ПРОГРАММА BUG BOUNTY

опыт внедрения с нуля

Bulatenko Igor

- CISO Группы компаний QIWI
- Co-Основатель проекта Vulners
- Специалист по безопасности

BUG BOUNTY

Публичная оферта, предлагаемая компаниями, с помощью которой люди могут получить вознаграждение за нахождение уязвимостей.

ИСТОРИЧЕСКАЯ СПРАВКА

ВСЕ НАЧАЛОСЬ С ОБЫЧНЫХ БАГОВ

Когда ребята из Netscape заметили феномен краудсорсинга для поиска недостатков в их продуктах. И в 1995 году основали первую программу “Bugs Bounty”.

ПОПУЛЯРНОСТЬ

Пришла к такому способу привлечения людей для поиска уязвимостей в 2010-2013, когда данные программы запустили такие гиганты как Facebook, Google и Yahoo. На сегодняшний день подобные оферты имеет почти любая крупная ИТ компания. Даже Пентагон.

ОБЪЕМЫ

Сейчас программы поиска уязвимостей имеют больше 500 компаний в мире. Кто-то платит за баги деньги, кто-то «карму», а некоторые выдают призы «натурой» – собственным железом. По статистике из Vulnerability Lab – на февраль 2018 года всего доступно больше 93,000 публичных тикетов с уязвимостями в этих программах. А, например, ресурс OpenBugBounty показывает более 200,000 публично найденных багов.

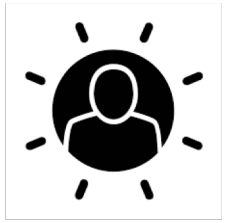
ЦЕННОСТИ

КАЧЕСТВО

Правильно выстроенная программа позволит получить вам сотни высококвалифицированных людей, тратящих дни и ночи на поиск уязвимостей на вашем периметре.

РЕПУТАЦИЯ

Ваша компания будет известна как “people who cares” об информационной безопасности.



ПРОЗРАЧНОСТЬ

Вы не боитесь признать, что вы тоже люди и публично можете признать свои ошибки. Ведь это показатель того, что вы работаете над проблемой, а не прячете ее под ковром «корпоративной тайны».

МЕТОДЫ РЕАЛИЗАЦИИ

Сама идея весьма проста – поощрять людей за поиск уязвимостей в ваших приложения.

Но это можно организовать по-разному.

ПРИВАТНАЯ

Вы можете запустить программу таким образом, что пригласите только «топ» хакеров в рейтинге к участию. Остальные о ней не узнают.

МОДЕРИРУЕМАЯ

Промежуточная компания обеспечит вам предварительную проверку багов и профессионализм участников.

ПУБЛИЧНАЯ

Любой смертный способный искать баги может принять участие.

ПЛОЩАДКИ

bugcrowd.com

- Заявленные ошибки при необходимости дополнительно модерируются командой bugcrowd
- Возможность «хостинга» бесплатных программ

hackerone.com

- Наиболее популярная платформа с почти 200 программ от ведущих it-корпораций
- Большое количество исследователей
- Возможность «хостинга» бесплатных программ

synack.com

- Высококвалифицированные исследователи, которые перед началом работы проходят ряд тестов и испытаний
- Своя RedTeam команда
- Высококачественные отчеты об уязвимостях

ВОЗМОЖНОСТИ

	Private	Public	Moderated
Плюсы	- Известный круг исследователей, выбранный владельцем программы - Гарантированная приватность	- Сканирование сети 24/7/365 - Низкая стоимость - «Свежая кровь» каждый день	- Под каждую программу подбираются определенные исследователи модераторами платформы - Высокое качество исследований
Минусы	- Ограниченный круг исследователей - Кратковременная программа (пока приглашенным интересно)	- Возможность публичного раскрытия ошибки до ее исправления	- Высокая стоимость

QIWI BUGBOUNTY

”РУЧНАЯ BUGBOUNTY”

- Получение репортов/общение через почту
- Крайне низкий поток обращений
- Долгие и тяжелые выплаты (в т.ч. с приездом участника в офис)

ЗАПУСК H1

NOWADAYS

- Невозможность доказать участнику, что это дубль
- Нет статистики, контроля, никакой автоматизации

QIWI BUGBOUNTY

”РУЧНАЯ BUGBOUNTY”

- Запуск публичной программы во время Zeronights 2014
- Первый репорт был в течение нескольких минут после открытия программы
- Несколько месяцев разбора репортов
- Ограниченный scope

ЗАПУСК H1

- Много новых полезных и не очень заголовков на сайтах
- «О, у нас оказывается и такой домен есть»
- Сложность с отслеживанием дублей
- Время реакции могло составлять несколько месяцев
- Размер выплат сильно варьировался
- «Горшочек, не вари»

NOWADAYS

QIWI BUGBOUNTY

”РУЧНАЯ BUGBOUNTY”

ЗАПУСК H1

NOWADAYS

- Scope не ограничен
- Разделение размера выплат исходя из уязвимости и домена
- Авто-ответы
- Привлечение topX хакеров на начальных стадиях
- Интеграция с таск-трекером

- SLA на время ответа
- Минимальное количество N/A, Duplicate репортов
- 5 RCE, выплаты 3137$ и 1337$

QIWI

УСВОЕННЫЕ ОШИБКИ

ПЛАВНО ПОВЫШАТЬ ТЕМПЕРАТУРУ

Открывать bug-bounty вначале в приватном режиме
Ограниченный scope, только на основные домены

ПРОЗРАЧНОСТЬ ВЫПЛАТ

Описанные критерии по выплатам, возможно иногда с множителями

ДУБЛИ

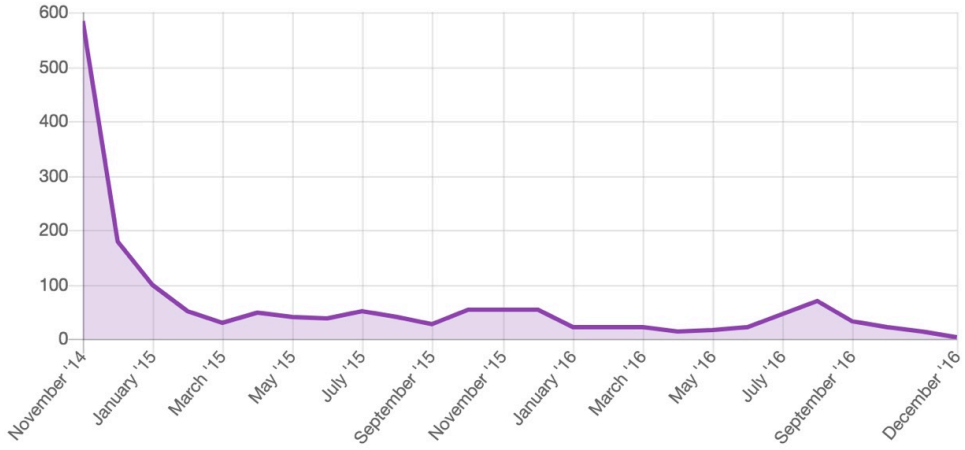
Реестр проверенных репортов со статусами
Показывать дубли хакерам

ГРАМОТНАЯ ОФЕРТА

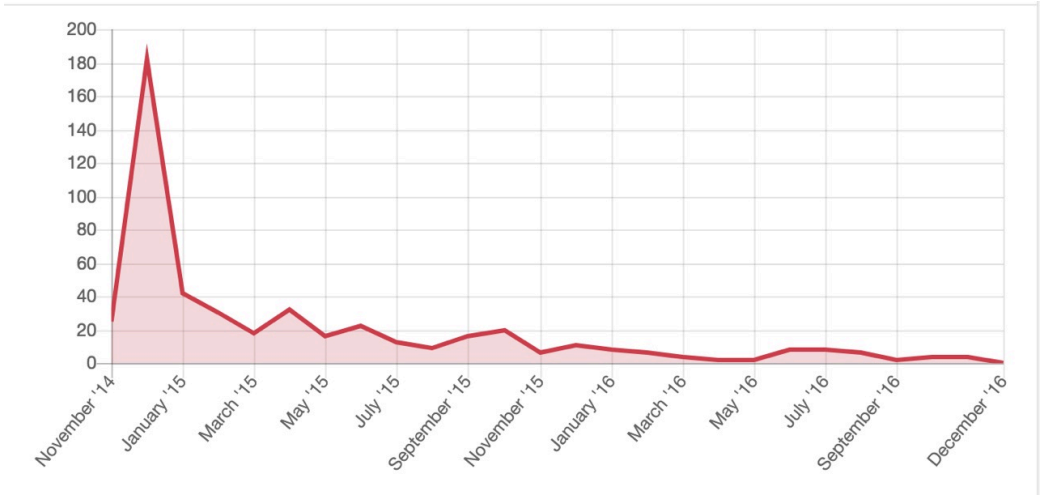
Заранее описанные out-of-scope уязвимости

СТАТИСТИКА ЗАПУСКА

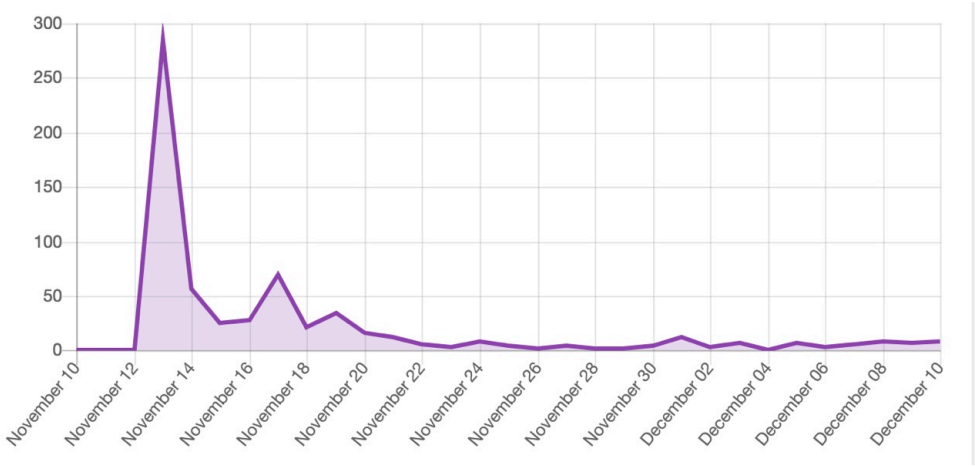
НОВЫЕ ОТЧЕТЫ



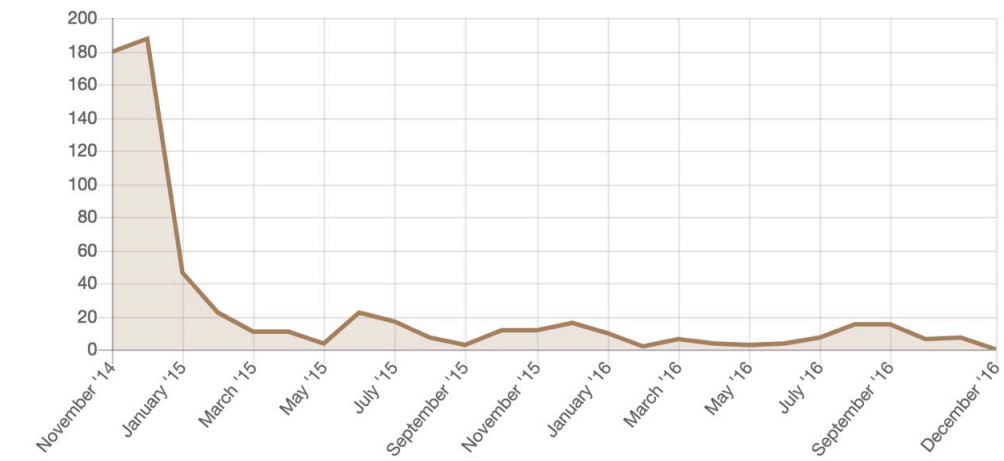
НЕ ПРИМЕНИМО



НОВЫЕ ОТЧЕТЫ (ПО ДНЯМ)



ДУБЛИКАТЫ



ПОДГОТОВКА ВАШЕЙ КОМПАНИИ

Ключевым моментом станет выстраивание правильных процессов и минимальная подготовка внутри вашей компании.

CRITICAL FIRST

Вам нужно договориться с IT про SLA по исправлению уязвимостей.

РАЗБОР БАГОВ

В среднем для работы по разбору очереди хватит 2 специалистов + 1 младшего специалиста.

ЛИНКОВКА

Вам необходимо продумать систему связей идентификаторов в Bounty-платформе и внутренней тикетнице.

КАТАЛОГ ДУБЛЕЙ

Понадобится создать внутренний каталог уязвимостей, который позволит быстро определять дубликаты.

ДЕНЬГИ ВПЕРЕД

Внесите в бюджет деньги заранее, что бы не попасть в ситуацию с невозможностью выплаты вознаграждения.

PR

Для эффективной работы Bug Bounty вам ее нужно будет разрекламировать. Подготовьте мотивирующие посты и пресс-релизы.

ПРЕДУПРЕДИТЕ БИЗНЕС

На первых этапах программы вы рискуете столкнуться с недоступностью сервисов и увеличением time to market.

КРИТЕРИИ ОПЛАТЫ

Сформируйте прозрачный и понятный «прайс-лист» по вашим уязвимостям. Ориентируйтесь на средний ценник на H1.

ПРОВЕДИТЕ ПЕНТЕСТ

Но акцентируйте на необходимости подготовки к запуску Bug Bounty.

ОГРАНИЧЬТЕ SCOPE

Выберите бизнес-критичные приложения и ресурсы.

ПРИВЛЕКИТЕ ЮРИСТОВ

Для создания юридически значимой оферты.

ПРОКОНСУЛЬТИРУЙТЕСЬ

У любой большой компании, которая имеет Bug Bounty. Один вечер в баре сделает больше чем мой мастер класс.

ПРОСТЫЕ ПРАВИЛА

Как сделать вашу программу привлекательной для исследователей.

ПРАВИЛО $50

Не жадничайте платить деньги даже за самые простые уязвимости.

ВЫПЛАТЫ

Вы смогли воспроизвести уязвимость? Уважайте труд исследователя – заплатите ему сразу.

N/A

Не портите карму исследователям просто так. N/A заслуживают только спамеры.

НЕ ТОРМОЗИТЕ

Старайтесь, чтобы среднее время ответа на уязвимость и ее проверку не превышала недели.

ПОЕХАЛИ!

МЯГКИЙ ЗАПУСК

Выберите основное приложение и оставьте в скоупе только его. Ограничьте круг приглашенных хакеров до 20 человек. Лимитируйте выплаты до $100 за типовые уязвимости.

ОБКАТАЙТЕ ПРОЦЕССЫ

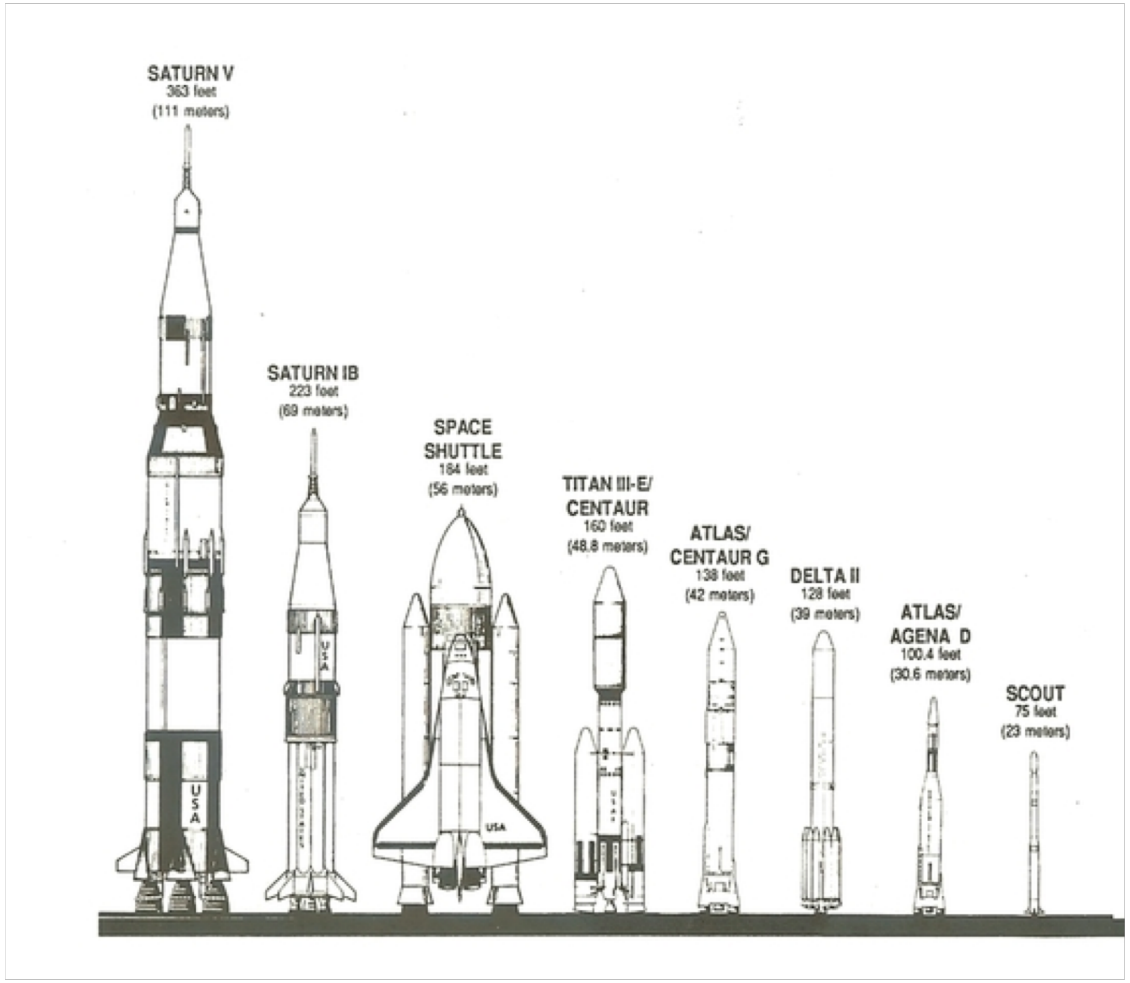
Маленький поток уязвимостей позволит проверить SLA обработки и исправления уязвимостей на вашей стороне.

РАСШИРЯЙТЕ КОЛИЧЕСТВО УЧАСТНИКОВ

По мере стабилизации потока заявок можно начать расширять скоуп и количество участников. Баланс будет зависеть от вас. Если вы увидите просадку по участникам – увеличивайте стоимость уязвимостей.

ПРОГРАММА МАКСИМУМ

За полгода вы должны выйти в состояние «открытой» программы но с ограниченным скоупом. За год достигнуть «открытого» скоупа – ломать можно все. Цены на ваши уязвимости должны стать «среднерыночными» - ориентируйтесь на Mail.ru, Yandex, Twitter, Uber.



TL;DR

ПОЧЕМУ BUG BOUNTY

Фактически это самый экономически выгодный и эффективный способ проведения внешнего vulnerability assessment.

СИЛА ТОЛПЫ

Сотни хакеров способны найти больше чем отдельная команда. Их мотивация в результате, а не затраченном времени.

ЦЕНА

Стоимость нахождения одной уязвимости для вас будет максимально низкой.

ЛЕГАЛИЗАЦИЯ

Зачем бороться с хакерами? Дайте им легально заработать!

Q&A

@V1DENS

VIDENS@QIWI.COM

QIWI.COM