

ПРОГРАММА ВЗАИМОДЕЙСТВИЯ С ИССЛЕДОВАТЕЛЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Author: Bekarys Kabi

BUG BOUNTY — ЭТО МОДЕЛЬ КИБЕРБЕЗОПАСНОСТИ, ПРИ КОТОРОЙ КОМПАНИИ ОТКРЫТО ИЛИ ПРИВАТНО ПРИГЛАШАЮТ НЕЗАВИСИМЫХ ИССЛЕДОВАТЕЛЕЙ (ЭТИЧЕСКИХ ХАКЕРОВ) ИСКАТЬ УЯЗВИМОСТИ В ИХ СИСТЕМАХ. ЗА НАЙДЕННЫЕ БАГИ ОНИ ПОЛУЧАЮТ ДЕНЕЖНОЕ ВОЗНАГРАЖДЕНИЕ ИЛИ ДРУГУЮ МОТИВАЦИЮ.



КАК ЭТО РАБОТАЕТ

 Компания публикует правила, цели и скоуп



Багхантеры ищут уязвимости



Модерация и триаж отчетов



Выплаты и оплата налогов, сборов и пр.



ЦЕННОСТЬ



Глобальное сообщество исследователей



Реальные атаки = реальные баги



Репутация и доверие: компания показывает открытость и зрелость в вопросах безопасности.

Современная киберзащита — это постоянный диалог бизнеса и исследователей, где каждый найденный баг укрепляет доверие клиентов.

Сравнение подходов к безопасности: Пентест и Bug Bounty

Пентест выявляет уязвимости в ограниченные сроки, а Tumar.One обеспечивает непрерывный поиск и постоянный контроль за безопасностью.

Сравнительный анализ

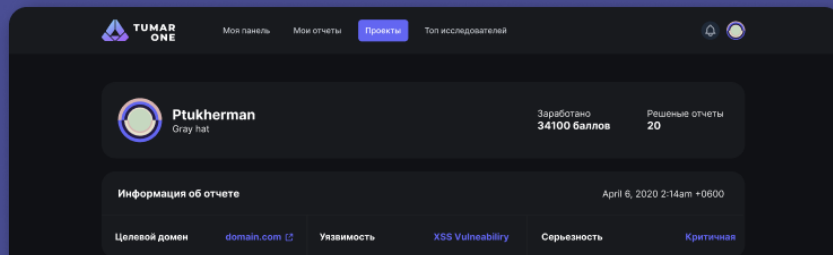
	 Пентест	 Bug Bounty
 Цена	фиксированная стоимость услуги, не зависит от найденных уязвимостей	сдельная оплата труда и оплата только за реальные подтверждённые баги
 Время	ограниченный срок проведения, обычно раз в год/проект.	тестирование идёт непрерывно 24/7/365.
 Навыки	привлеченная или штатная ИБ-команда (2-10 специалистов)	Независимые исследователи со всего мира с разными навыками и креативным подходом находят уязвимости, которые не выявляет классический аудит
 Результат	единый технический отчёт по завершению работ	постоянный поток отчётов и защита между релизами

На самом деле эти подходы взаимодополняют друг друга: пентест закладывает фундамент безопасности, выявляя основные векторы атак, а краудсорсинговая модель обеспечивает непрерывный поиск новых уязвимостей и постоянный контроль между релизами.



Первая и самая масштабная Bug Bounty платформа в Центральной Азии. Пул проверенных исследователей помогает находить уязвимости быстрее, чем это сделают злоумышленники.

Платформа для выявления уязвимостей в информационных системах за вознаграждение



Cloud, Open-Source On-Premise Bug Bounty платформа

~3 000

Независимых этических хакеров со всего мира

от 40 до 100+

Уязвимостей в год

20 публичных программ и весь QazNet (Национальная баг баунти платформа)



4 500+

Отчетов об уязвимостях получено



1	Remote Code Execution (RCE)	13%
2	Sensitive Data Exposure	11.3%
3	SQL Injection	9%
4	Insecure Data Object References (IDOR)	7%
5	Path Traversal	6,7%
6	Account Takeover	3%
7	Stored XSS	3%
8	Reflected XSS	3%
9	Прочие виды уязвимостей	44%



12 месяцев – полный цикл контроля уязвимостей



Ключевые инциденты, предотвращённые с помощью платформы

За 5 лет работы мы помогли компаниям и госструктурам избежать критических последствий, обнаружив и закрыв тысячи уязвимостей до того, как ими воспользовались злоумышленники.

Образование

предотвращена утечка
данных 10 ведущих вузов.

Госуслуги

300 уязвимостей в электронном
правительстве

Критическая инфраструктура

предотвращён доступ к системе
водоснабжения г. Астаны

ЭЦП

Ошибка настройки ЭЦП дала
доступ к личным кабинетам физ
и юр.лиц на более чем 50 веб-
ресурсах.



КЛЮЧЕВЫЕ ДОСТИЖЕНИЯ ЗА 5 ЛЕТ

ЗА ПЯТЬ ЛЕТ МЫ ПРОШЛИ ПУТЬ ОТ ИДЕИ ДО ЗРЕЛОЙ ЭКОСИСТЕМЫ, КОТОРАЯ МЕНЯЕТ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ В РЕГИОНЕ И ФОРМИРУЕТ НОВЫЕ СТАНДАРТЫ РАБОТЫ С УЯЗВИМОСТЯМИ.

1

TUMAR.ONE СТАЛ ДЕ-ФАКТО
НАЦИОНАЛЬНОЙ ПЛАТФОРМОЙ

2

ПОДДЕРЖКА ВЕДУЩИХ КОРПОРАЦИЙ И БАНКОВ
КАЗАХСТАНА, УЗБЕКИСТАНА И КЫРГЫЗСТАНА

3

ПРИНЯТИЕ ЗАКОНОДАТЕЛЬСТВА О “БЕЛЫХ
ХАКЕРАХ” И ЛЕГАЛИЗАЦИЯ БАГБАУНТИ-
ПЛАТФОРМ.

4

ЗАПУСК ПЕРВОЙ В МИРЕ OPEN-SOURCE BUG
BOUNTY ПЛАТФОРМЫ



ПРИЗНАНИЕ НА ГОСУДАРСТВЕННОМ И
РЕГИОНАЛЬНОМ УРОВНЕ.



ВКЛЮЧЕНИЕ TUMAR.ONE В РЕЕСТР
ДОВЕРЕННОГО ПО РЕСПУБЛИКИ
КАЗАХСТАН

Наши клиенты

Телекоммуникации

Финансовый сектор

Государственный сектор

Крупные и средние корпорации

Промышленность



Development Bank
Kazakhstan



Kaspi.kz



e.gov



Kcell

БАНК
КОМПАНИОН®

mbank

Payme



UZTELECOM

 uztelecom.uz

TSARKA GROUP



**TUMAR
ONE**

Let's work together



+998 95 008 01 75



info@tumar.one