Написан инструмент сканирования уязвимостей.

Ли И начал испытание.

Войдите на платформу Hackerone, зарегистрируйте учетную запись, войдите на платформу, войдите в проект публичного тестирования уязвимостей, инициированный компанией, и получите IP-адрес соответствующего сервера. Затем Ли И запускает самодельный инструмент сканирования уязвимостей одним щелчком мыши.

В следующую секунду лихорадочно возник водопад зеленого кода, инструмент сканирования уязвимостей заработал без сбоев, и каждый подмодуль начал работать над анализом уязвимости сайта сервиса.

…

Fenggu Technology, зарегистрированная на бирже компания-разработчик программного обеспечения со штаб-квартирой в Magic City, стремится содействовать глубокой интеграции информатизации и индустриализации, а также повышать уровень городского интеллекта. Его бизнес охватывает сталь, транспорт, медицину, химическую промышленность, финансы и другие отрасли, и он глубоко вовлечен в программное обеспечение. В этой области он в конечном итоге стремится к безопасности программного обеспечения и системной безопасности.

Чжан Пейюн, глава научно-технического отдела Фэнгу, как и в прошлом, включал компьютер как можно скорее после выхода на работу, проверял свой почтовый ящик, просматривал ход работы своих подчиненных и планировал следующий шаг.

Внезапно раздался стук в дверь, прервавший мысли Чжан Пейюн.

"Заходи!" Чжан Пейюн поднял глаза и выглянул за дверь.

«Брат Юн, это нехорошо. В проекте Rongcheng Smart Cloud было обнаружено много ошибок. После исправления этих ошибок рабочая нагрузка почти эквивалентна его сносу и переделке». Молодой человек с редкими волосами, Чжао Сяохуэй, толкнул дверь и сообщил с грустным лицом.

«Rongcheng Wisdom Cloud? Какой проект открыт для публичного тестирования на платформе?» Чжан Пейюн спокойно посмотрел на Чжао Сяохуэй и спросил.

«Да! Мастер обнаружил много лазеек». Чжао Сяохуэй подтвердил это с горьким лицом.

Чжан Пейюн быстро открыл платформу и зашел в фоновом режиме.

В следующий момент серверная часть веб-сайта отображает часть данных об уязвимости, уязвимость RCE, уязвимость внедрения SQL, уязвимость захвата учетной записи, CORS, CSRF, утечку исходного кода, ограничение скорости, … и т. д., всего 227 уязвимостей.

Чжан Пейюн увидел, как онемел его череп.

Существует так много?

оригинал или подделка!

Чжан Пейюн был полон недоверия и нажал на данные об уязвимости RCE.

Эта уязвимость нацелена на поддомен, и его каталог .git был обнаружен при использовании Dirb для взрыва каталога. При использовании углубленного обнаружения POST-параметры звонка не подвергались фильтрации и аудиту, и это было связано с уязвимостью удаленного выполнения кода.

Выражение лица Чжан Пейюна напряглось, и, судя по приведенному выше описанию уязвимости, он немедленно начал тест.

Чжан Пейюн положил руки на клавиатуру и сделал серию операций. Вскоре, судя по описанию уязвимости, он напрямую врубился в уязвимость проекта Rongcheng Smart Cloud.

Вот дерьмо!

Эта лазейка действительно есть.

Чжан Пейюн запаниковал и без всякой веры продолжил проверять следующую лазейку.

Вскоре Чжан Пейюн продемонстрировал по описанию средство обнаружения уязвимостей и успешно получил весь исходный код службы приложений на сайте. Эта уязвимость намного серьезнее, чем предыдущая уязвимость RCE.

Капля холодного пота упала на лоб Чжан Пейюна.

Если эта уязвимость не будет обнаружена после запуска проекта, она будет использована, что серьезно угрожает безопасности данных клиентов.

Чжан Пейюн глубоко вздохнул и продолжил смотреть на следующую лазейку.

Это уязвимость для взлома аккаунта. Заменив адрес электронной почты на адрес электронной почты другого пользователя, пароль, содержащийся в пакете запроса, можно использовать для замены и изменения пароля учетной записи других лиц. Весь процесс не требует какого-либо механизма проверки.

Чжан Пейюн постоянно проверял пять или шесть лазеек, и каждая лазейка была настоящей.

отлично!

Чжан Пейюн был одновременно и зол, и счастлив, и его настроение было очень сложным.

Причина его гнева в том, что его техническая команда написала баг с множеством лазеек, что представляет собой просто кучу мусора.

Причина счастья в том, что эти проблемы были обнаружены, что позволило избежать передачи их клиентам и создало огромные скрытые опасности.

«Брат Юн, что ты будешь делать дальше?» — с тревогой спросил Чжао Сяохуэй, глядя на разгневанное лицо Чжан Пэйюна.

"Что делать? Что делать! Все помогли нам найти лазейки, почему бы вам просто не оставить это в покое? Скажите всем, чтобы собраться в конференц-зале!" Чжан Пей отчаянно закричал.

"Хорошо!" Чжао Сяохуэй поклонился в ответ и покинул офис, словно убегая.

Чжан Пейюн встала и бросилась в конференц-зал, чтобы договориться о проверке.

Вскоре после этого в конференц-зале раздались траурные взрывы программистов.

В указанный срок необходимо исправить более 200 лазеек. Огромная рабочая нагрузка и длительная сверхурочная работа, выходные, праздники и т. д. обречены на какой-то период времени в будущем. Даже не думай об этом.

Наблюдая, как его подчиненные в отчаянии уходят один за другим, у Чжан Пейюна тоже было грустное лицо. Изначально он планировал провести выходные с дочерью в день ее рождения. Если бы у проекта была такая серьезная проблема, он, ответственное лицо, точно не смог бы уйти.

«Брат Юн, как следует вознаграждать искателя ошибок? Если ошибок больше 200, если награда слишком велика, финансовая сторона определенно не одобрит деньги». Чжао Сяохуэй нервно посмотрел на Чжан Пейюна и попросил инструкций.

Услышав это, лицо Чжан Пейюн стало еще более уродливым.

Вообще говоря, выкапывание лазейки обычно дает первооткрывателю несколько тысяч или даже десятков тысяч бонусов. Если его заменят международные гиганты, такие как Microsoft и Apple, если будет обнаружена крупная лазейка, они могут получить даже сотни тысяч, а то и десятки миллионов бонусов. , единица все еще американский нож.

Награда в несколько тысяч юаней за ошибку очень мала.

Даже если на лазейку дается всего несколько тысяч, более двухсот лазеек обойдутся почти в миллион. Для компании это большие непредвиденные расходы. Странно, что финансовый менеджер его не беспокоит.

Более того, деньги должны быть отданы. Этот парень может найти так много лазеек. Он должен быть мастером техники. Кто знает, есть ли у него другие лазейки в руках?

Меньше давать нецелесообразно, и финансы не одобрят, если вы дадите слишком много.

Думая об этом вопросе, Чжан Пейюн был ошеломлен.

«Брат Юн, если все в порядке, я сначала пойду на работу!» Видя, что лицо Чжан Пейюн становится все хуже и хуже, Чжао Сяохуэй поспешно попрощался.

— Подожди, у меня есть для тебя задание. Чжан Пейюн быстро остановил Чжао Сяохуэй.

Чжао Сяохуэй сделал паузу, показывая раскаявшееся лицо, жалея, что не может ударить себя.

Я хочу, чтобы вы больше говорили, а вот и миссия!

«Брат Юн, в чем заключается миссия!» Чжао Сяохуэй обернулся и спросил с кривой улыбкой.

«Вы можете связаться с этим экспертом и получить скидку». Чжан Пейюн устроил.

«Брат Юн, я не умею торговаться! Почему бы тебе не поговорить с ним лично!» Чжао Сяохуэй выглядел смущенным, трудно сказать.

— Ты сначала с ним поговори, если не договоришься, я уйду. Должен быть переход, понял? Чжан Пейюн посмотрел на Чжао Сяохуэй и напомнил.

«Хорошо! Брат Юн, каковы ваши ожидания от торга?» Чжао Сяохуэй кивнул и спросил.

— Конечно, чем меньше, тем лучше. Лазейка — две-три тысячи, а серьезная — меньше десяти тысяч. Попробуй и посмотри, сможешь ли ты о ней говорить. Чжан Пейюн ответил.

«Брат Юн, это слишком мало! Он может согласиться?» Чжао Сяохуэй почесал затылок, чувствуя, что это задание очень сложное.

"Сделайте все возможное! Такие большие траты обязательно будут вычтены из бонуса за проект. Для бонуса каждого, пожалуйста, сделайте все возможное! Я действительно не могу говорить об этом, я расскажу об этом еще раз." Чжан Пейюн воодушевлен.

Когда такой большой горшок был разбит, Чжао Сяохуэй был ошеломлен, сбит с толку и каким-то образом вышел из конференц-зала.