**ПУБЛИЧНАЯ ОФЕРТА №KHS/23/30**

**г. Астана 13.11.2023**

ТОО «KazHackStan» (БИН 120540005677), именуемое в дальнейшем «Оператор», в лице Директора Сатиева О.Ш., действующего на основании Устава, выражает намерение заключить Договор об оказании услуг по предоставлению доступа к веб-ресурсу, расположенному в сети Интернет по адресу: <https://tumar.one/> (далее – Договор) и представляет собой официальное предложение по предоставлению доступа к Платформе TumarOne.

**Термины и определения**

1. «Оператор» – юридическое лицо, которому принадлежит Платформа, и которое самостоятельно и по своему усмотрению определяющее порядок использования Платформы в сети Интернет, в том числе порядок размещения информации на «Платформе». Все исключительные имущественные права на Платформу принадлежат Оператору.
2. «Платформа» – веб-ресурс, расположенный в сети Интернет по адресу: <https://tumar.one/>. Платформа представляет собой программу вознаграждения за найденные уязвимости в информационных системах и ресурсах.
3. Оферта – текст настоящего Договора – оферты, опубликованного на Сайте Оператора: <https://tumar.one/offer> и является Офертой Оператора всем исследователям в соответствии п. 5 ст. 395 Гражданского кодекса Республики Казахстан.
4. Акцепт – в соответствии со ст. 396 Гражданского кодекса Республики Казахстан, ответ потенциального Пользователя, которому адресована настоящая Оферта, о полном и безоговорочном ее принятии и согласии с условиями настоящего Договора путем совершения действий, указанных в разделе 1 настоящего Договора. Акцепт Оферты влечет за собой заключение Договора между Оператором и Пользователем. Совершая действия по Акцепту настоящей Оферты, Пользователь подтверждает свою правоспособность и дееспособность, отсутствие каких-либо ограничений, в том числе, определенные действующим законодательством на заключение настоящего Договора, а также свое законное право вступать в договорные отношения с Оператором.
5. Пользователь (исследователь) – полное дееспособное физическое лицо, выразившее акцепт Оферты в соответствии с пунктом 1.2. Договора и зарегистрированные на Платформе, которые осуществляют работу по поиску уязвимостей в соответствии с условиями Договора, действующее от своего имени.
6. Регистрация — заполнение Пользователем регистрационной формы, расположенной на Платформе, путем указания необходимых сведений.
7. Регистрационная форма — форма, расположенная на Платформе, которую Пользователь должен заполнить для возможности использования сайта в полном объеме.
8. Личный кабинет – персональный раздел Пользователя в Платформе, защищенный параметрами авторизации посредством применения логина и пароля, предоставляющий функции Платформы согласно Регламенту, доступный Пользователю после авторизации на Сайте Оператора.
9. Регламент – документ, в котором определяется порядок работы в Платформе согласно Приложению №1 к настоящему Договору, являющегося неотъемлемой его частью.
10. Верификация – процесс подтверждения личности Исследователя в целях произведения оплаты за подтвержденные уязвимости.
11. Программа – инициатива по выявлению уязвимостей в веб-сервисах и приложениях Клиента, а также по определению способов реализации недопустимых событий, которая размещена на соответствующей странице Платформе.
	1. **Общие положения**
	2. Текст Договора является публичной офертой. Акцепт оферты – регистрация на Платформе по следующему адресу <https://tumar.one/offer> и продолжение ее использования.

Совершая действия по акцепту настоящего публичного Договора – оферты, Пользователь гарантирует свою правоспособность и дееспособность, а также свое законное право вступать в договорные отношения с ТОО «KazHackStan». Перед началом пользования Платформы Пользователю необходимо внимательно ознакомится с условиями его использования, содержащихся в настоящем Договоре. Начало использования Платформы означает надлежащее заключение настоящего Договора и полное согласие Пользователя со всеми его условиями.

* 1. Акцептом Пользователя по заключению Договора является выраженное согласие с его условиями и совокупность следующих действий Пользователя во время регистрации в Платформе Оператора:
		1. введение регистрационных данных согласно регистрационной формы.
		2. ознакомление, согласие и принятие условий Оферты.
		3. совершение Пользователем действий, определенных данным Договором, свидетельствующих о полном и безоговорочном принятии всех его условий, а также проставлением галочки в графе «Я согласен с условиями предоставления сервиса» на сайте Оператора при регистрации.
1. **Предмет Договора**
	1. Оператор на безвозмездной основе предоставляет Пользователю доступ к Платформе, в которой размещены программы Клиентов Оператора, в которых Пользователь производит поиск уязвимостей. В свою очередь за найденные уязвимости Оператор выплачивает вознаграждение Пользователю в соответствии с Договором и положениями каждой отдельной программы.
	2. Пользователь осуществляет поиск уязвимостей программ, размещенных в Платформе в порядке, определенном Договором.
2. **Права и обязанности Сторон**
	1. Пользователь вправе:
		1. Пользоваться Платформой за исключением времени проведения профилактических, технических и аварийных работ.
		2. Вносить и отправлять Оператору предложения по улучшению функциональных возможностей Платформы либо в письменном виде на электронную почту Оператора, указанную на сайте Оператора.
		3. Направлять запрос в службу технической поддержки Оператора по факту распространения данных об уязвимостях.
		4. Принимать участие в акциях, мероприятиях, получать бонусы.
		5. Получать вознаграждение от Оператора.
	2. Пользователь обязуется:
		1. Соблюдать условия настоящего Договора.
		2. Использовать Платформу в соответствии с его назначением, а также в соответствии с положениями Договора, Регламента и иных документов, и информации, опубликованных на Сайте Оператора и в Платформе.
		3. Использовать в Платформе действительные данные, удостоверяющие личность, контактные данные.
		4. Отслеживать уведомления в Платформе и электронной почте, указанной при регистрации в Платформе. На принятие повторного тестирования со стороны Пользователя есть ровно 2 недели с появление заявки, после истечения срока заявка на повторное тестирование будет автоматически отклонена.
		5. Не выдавать себя за другое лицо в Платформе.
		6. Не публиковать в средствах массовой информации, интернете, социальных сетях данные, информацию о Платформе без официального письменного согласия Оператора.
		7. Не допускать обманных, неправомерных или неэтичных действий, которые могут нанести имущественный или репутационный вред Оператору.
		8. Соблюдать и не нарушать авторские и интеллектуальные права Оператора.
		9. Проходить процесс верификации для получения оплаты за подтвержденные уязвимости.
		10. Предоставлять акт выполненных работ/оказанных услуг Оператору на подписание.
		11. Зарегистрироваться на платформе по подписанию ЭАВР по ЭЦП и подписывать ЭАВР в случае, если Пользователь является гражданином или резидентом Республики Казахстан. Платформа определяется Оператором самостоятельно.
		12. В случае, если Пользователь не является гражданином и резидентом Республики Казахстан, в таком случае Пользователь обязуется предоставить Оператору скан-копию Акта выполненных работ (АВР) в соответствии с формой, установленной и предоставленной Оператором. Данная скан-копия должна быть предоставлена до момента обмена оригиналами между сторонами.
	3. Пользователю запрещается: использовать любые средства «глубинного связывания», осуществлять сбор информации на страницах, роботов, «пауков» или другие автоматические устройства, программы, алгоритмы или методы, а также любые похожие или эквивалентные ручные процессы для доступа, приобретения, копирования или отслеживания любой части Системы и его содержимого, пытаться обойти технические ограничения в Системе, осуществлять любые действия, направленные на восстановление, изучение, копирование исходного кода (исходного текста) Платформы, вскрывать технологию, разбирать или каким-либо другим способом пытаться извлечь исходный код Системы, копировать графический интерфейс Системы, проводить испытание, проводить тестирование производительности, тестирование на проникновение, в том числе с помощью/участием третьих лиц, использовать Платформу каким- либо противозаконным способом, воспроизводить или обходить навигационную структуру или представление Платформы или ее содержимого для получения или попытки получения любых материалов, документов или информации любыми средствами, которые не были специально предоставлены Платформой, допускать несанкционированный доступ к Платформе путем взлома, «анализа» пароля или любыми другими незаконными средствами, совершать действия, представляющих угрозу информационной безопасности Платформы и/или предоставлять возможность для совершения указанных действий для третьих лиц, а также совершать действия подпадающие под действие Уголовного Кодекса РК и Кодекса РК об административных правонарушениях.
	4. В случае, если Пользователю станут известны факты совершения действий, предусмотренных пунктом 3.3. настоящего Договора, Пользователь обязан сообщить об этом Оператору и предоставить подтверждающие материалы (при необходимости).
	5. Оператор вправе:
		1. Модифицировать или выпускать новую версию Платформы в любое время, в том числе добавлять новые свойства и функциональные возможности в Платформу или удалять из Платформы уже существующие свойства и функциональные возможности.
		2. Проводить технические, профилактические и аварийные работы в Платформе.
		3. В одностороннем порядке добавлять новые, изменять и отменять существующие условия использования, опубликованные на Сайте Оператора и в Платформе, изменять условия и тарифы вознаграждения.
		4. Вносить изменения и дополнения в условия Договора в одностороннем порядке, отменять и издавать в новой редакции путем публикации на Сайте Оператора и отправлять уведомление об этом в Личный кабинет.
		5. Рассмотреть в индивидуальном порядке поступивший запрос от Пользователя в соответствии Договором и при необходимости заключать отдельный договор.
		6. Оператор вправе блокировать доступ Пользователя к Платформе за нарушение Пользователем условий настоящего Договора.
		7. Оператор вправе в одностороннем порядке в любое время без объяснения причин и какого-либо уведомления блокировать доступ Пользователя к Платформе и/или расторгнуть Договор.
		8. Проводить акции, мероприятия, предоставлять бонусы, дисконты и совершать иные действия касательно пользования Системы.
	6. Оператор обязуется:
		1. Обеспечивать выполнение функций Платформы в режиме 24/7, круглосуточную доступность Системы за исключением времени проведения профилактических, технических и аварийных работ.
		2. Уведомлять Пользователя об изменениях и дополнениях, внесенных в настоящий Договор.
		3. Выплачивать вознаграждение Пользователю в соответствии с условиями каждой отдельной программы.
3. **Финансовые условия и порядок расчетов**
	1. Оператор выплачивает вознаграждение Пользователю в порядке, сроке и размере, предусмотренном Договором, отдельным положением на странице программы Клиента Оператора.
	2. Вознаграждение выплачивается после прохождения этапа верификации и заполнения реквизитов для получения оплаты.
	3. Вознаграждение Пользователю может выплачиваться с помощью третьей стороны. При расчете с Пользователем третьей стороной обязательств Оператора по выплате вознаграждения считаются выполненными.
	4. Вознаграждение, выплачиваемое Пользователю в рамках настоящего Договора, оплачивается за вычетом суммы налогов, сборов, отчислений и других обязательных платежей, установленных действующим законодательством Республики Казахстан.
	5. Организатор выплачивает вознаграждение Пользователю денежных средств на основании указанных банковских реквизитов Пользователем на Платформе, соответственно Оператор не несет ответственность за корректность и правильность указанных Пользователем реквизитов. Организатор считается выполнившим свои обязанности по выплате вознаграждения за подтвержденные уязвимости в полном объеме в случае отсутствия у Пользователя претензий и уведомлении в течение 14 (четырнадцать) календарных дней с даты выплаты Организатором вознаграждения Пользователю.
4. **Ответственность сторон.**
	1. Пользователь несет ответственность за:
		1. нарушение, невыполнение или ненадлежащее выполнение обязательств по Договору, в том числе за нарушение Регламента и требований, опубликованных на Сайте Оператора и в Платформе.
		2. за все действия, совершенные в Платформе под логином Пользователя.
		3. недостоверность информации предоставленных Пользователю при регистрации в Системе.
		4. за распространение, использование уязвимостей по своему усмотрению.
		5. не прочтение уведомлений, направленных в Личный кабинет и/или на электронную почту, указанную при регистрации в Пользователя.
		6. нарушение авторских и интеллектуальных прав Оператора.
		7. нарушение условий Договора, а также авторских и интеллектуальных прав Оператора Пользователь обязан выплатить Оператору вне судебного порядка твердую денежную сумму, равной стоимости за причиненный реальный ущерб Оператору. Стоимость реального ущерба, причиненного Оператору вследствие нарушения Договора, а также авторских и интеллектуальных прав Оператора оценивается Оператором. Оператор вправе требовать исполнение настоящего пункта в судебном порядке в соответствии с условиями настоящего Договора.
		8. распространение ложной информации об Операторе и Платформе, совершение обманных, мошеннических и иных неправомерных действий, подпадающих под действие Уголовного Кодекса РК и Кодекса РК об административных правонарушениях.
		9. совершение обманных, неправомерных или неэтичных действий, которые могут нанести/нанесли имущественный или репутационный вред Оператору, Платформе.
		10. Нарушение Партнерской программы в соответствии с условиями Соглашения о партнерстве и действующим законодательством Республики Казахстан.
	2. Оператор ни при каких обстоятельствах не несет ответственность за:
		1. недоступность Платформы по причинам независящим от Оператора, в случае если недоступность Платформы зависит от услуг третьих лиц, оказываемых Оператору, в том числе включая, но не ограничиваясь: услуги по колокейшну, хостинга, Rent a Rack, предоставление VPN каналов, в случае неисправности каналов связи или дата-центров, действия/бездействия третьих лиц, обеспечивающих предоставление канала связи, интернета, электрической энергии, а также информационных систем участников, владельцев систем оплаты, и в иных обстоятельствах, находящихся вне контроля Оператора и оказывающие влияние на предоставление Платформы по Договору.
		2. несвоевременное прочтение Пользователем уведомлений, направленных в Личный кабинет и на электронную почту, указанную им при регистрации в Платформе.
		3. невозможность использования Пользователем Платформы по причине несоблюдения Пользователем положений Договора, Регламента, отсутствия у Пользователя подключения к Интернету, функционирования Платформы на неисправном компьютере и другим причинам, не зависящим от Оператора.
		4. потерю данных Пользователя, хранящихся в Системе, в случае наступления обстоятельств непреодолимой силы (форс-мажор), определенных в соответствии с законодательством Республики Казахстан и в Договоре.
		5. любой ущерб, любую потерю доходов, прибыли, информации или сбережений, за прямые или косвенные убытки, включая упущенную выгоду Пользователя, связанных с использованием или с невозможностью использования Платформы, в том числе в случае предварительного уведомления со стороны Пользователя о возможности такого ущерба, или по любому иску третьей стороны.
		6. ненадлежащее исполнение условий Договора, за любой ущерб, любую потерю доходов, прибыли, информации или сбережений, за прямые или косвенные убытки, включая упущенную выгоду Пользователя, связанных с использованием или с невозможностью использования Системы, в том числе в случае предварительного уведомления со стороны Пользователя о возможности такого ущерба, или по любому иску третьей стороны в случае бесплатного использования Пользователем Платформы, и Пользователь не вправе предъявлять Оператору какие-либо штрафные санкции (пени, неустойки), исковые требования, претензии и т.п.
		7. Потерю или невозможность получения налоговых вычетов или льгот со стороны Пользователя, связанных с услугами, предоставляемыми Оператором.

5.4. Совокупный размер ответственности Оператора по Договору, включая размер штрафных санкций (пеней, неустоек) и/или возмещаемых убытков, по любому иску или претензии в отношении Оператора/ Договора или его исполнения, ограничивается 100 МРП и на дату в котором был предъявлен иск.

* 1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы, определенных в соответствии с законодательством Республики Казахстан и в Договоре.
	2. Пользователь возмещает Оператору и освобождает его от ответственности за все и любые претензии, убытки, ущерб, затраты, судебные иски, долги, требования, сборы, судебные разбирательства, причины таких разбирательств, обременения, привилегии, удержания и расходы, включая гонорар за оказание юридических услуг, связанные с ущербом или разрушением собственности, как движимой и личной, так и иначе, находящейся в бенефициарном или абсолютном владении Оператора/третьих лиц, или находящейся под его/их ответственностью, в результате любого действия или бездействия Пользователя, независимо от того, причинен ли ущерб или убыток полностью или частично любым действием, бездействием, виной, халатностью или недостатком должного прилежания со стороны Пользователя, как по общему праву, так и по закону.
	3. Пользователь настоящим освобождает Оператора от любой ответственности перед третьими лицами, в том числе за все и любые претензии, убытки, ущерб, затраты, судебные иски, долги, требования, сборы, судебные разбирательства, причины таких разбирательств, обременения, привилегии, удержания и расходы, включая гонорар за оказание юридических услуг, а также связанные с: (а) нанесением увечий, включая смерть; (б) убытком, понесенным третьей стороной, включая повреждение собственности, возникшее в связи или связанным частично или полностью с Договором.
1. **Согласие на сбор, обработку и хранение персональных данных, конфиденциальность**
	1. Условия сбора, обработки и хранения персональных данных предусмотрены приложением №2 к Договору.
	2. К конфиденциальной информации относится: коммерческая тайна, информация (сведения) о лицах, предметах, фактах, событиях и / или процессах, независимо от формы их предоставления, прямо или косвенно связанные с Оператора, ее аффилированными лицами и / или клиентами, а именно, в том числе: о подписании Оператором Договоров и их исполнении, сведения о сотрудничестве и проектах Оператора, сведения о реализации конкретных проектов, сведения относительно деятельности Оператора, любые сведения об использованных или разработанных Оператором методах, технологиях, идеях, концепциях, инструментах, компонентах, технологиях, рецептах, программ ЭВМ, сведения об организационных аспектах Оператора, сведения о правилах учета как бухгалтерского, так и управленческого, положения учетной политики Оператора, используемые ею планы счетов, процедуры ввода и хранения учетной информации, сведения об информационных системах, программных продуктах Оператора и обслуживающего персонала, а также, любая информация, ставшая известной в связи с оказанием Услуг.
	3. К коммерческой тайне относится:
		1. о себестоимости продукции, рентабельности;
		2. об имуществе Оператора, его составе, стоимости;
		3. договоры (хозяйственные, гражданско-правовые и иные договоры с клиентами и с третьими лицами) и об условиях всех заключаемых договоров;
		4. о структуре производства и технологических процессах;
		5. об организации охраны Оператора, связи и сигнализации;
		6. о внутренних документах Оператора (все внутренние положения организации);
		7. личные и служебные переписки с клиентами и с третьими лицами;
		8. учредительные документы Оператора и клиентов, а также третьих лиц;
		9. личная, контактная информация, телефоны и сведения клиентов и партнеров Заказчика.
	4. Пользователь обязуется не разглашать конфиденциальную информацию, сведения, составляющие коммерческую тайну, Оператора, которые будут доверены Пользователю или станут известны в результате оказания Услуг.
	5. Пользователь обязуется не передавать третьим лицам и не раскрывать публично сведения, составляющие коммерческую тайну Оператора, без его письменного согласия.
	6. Пользователь обязуется выполнять требования инструкции и положений Заказчика по обеспечению сохранности коммерческой тайны.
	7. Пользователь обязуется в случае попытки посторонних лиц получить от меня сведения коммерческой тайны/конфиденциальной информации немедленно сообщить Заказчику.
	8. Пользователь обязуется сохранять коммерческую тайну/конфиденциальную информацию и личные сведения клиентов и/или партнеров Оператора.
	9. Пользователь обязуется не использовать/передавать/разглашать/копировать конфиденциальную информацию в любых целях, независимо от текущих отношений с Заказчиком.
2. **Дополнительные положения**
	1. Платформа предоставляется на условиях «as is» (как есть). Оператор не гарантирует соответствие Платформы или ее компонентов целям и ожиданиям Пользователя.
	2. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение условий настоящего Договора в случае наступления обстоятельств непреодолимой силы (форс-мажор), определяемых в соответствии с действующим законодательством РК, если они предъявляют доказательства того, что эти обстоятельства воспрепятствовали исполнению обязательств по настоящему Договору. К непреодолимой силе относятся стихийные бедствия (землетрясения, наводнения, сели, иные природные катаклизмы и катастрофы), пожары, в том числе серверного оборудования, на котором расположена Система и все данные, хранящиеся в Системе, обстоятельства, которые невозможно предусмотреть или предотвратить (либо возможно предусмотреть, но невозможно предотвратить), а также издание государственными органами Республики Казахстан актов, запрещающих и/или препятствующих Сторонам исполнению своих обязательств по настоящему Договору, иные решения высших государственных органов Республики Казахстан (запрет импорта или экспорта, валютные ограничения и др.), блокады, войны, военные конфликты, забастовки, революции, услуги третьих лиц оказываемых Оператору, в том числе по колокейшну, неисправности каналов связи или дата- центров, действие/бездействие третьих лиц, обеспечивающих предоставление канала связи, интернета, электрической энергии, а также обслуживающих участников информационных систем, собственников владельцев электронно-цифровой подписи, систем оплаты, обстоятельства, находящиеся вне контроля Оператора и оказывающие влияние на выполнение обязательств Сторонами по Договору и т.п. Сроки выполнения обязательств по Договору соразмерно сдвигаются на время действия форс-мажорных обстоятельств, если они значительно влияют на сроки оказания услуг по Договору или той его части, которая подлежит выполнению после наступления обстоятельств форс-мажора. С момента устранения обстоятельств непреодолимой силы настоящий Договор действует в обычном порядке. В случае наступления обстоятельств непреодолимой силы: а) Пользователь направляет Оператору уведомление в течение 5 календарных дней; б) Оператор сообщает об этом на своем официальном Сайте; в) Оператор сообщает об этом в личном кабинете Платформы.
	3. Стороны договорились и согласились, что все судебные споры будут рассмотрены в Суде по месту нахождения Оператора.
	4. Договор действует на всей территории Республики Казахстан и иного государства Пользователя (если Пользователь является гражданином другого государства).
	5. Договор вступает в силу с момента Акцепта Пользователем Оферты и действует бессрочно. Регистрация на Платформе в порядке, предусмотренном настоящим Договором, означает полное и безоговорочное согласие Участника со всеми условиями Программы, Договора и Приложениями.
	6. Настоящий Договор опубликован на Сайте Оператора.
	7. В случае признания любой части и условий настоящего Договора недействительной или не имеющей законной силы, остальные положения сохраняют свою юридическую силу и останутся в силе в полном объеме.

**Приложение № 1 к Договору публичной оферты об оказании услуг по предоставлению доступа к веб-ресурсу, расположенному в сети Интернет по адресу:** [**https://tumar.one/**](https://tumar.one/)

**РЕГЛАМЕНТ**

**работы на Платформе**

**Начало работы с TumarOne:**

1. Пользователь должен зарегистрироваться в системе для того, чтобы начать пользоваться BugBounty платформой TumarOne,. При регистрации, необходимо создать аккаунт в качестве исследователя.
2. Необходимо пройти через процесс onboarding-а, где система собирает данные о вашем опыте в качестве исследователя, интересы и время, которое Пользователь готов посвятить исследованиям информационных систем TumarOne.
3. После успешной регистрации Пользователя ожидает инструкция пользования платформой, которая поможет Пользователю заполнить личные и контактные данные, а также покажет, как отправлять отчеты, следить за вознаграждениями и получать выплаты в случае успешно подтвержденных отчетов.
4. Прежде чем отправлять отчеты по уязвимостям, Пользователь должен внимательно ознакомиться с правилами пользования платформы в разделе “Правила”.

**Политика раскрытия информации об уязвимостях:**

Программа ограничена поиском технических уязвимостей в сервисах компании. Уязвимости — недостатки в системе, использование которых может намеренно нарушить её целостность, конфиденциальность или вызвать неправильную работу.

• Не раскрывать и не распространять информацию о найденной уязвимости общественности или третьим лицам до ее исправления.

• Если Пользователь будет следовать установленным правилам Bug Bounty, Оператор не будет преследовать или предпринимать какие-либо юридические действия, связанные с исследованием.

• Взаимодействовать только с собственными аккаунтами или с явного разрешения владельца аккаунта.

**Приватные и Публичные программы:**

Приватные программы – это программы, не предназначенные для общего доступа. Это подразумевает, что Пользователь можете искать уязвимости в таких программах только после получения специального приглашения на их взлом. Все отчеты о выявленных уязвимостях в этих программах остаются конфиденциальными, и Пользователь не имеет права публично обсуждать обнаруженные уязвимости.

Все программы начинают свой путь как частные, но по мере того, как они становятся более опытными в обработке отчетов, при желании, они могут перейти в открытый доступ для широкой аудитории.

Публичные программы – это программы, являющиеся доступными для всех исследователей платформы. Это означает, что все исследователи на платформе, работа с публичными программами – отличный способ научиться определять уязвимости и повысить свою репутацию на платформе.

**Личный кабинет:**

1. После успешной регистрации, требуется включить функцию двухфакторной авторизации для защиты аккаунта и отчетов по найденным уязвимостям. Для подключения двухфакторной аутентификации Пользователь может перейти в личный кабинет и активировать его после установки приложения (подробная инструкция появляется при подключении двухфакторной аутентификации).
2. Затем, Пользователь может заполнить аккаунт личными данными, в том числе: контактная информация, социальные сети и платежная информация для успешной реализации выплат.

**Отправка отчетов по уязвимостям:**

1. Для того, чтобы отправить отчет по программам от TumarOne, Пользователю нужно перейти во вкладку “Мои отчеты” и нажать на кнопку “Добавить отчет”.
2. Далее, Пользователь может выбрать программу из списка доступных программ и нажать на кнопку “Отправить уязвимость”. Прежде чем отправлять какую-либо уязвимость, требуется ознакомиться с описанием программы, которая включает список доступных для проверки доменов, допустимые уязвимости и выставление баллов по уровням критичности уязвимостей.
3. Виды уязвимостей, которые не оплачиваются (уязвимости низкого уровня, которые не имеют критических последствий в случае их эксплуатации, в том числе):
* IDOR (отчеты по данному типу уязвимости принимаются только в случае высокого уровня критичности; уровень критичности определяется нашим специалистом при подтверждении наличия уязвимости);
* Любые виды уязвимости XSS, помимо Stored XSS (отчеты по уязвимости Stored XSS принимаются в зависимости от значимости веб-ресурса);
* Clickjacking;
* Insecure Redirect URI;
* Directory Listing Enabled (в зависимости от раскрывающихся данных; отчеты по этой уязвимости принимаются, в случае обнаружения критичных данных (пароли, бекапы, и т.д);
* Sensitive data exposure (в зависимости от раскрывающихся данных; отчеты по этой уязвимости принимаются, в случае обнаружения критичных данных);
* Включенный debug mode, в котором не раскрываются критические данные;
* CSRF уязвимости, найденные в функционале, который не является критичным;
* Раскрытие панели админа (Если багхантер находит панель админа, однако не способен произвести захват аккаунта или получать иную критическую информацию);
* User Enumeration без раскрытия критичных данных;
* Security Misconfiguration, в случае отсутствия доказательств реализации угрозы;
* Отказ в обслуживании;
* Спам;
* Социальная инженерия, направленная против сотрудников, подрядчиков или клиентов;
* Любые физические попытки по получению доступа к собственности или центрам обработки данных
* Владельца системы;
* Отчет с помощью автоматизированных инструментов и сканирований;
* Ошибки в стороннем программном обеспечении;
* Отсутствие заголовков безопасности, которые не ведут напрямую к уязвимости;
* Нарушение доверия SSL / TLS;
* Уязвимости, влияющие только на пользователей устаревших или непатентованных браузеров и платформ;
* Политики восстановления пароля и учетной записи, такие как срок действия ссылки для сброса или сложность пароля;
* Устаревшая запись DNS, указывающая на систему, которая не принадлежит владельцу системы.
1. При отправке отчета, требуется убедиться в наличии всех дополнительных подтверждающих файлов. Благодаря ним, команда модераторов может полностью убедиться в корректности отчета, что благополучно скажется на вероятности награждения за отправленную уязвимость.
2. После успешной отправке отчета, отчет переходит на статус “на рассмотрении. В следующем разделе Пользователь может ознакомиться со статусами отчетов на платформе TumarOne.
3. У исследователей есть возможность отозвать отчет в разделе "Мои отчеты" если при отправке отчета были введены некорректные данные или уязвимость не является актуальной. Данная функция доступна только когда статус отчета стоит "на рассмотрении", то есть, когда отчет еще не был проверен командой аналитиков безопасности.

**Статусы отчетов:**

1. Процесс с поступления отчетов до выплаты вознаграждения является не скорым и обработка запросов осуществляется до 3-х месяцев. Так как Оперататор отправляет отчеты владельцам систем еженедельно, некоторые владельцы систем (в публичных программах) могут не принимать отправленные уязвимости или же обработка уязвимостей может занимать долгое время. Команды платформы старается ускорить процесс обработки уязвимостей, и при успешном принятии отчета, Оператор незамедлительно выставляем вознаграждения при их наличии.
2. Составленные Пользователем отчеты поступают в систему сбора bugbounty, после чего им присваивается статус «**на рассмотрении**».
3. Следующим этапом отчеты проходят предварительный анализ и назначаются определенному аналитику безопасности. После чего отчету присваивается статус «**отсортирован**». Это означает, что отчет был проверен аналитиком безопасности, но еще не отправлен владельцем системы.
4. Аналитик безопасности в свою очередь проводит полный мониторинг и присваивает отчету один из следующих статусов:
	1. «**Отклонен модератором**»: В случае если аналитик безопасности не обнаружит в вашем отчете уязвимость, отчет будет отклонен;
	2. «**Нужно больше информации**»: В случае недостаточности информации для подтверждения уязвимости, аналитик безопасности отправляет Пользователю отчет на доработку и процесс обработки отчета осуществляется заново;
	3. «**Дубликат**»: Если в отчете указаны уязвимости, которые ранее были обнаружены другим пользователем, отчет будет считаться дублированным. В таком случае очки и вознаграждение не начисляются;
5. **«Отправлено владельцу»**: Аналитик безопасности подтверждает наличие уязвимости и отправляет специалисту по работе с организациями. Специалист подготавливает официальное письмо с приложением справки об уязвимостях (отчета) и направляет в соответствующие организации, на информационных системах которых были обнаружены уязвимости.
6. Отчеты, отправленные на подтверждение владельцам информационных систем (сайтов) могут быть **приняты** или **отклонены** мотивированным отказом. В случае отклонения, Пользователю будут предоставлены ответы, полученные от владельцев сайтов. В случае принятия отчета, Пользователю может быть выделено награждение (по правилам награждения отчетов ознакомьтесь с разделом “Выплаты”).
7. Если владелец не ответит на отчет по уязвимости в течении 30 дней после ее отправки, отчет уходит в статус “**Нет ответа от владельца**” и Пользователю будут начислены соответствующие баллы без выплаты вознаграждения.
8. **«Информативный»**: Данный статус означает, что уязвимости, указанные в вашем отчете, являются лишь не критичной ошибкой и Пользователю могут начисляться только соответствующие баллы без выплаты вознаграждения.
9. За принятые отчеты владельцы информационных систем могут назначить определенную сумму вознаграждения. В случае, произведения выплаты вознаграждения, отчету присваивается конечный статус **«Оплачен»**. Статус **«Оплачен»** отображается в разделе **«Выплаты»** в личном кабинете исследователя, где Пользователь может проследить свои вознаграждения за подтвержденные уязвимости (по правилам награждения отчетов подробнее в разделе “Выплаты”).
10. Если владелец системы принимает, однако не назначает вознаграждение или по прошествии 2-х месяцев, ответ от владельца информационных систем не будет получен, отчету присваивается статус **«Принят»**, Пользователю начисляются соответствующие очки и отчет будет закрыт.
11. Приватные программы могут запросить повторную проверку на успешность устранения уязвимости, в таком случае, отчету присваивается статус **«Повторная проверка».** В личный кабинет исследователя приходит заявка на повторное тестирование, которое Пользователь может принять, в случае чего ему/ей начисляются дополнительные очки.
12. После прохождения повторной проверки Пользователь может указать в ответе была ли успешно исправлена уязвимость, присвоив статусы **«Исправлено»** и **«Не исправлено».** Статус меняется на **«Исправлено»** если Пользователь подтверждает исправность уязвимости, и на **«Не исправлено»** в обратном случае. На принятие повторного тестирования со стороны Пользователя есть ровно 2 недели с появление заявки, после истечения срока заявка на повторное тестирование будет автоматически отклонена.
13. После прохождения повторного тестирования, отчету присваивается статус **«Принят»** и далее процесс отчета проходит пункты 6, 9 и 10.

**Верификация пользователей:**

1. Для повышения уровня этичности сообщества исследователей существует процесс верификации аккаунта. Так как процесс вознаграждения не включает в себя подписание других договоров, Пользователи должны пройти процесс верификации.

2. Процесс верификации включает в себя предоставление электронной версии документа, удостоверяющего личность исследователя. Также, предоставление фотографии, где отчетливо видно ваше лицо с документом.

3. После успешной загрузки документов Оператор подтверждает личность пользователя.

4. При успешной верификации пользователя, исследователю будет доступна функция выплат в личном кабинете. Данный процесс значительно ускорит процесс награждения исследователей за найденные уязвимости, позволяя сократить количество подтверждающих договоров и прочих документов.

5. Важно отметить, что административная команда платформы не передает ваши данные третьим лицам.

6. Административная команда платформы/Оператор не несет ответственность за некорректно предоставленные данные исследователей.

**Выплаты за подтвержденные уязвимости:**

1. После того как отчету был присвоен статус **«Принят»** и была указана количественная выплата, отчет автоматически переходит в раздел “Выплаты”, где ему будет начислено вознаграждение. **Важное примечание**: для того, чтобы получить вознаграждение, Пользователю нужно пройти процесс верификации в личном кабинете. Подробнее в разделе "Верификация пользователей". Оператор свяжется с Пользователем лично для осуществления выплаты и подписания документов. Пользователи, в свою очередь, обязаны ознакомиться с публичной офертой и подписать АВР в качестве закрывающего документа.
2. Пользователь можете посмотреть вознаграждения по публичным и приватным программам, выбрав раздел “Публичные выплаты” или “Приватные выплаты”.
3. У каждой выплаты есть 5 статусов:
	1. Выплате присваивается статус "На рассмотрении" при выделении вознаграждения Пользователю и ожидания подтверждения данной выплаты Оператором (администратором платформы).
	2. Выплате присваивается статус “Требуется согласие” когда вознаграждение было подтверждено и вам нужно принять условия публичного договора путем нажатия на кнопку “Я согласен(-на) с условиями предоставления сервиса” в нижнем правом углу страницы.
	3. После согласия с условиями предоставления сервиса, Пользователю необходимо выбрать метод оплаты. Выплата осуществляется с помощью банковской карты. Далее, Пользователю нужно указать реквизиты и сохранить данные. Оператор не хранит и не передает данные Пользователя третьим лицам, система выплат является занимается лишь сбором реквизитов и отправкой вознаграждений.
	4. Далее, выплате присваивается статус “В обработке”, означающий что процесс выплаты проходит подтверждение со стороны команды сервиса обслуживающего банка.
	5. При успешной верификации личности, согласия с условиями предоставления сервиса, подтверждения метода оплаты и принятия вознаграждения, статус выплаты меняется на “Оплачено” или “Отклонено”.
	6. В случае статуса “Отклонено” статус, и причина ошибки отображается в личном кабинете, в разделе “Уведомления”. Далее, для того чтобы устранить ошибку, необходимо поменять реквизиты или метод оплаты в разделе “Платежная информация”, перейдя в “Личные данные”.
	7. Если статус “Отклонено” присваивается из-за ошибки на стороне сервиса, Оператор незамедлительно приступает к ее устранению и связывается с Пользователем. В любом случае, пользователь может обратиться в техническую поддержку по электронному адресу info@tumar.one.
4. При согласии с условиями, Пользователю следует внимательно ознакомиться с их содержанием и подробной инструкцией.
5. Исследователям предоставляется Публичный договор об оказании услуг по предоставлению доступа к веб-ресурсу. Данный договор является публичным, соответственно согласие и акцепт условий выражается через форму сайта (checkbox), путем его нажатия.

**Дополнительно:**

**Методические рекомендации:**

* При обнаружении уязвимости, требуется сообщить Оператору об этом как можно скорее, чтобы команда платформы могла приложить все усилия для быстрого решения этой проблемы
* Нужно уметь вовремя остановиться. К примеру при SQLi достаточно вывести version() или подобную информацию и остановиться, а не дампить (сбрасывать) всю базу пользователей.
* Нужно действовать разумно и с ответственностью, чтобы избежать нарушений конфиденциальности, уничтожения данных, а также прерывания или ухудшения работы сервисов.
* Не использовать инструменты автоматического сканирования, это однозначно не прибавит Пользователю очков при рассмотрении отчёта.

**Правила участия**

1. Не распространять информацию о найденной уязвимости до ее исправления.

2. Приложить все усилия, чтобы не причинить ущерб нашим пользователям и услугам (действовать добросовестно).

3. Обязательно использовать свои собственные учетные записи, номера телефонов и т. д. для проведения исследования. Не пытаться получить доступ к чужим учетным записям или любой конфиденциальной информации. Если для поиска уязвимостей нужен доступ к аккаунту, Пользователь обязуется использовать свой личный аккаунт.

4. Если в ходе исследования участником был случайно получен доступ к личным данным, Оператор настоятельно просит удалить со своих носителей всю связанную с ними информацию, включая коды подключения, личные данные и т.д., после того, как оповестили команду платформы об этом.

5. Прилагать все необходимые усилия, чтобы избежать случаев нарушения конфиденциальности и работы других пользователей, в том числе несанкционированного доступа к данным, уничтожения данных, прерывания или ухудшения работы сервисов и т. д.

6. Оператор посчитает недопустимым и вознаграждение не будет выплачено, если обнаружится, что в ходе тестирования и поиска уязвимости Пользователем:

* Было совершено физическое вмешательство в дата-центры или офисы.
* Применялись методы социальной инженерии, направленной на сотрудников компании.
* Произошел взлом инфраструктуры компании и использование полученной информации для сообщения об уязвимостях.
* Совершены попытки получить доступ к учетной записи или данным других пользователей.

7. Для инструментов автоматического сканирования должно быть выставлено ограничение в виде не более чем 5 запросов в секунду (300 запросов в минуту) на один целевой хост и не должно превышать лимит в 3 параллельных запроса одновременно (5 потоков).

8. Агрессивные приемы проверки безопасности запрещены. Следует помнить, что Пользователь тестирует производственную среду, которая функционирует, поддерживается и контролируется. Чтобы предотвратить негативные последствия, требуется проводить исследования ответственно и разумно контролировать влияние своих тестов на пользователей, модераторов и администраторов системы.

Агрессивные способы проверки безопасности и тесты могут привести к срабатыванию защитных механизмов и формированию инцидента ИБ, что, в свою очередь, приведет к другим принудительным мерам, таким как блокировка учетной записи, номера телефона или IP- адреса.

**Виды уязвимостей по уровням критичности для публичных программ:**

**Баллы по уровням критичности уязвимостей присуждаются следующим образом:**

1) За низкий уровень критичности - от 0 до 30 баллов;

2) За средний уровень критичности - от 31 до 60 баллов;

3) За высокий уровень критичности - от 61 до 100 баллов.

Path Traversal -- 40-70 средне/высокая
Directory Listing Enabled -- 10-40 низкая/средняя

Insecure Redirect URI -- 5-10
Clickjacking -- 5
Brute Force -- 5
SQL Injection -- 50 - пустая база, 70 - полезная база

XML External Entity Injection -- 50-70
Local File Inclusion -- 50
Remote Code Execution -- 50-100
Authentication Bypass -- 50-90
Account Takeover -- 50-90
Insecure Direct Object References -- 10-90
Stored XSS -- 20-30
Reflected XSS -- 10-20
Server-Side Request Forgery -- 40-60
Cross-Site Request Forgery -- 10-20
Race Condition -- 10-90
Server-Side Template Injection -- 20-80

**1. Высокий уровень критичности:**

Path Traversal (Directory Traversal)

SQL Injection

Remote Code Execution (RCE)

Local File Inclusion

Remote File Inclusion

Authentication Bypass

Account Takeover

Insecure Direct Object References (IDOR) XML External Entity Injection (XXE)

**2. Средний уровень критичности:**

Directory Listing Enabled

Insecure Direct Object References (IDOR) Server-Side Request Forgery

Race Condition

Sensitive Data Exposure

Server-Side Template Injection

Stored XSS

XML External Entity Injection (XXE)

**3. Низкий уровень критичности:**

Cross-site Request Forgery Sensitive Data Exposure Insecure Redirect URI Clickjacking

Brute Force

Reflected XSS

SMS flood

Open Redirect URI

Нужно учитывать, что уровень критичности зависит от того, к чему может привести выявленная уязвимость. Следовательно, аналитики безопасности индивидуально оценивают каждый отчет о выявленных уязвимостях. Также, следует помнить, что оценки уязвимостей отличаются у разных программ, поэтому прежде, чем отправлять отчет, Пользователь должен ознакомиться с описанием программы и следовать их правилам.

**Приложение № 2 к Договору публичной оферты об оказании услуг по предоставлению доступа к веб-ресурсу, расположенному в сети Интернет по адресу:** [**https://tumar.one/**](https://tumar.one/)

* + - 1. **СБОР И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Оператор собирает и хранит только те Персональные данные, которые необходимы для оказания Услуг Оператором и взаимодействия с Пользователем.
	2. Персональные данные могут использоваться в следующих целях:
		1. оказание Услуг Пользователю;
		2. идентификация Пользователя;
		3. взаимодействие с Пользователем;
		4. направление Пользователю рекламных материалов, информации и запросов;
		5. проведение статистических и иных исследований;
		6. верификация пользователей.
	3. Оператор в том числе обрабатывает следующие данные:
		1. фамилия, имя и отчество
		2. адрес электронной почты;
		3. telegram аккаунт и/или номер телефона (в том числе мобильного);
		4. биометрические данные для верификации;
		5. банковские реквизиты;
		6. документы, удостоверяющие личность;
		7. иные личные данные (при необходимости);
	4. Пользователю запрещается указывать на Платформе персональные данные третьих лиц (за исключением условия представления интересов этих лиц, имея документальное подтверждение третьих лиц на осуществление таких действий).
1. **ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ И ИНЫХ ДАННЫХ**
	1. Оператор обязуется использовать Персональные данные в соответствии с Законом «О персональных данных» Республики Казахстан и внутренними документами Оператора.
	2. В отношении Персональных данных и иных Данных Пользователя сохраняется их конфиденциальность, кроме случаев, когда указанные данные являются общедоступными.
	3. Оператор имеет право сохранять архивную копию Персональных данных. Оператор имеет право хранить Персональные данные и Данные на серверах вне территории Республики Казахстан.
	4. Оператор имеет право передавать Персональные данные и Данные Пользователя без согласия Пользователя следующим лицам:
		1. государственным органам, в том числе органам дознания и следствия, и органам местного самоуправления по их мотивированному запросу;
		2. в иных случаях, прямо предусмотренных действующим законодательством Республики Казахстан.
	5. Оператор имеет право передавать Персональные данные и Данные третьим лицам, не указанным в п.2.4. настоящей Политики конфиденциальности, в следующих случаях:
		1. Пользователь выразил свое согласие на такие действия;
		2. передача необходима в рамках использования Пользователем Сайта или оказания Услуг Пользователю;
	6. Оператор осуществляет автоматизированную обработку Персональных данных и Данных.
2. **ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ**
	1. Оператор осуществляет надлежащую защиту Персональных и иных данных в соответствии с Законодательством и принимает необходимые и достаточные организационные и технические меры для защиты Персональных данных.
	2. Применяемые меры защиты в том числе позволяют защитить Персональные данные от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними третьих лиц.
3. **ИНЫЕ ПОЛОЖЕНИЯ**
	1. К настоящей Политике конфиденциальности и отношениям между Пользователем и Оператором, возникающим в связи с применением Политики конфиденциальности, подлежит применению право Республики Казахстан.
	2. Все возможные споры, вытекающие из настоящей Политики конфиденциальности, подлежат разрешению в соответствии с действующим законодательством по месту регистрации Оператора. Перед обращением в суд Пользователь должен соблюсти обязательный досудебный порядок и направить Оператору соответствующую претензию в письменном виде. Срок ответа на претензию составляет 30 (тридцать) рабочих дней.
	3. Если по тем или иным причинам одно или несколько положений Политики конфиденциальности будут признаны недействительными или не имеющими юридической силы, это не оказывает влияния на действительность или применимость остальных положений Политики конфиденциальности.
	4. Оператор имеет право в любой момент изменять Политику конфиденциальности (полностью или в части) в одностороннем порядке без предварительного согласования с Пользователем. Все изменения вступают в силу с момента ее размещения на Сайте.
	5. Пользователь обязуется самостоятельно следить за изменениями Политики конфиденциальности путем ознакомления с актуальной редакцией.
	6. Все предложения или вопросы по настоящей Политике конфиденциальности следует сообщать по электронной почте: info@tumar.one.