании самого мощного виртуального сервера из доступных его ресурсы быстро исчерпываются.
- Часть обнаруженных недостатков конфигурации удаётся устранить, но это не оказывает заметного эффекта.
- Понять причину нехватки ресурсов не удаётся до конца соревнования.
- С отдельными тасками возникают проблемы, связанные с недостаточным тестированием и отсутствием защиты от вандализма.

~ 14:00

- Вторая попытка загрузки статики на сервер с проверяющей системой. В этот раз удаётся загрузить больше, но на диске кончается свободное место, что опять же приводит к отсутствию файлов у части команд.

~ 14:30

- Разработчики оставляют попытки решить проблемы с проверяющей системой и статикой, понимая, что они не в состоянии это сделать.
- Три разработчика начинают вручную раздавать файлы для тасков через телеграм.

~ 15:50

- Выясняется, что в проверяющей системе было указано неверное время окончания соревнований в первом часовом поясе. Аналогичные проблемы возникают позже и с остальными часовыми поясами. Ошибки исправляются.
- В последующие часы соревнования основными занятиями разработчиков становятся поддержка в телеграме и сон.

«Все уснули до окончания контеста в последнем часовом поясе»
Из ретроспективы QCTF Starter 2018.2

Возникшие проблемы и пути их решения

Глобальные проблемы

1. *Недостаточное количество разработчиков для реализации всех планов.*
    - Более тщательное планирование задач и распределение ресурсов.
    - Отказ от идей, которые сложны в реализации.
2. *Два ключевых разработчика, которые делают основную часть задач, в том числе подготовку к деплою (докеризацию) всех тасков.*
    - Разработчик должен быть полностью ответственен за свой таск, в том числе за его деплой.
    - Для упрощения процесса докеризации полезно иметь готовые шаблоны.
    - Разделение и ограничение ролей: тимлид, админ, разработчик проверяющей системы, разработчик тасков. Нежелательно смешивать эти роли.
3. *Неправильная расстановка приоритетов по деплою: основная часть времени в последние дни ушла на доработку проверяющей системы. При этом вся работа велась на данных предыдущего контеста вместо актуального набора тасков. Это привело к необходимости срочных доделок прямо перед стартом.*
    - Использовать принципы CI: добавлять и деплоить (вместе со статикой) актуальные таски по мере их готовности.
    - Во время разработки для деплоя лучше использовать то же самое окружение, которое будет на контесте.
    - Неработающая чексистема - лучше, чем неработающие таски. Даже если чексистема временно недоступна, участники всё ещё могут решать таски (которые можно получить по сторонним каналам, типа VK и Telegram), а

полученные флаги сдать позже. Следовательно, в первую очередь, должен происходить деплой и тестирование тасков, а только после этого - проверяющей системы.

4. *Недостаточное тестирование.*
    - Таски нужно тестировать, причём не только силами разработчика, но и силами других людей. В том числе, требуется тестирование в боевом окружении.
    - Проверяющую систему нужно тестировать нагрузочно, в особенности узкие места, вроде генерации скорборда.
    - Для генерации скорборда следует применять кэширование.
    - Для Defense-таска нужно было сделать полноценное интеграционное тестирование (т.к. в нём использовалось 3 связанных микросервиса) ранее, чем в ночь перед соревнованием.
5. *Нестабильность проверяющей системы: по историческим причинам, для каждого нового соревнования делается fork Drapo с предыдущего соревнования. Для каждого соревнования вносятся уникальные правки, при этом разработчики со временем меняются. В результате, никто из разработчиков, кроме последнего, полноценно не разбирается в существующем коде.*
    - Нужно вливать полезные общие изменения в базовую версию.
    - Нужно каждый раз наследоваться от базовой версии.
6. *Нерешённые инфраструктурные задачи: автоматическая генерация файлов для проверяющей системы, стандартная защита от вандализма для pwn-тасков.*
    - Проблема являлась следствием п.1 и п.2. Для её решения требовалось перераспределить задачи, выделить отдельного человека, ответственного только за инфраструктуру.
7. *Неправильная оценка числа участников, которая основывалась только на одном QCTF Starter 2018.*
    - Использовать всю историю соревнования для оценки роста числа участников, а также учитывать популярность и рекламную кампанию текущего года.
8. *Поздняя генерация статической раздатки для тасков: из-за большого количества команд создание уникальных заданий занимает значительное время.*
    - Генерировать статику сразу после готовности таска.
9. *Перенос даты QCTF на месяц вперёд, который привёл, с одной стороны, к расслаблению разработчиков, а с другой стороны, к их постоянной занятости: в каждые выходные последнего месяца были какие-либо важные соревнования.*
10. *Недостаток сна у разработчиков, повлиявший на возможность принимать адекватные решения во время соревнования.*
    - Следствие п.1 и п.2.

Частные проблемы

1. В механизме выдачи серверов для Defense-таска был недостаток, который приводил к невозможности получения машины командой. Если в момент создания виртуалки перезапускалась база данных (что происходило часто в связи с решением проблем проверяющей системы), машина считалась созданной, но при этом у неё отсутствовали данные для входа. Единственным способом решения была ручная очистка базы, которая была сделана один раз в середине игры.
2. Случайное удаление скриптов для деплоя проверяющей системы непосредственно перед стартом: работа шла в git-репозитории, но изменения не были запушены на GitHub.
    - Делать `git push` после коммита.
    - Не делать `~/deploy>rm -rf some_dir/ *`, когда нужно `~/deploy>rm -rf some_dir/*`
3. В web-тасках использовался бот от Let's Encrypt, который генерировал TLS-сертификаты для каждого поддомена. Предположительно, из-за повторного деплоя тасков был превышен лимит генерации для IP-адреса сервера, в результате бот перестал выдавать новые сертификаты, и web-таски стали недоступны. Следовало использовать wildcard-сертификат, но разработчики не знали о возможности его получения через Let's Encrypt.
4. Проблемы с производительностью проверяющей системы предположительно были связаны с высокой нагрузкой на скорборд, который обновлялся автоматически и при этом не кэшировался.
5. Кроме того, при деплое на виртуальный сервер проверяющей системы разработчики не обратили внимание на разметку дискового пространства: на сервере был доступен не примонтированный диск на 100 Гб, но деплой выполнили на диски с ОС размером 20 Гб. В результате место быстро закончилось и система начала вести себя неадекватно вплоть до невозможности пользоваться ssh.
    - Не делать деплой в спешке (использовать CI-подход).
    - Проверять достаточность системных ресурсов.
6. В описание нескольких тасков забыли добавить ссылки на исходные файлы, в некоторых случаях ссылки были неправильными. Это произошло, поскольку написанием файлов с условиями для проверяющей системы занимались в ночь перед соревнованиями два выделенных разработчика, которые не были знакомы со всеми тасками.
7. Несовершенство админ-панели проверяющей системы: отсутствие явной возможности править описания задач.
8. В pwn-таске "Аниме" была запланированная RCE-уязвимость, но отсутствовала защита от вандализма: решившая его команда могла удалить флаг из контейнера, и

не дать получить флаг другим командам. Кроме того, в коде таска была проблема с многопоточностью, приводившая к тому, что ответы не соответствовали вопросам. Вторая проблема не мешала решению задания, однако из-за вандализма контейнер пришлось несколько раз создавать повторно. Из-за непрекращающихся удалений флага разработчики принимают решение полностью отключить таск.

9. В какой-то момент один из разработчиков решает, что в таске “Сфинкс” есть проблема, приводящая к невозможности получить флаг. Он также выключается. Только на следующий день после соревнования разработчик понимает, что его предположение было ошибкой.
10. В таске “Драйв” была проблема, связанная с https: в jar-клиенте адрес сервера был указан со схемой http, при обращении по http сервер выполнял редирект на https, но библиотека http-клиента была не готова к редиректам. Это приводило к невозможности полноценно пользоваться выданным исполняемым файлом (возникали исключения), но не мешало решению таска.
11. Когда стало известно о проблемах, несколько не связанных с командой человек предложили свою помощь. Однако разработчики не смогли сформулировать чётких задач, поскольку у них в тот момент не было понимания причин возникших проблем и возможных путей решения. Единственное, о чём могла попросить команда разработки - «починить всё».

Во время проведения соревнования команда разработки накопила ценный опыт, который поможет избежать повторения тех же ошибок в будущем. Предложенные решения будут использоваться при подготовке следующих QCTF. Также они могут быть полезны и при организации других соревнований.

Команда разработки QCTF
Екатеринбург, 19.03.2019