**PUBLIC OFFER №KHS/23/30**

**Astana city 13.11.2023**

KazHackStan LLP (BIN 120540005677), hereinafter referred to as the “Operator”, represented by Director O.Satiyev, acting on the basis of the Charter, expresses its intention to conclude an Agreement on the provision of services to provide access to a web resource located in the Internet at the address: <https://tumar.one/> (hereinafter referred to as the Agreement) and is an official offer to provide access to the TumarOne Platform.

**Terms and Definitions**

1. “Operator” is a legal entity that owns the Platform, and which, independently and at its own discretion, determines the procedure for using the Platform on the Internet, including the procedure for posting information on the Platform. All exclusive property rights to the Platform belong to the Operator.
2. “Platform” is a web resource located on the Internet at <https://tumar.one/>. Platform is a reward program for vulnerabilities found in information systems and resources.
3. Offer in the text of this Agreement – is an offer published on the Operator's Website: <https://tumar.one/offer> is the Operator's Offer to all researchers in accordance with paragraph 5 of Article 395 of the Civil Code of the Republic of Kazakhstan.
4. Acceptance – in accordance with Article 396 of the Civil Code of the Republic of Kazakhstan, the response of the potential User, to whom this Offer is addressed, on its full and unconditional acceptance and consent to the terms of this Agreement by performing the actions specified in section 1 of this Agreement. Acceptance of the Offer entails the conclusion of an Agreement between the Operator and the User. By performing actions on the Acceptance of this Offer, the User confirms his legal status and capacity, the absence of any restrictions, including those determined by the current legislation on the conclusion of this Agreement, as well as his legal right to enter into contractual relations with the Operator.
5. User (researcher) is a fully capable individual who has expressed acceptance of the Offer in accordance with clause 1.2. of the Agreement and registered on the Platform, who carry out work on the search for vulnerabilities in accordance with the terms of the Agreement, acting on their own behalf.
6. Registration is filling out the registration form by the User located on the Platform by specifying the necessary information.
7. Registration Form is a form located on the Platform, which the User must fill out in order to be able to use the website in full.
8. Personal Account is a personal section of the User in the Platform, protected by authorization parameters using a login and password, providing the functions of the Platform in accordance with the Regulations, available to the User after authorization on the Operator's Website.
9. Regulations is a document that defines the procedure for working in the Platform in accordance with Appendix No. 1 to this Agreement, which is an integral part thereof.
10. Verification is the process of confirming the identity of the Researcher in order to pay for confirmed vulnerabilities.
11. Program is an initiative to identify vulnerabilities in the Client's web services and applications, as well as to determine ways to implement unacceptable events, which is posted on the relevant page of the Platform.
	1. **General Provisions**
	2. The text of the Agreement is a public offer. Acceptance of the offer means registration on the Platform at the following address <https://tumar.one/offer> and continuation of its use.

By accepting this Public Offer Agreement, the User guarantees his legal status and capacity, as well as his legal right to enter into contractual relations with KazHackStan LLP. Before using the Platform, the User must carefully read the terms of its use contained in this Agreement. The start of using the Platform means the proper conclusion of this Agreement and the User's full consent to all its terms.

* 1. The User's acceptance upon conclusion of the Agreement is the expressed consent to its terms and a set of the following actions of the User during registration in the Operator's Platform:
		1. Entering the registration data according to the registration form.
		2. familiarization, agreement and acceptance of the terms of the Offer.
		3. performance by the User of the actions specified in this Agreement, indicating full and unconditional acceptance of all its terms, as well as by ticking the box “I agree with the terms of service” on the Operator's website during registration.
1. **Subject of the Agreement**
	1. The Operator provides the User with access to the Platform free of charge, which hosts the programs of the Operator's Clients, in which the User searches for vulnerabilities. In turn, the Operator pays a reward to the User for the vulnerabilities found in accordance with the Agreement and the provisions of each individual program.
	2. The User searches for vulnerabilities of programs placed on the Platform in the manner specified in the Agreement.
2. **Rights and Obligations of the Parties**
	1. The User has the right to:
		1. Use the Platform except for the time of preventive, technical and emergency maintenance.
		2. Make and send proposals to the Operator to improve the functionality of the Platform or in writing to the Operator's e-mail specified on the Operator's website.
		3. Send a request to the Operator's technical support service regarding the spread of data on vulnerabilities.
		4. Take part in promotions, events, receive bonuses.
		5. Receive remuneration from the Operator.
	2. The User undertakes:
		1. Comply with the terms of this Agreement.
		2. Use the Platform in accordance with its purpose, as well as in accordance with the provisions of the Agreement, the Regulations and other documents and information published on the Operator's Website and in the Platform.
		3. Use valid identity and contact details on the Platform.
		4. Monitor notifications on the Platform and email specified when registering on the Platform. The User has exactly 2 weeks from the appearance of the application to accept the retest, after the expiration of the deadline, the application for retesting will be automatically rejected.
		5. Impersonate another person on the Platform.
		6. Not to publish in the media, the Internet, social networks data, information about the Platform without the official written consent of the Operator.
		7. Not to allow deceptive, illegal or unethical actions that may cause property or reputational damage to the Operator.
		8. Observe and not violate the copyright and intellectual property rights of the Operator.
		9. Go through the verification process to receive payment for confirmed vulnerabilities.
		10. Submit an Act of work performed/services rendered to the Operator for signing.
		11. Register on the platform for signing the EDS (Act of Work Performed/Services Rendered) and sign the EDS (Act of Work Performed/Services Rendered) if the User is a citizen or resident of the Republic of Kazakhstan. The Platform is determined by the Operator independently.
		12. If the User is not a citizen and resident of the Republic of Kazakhstan, in this case, the User undertakes to provide the Operator with a scanned copy of the Act of Work Performed/Services Rendered in accordance with the form established and provided by the Operator. This scanned copy must be provided before the exchange of originals between the parties.
	3. The User is prohibited from: using any means of “deep linking”, collecting information on pages, robots, “spiders” or other automatic devices, programs, algorithms or methods, as well as any similar or equivalent manual processes to access, acquire, copy or track any part of the System and its contents, attempt to circumvent technical limitations in the System, perform any actions aimed at restoring, studying, copying of the source code (source code) of the Platform, reverse engineer, disassemble or in any other way attempt to extract the source code of the System, copy the graphical interface of the System, conduct testing, conduct performance testing, penetration testing, including with the help/participation of third parties, use the Platform in any illegal way, reproduce or circumvent the navigational structure or presentation of the Platform or its contents in order to obtaining or attempting to obtain any materials, documents or information by any means that have not been specifically provided by the Platform, allowing unauthorized access to the Platform by hacking, password “analysis” or any other illegal means, committing actions that pose a threat to the information security of the Platform and/or providing an opportunity for third parties to perform these actions, as well as committing actions falling under the Criminal Code of the Republic of Kazakhstan and the Code of the Republic of Kazakhstan on Administrative Offences.
	4. If the User becomes aware of the facts of performing the actions provided for in clause 3.3. of this Agreement, the User is obliged to inform the Operator thereof and provide supporting materials (if necessary).
	5. The Operator has the right to:
		1. Modify or release a new version of the Platform at any time, including adding new features and functionality to the Platform or removing existing features and functionality from the Platform.
		2. Carry out technical, preventive and emergency work on the Platform.
		3. Unilaterally add new, change and cancel existing terms of use published on the Operator's Website and in the Platform, change the terms and rates of remuneration.
		4. Make changes and additions to the terms and conditions of the Agreement unilaterally, cancel and publish a new edition by publishing on the Operator's Website and send a notification about this to the Personal Account.
		5. Consider on an individual basis the request received from the User in accordance with the Agreement and, if necessary, conclude a separate agreement.
		6. The Operator has the right to block the User's access to the Platform for violation of the terms of this Agreement by the User.
		7. The Operator has the right to unilaterally block the User's access to the Platform and/or terminate the Agreement at any time without explanation or any notice.
		8. Conduct promotions, events, provide bonuses, discounts and perform other actions related to the use of the System.
	6. The Operator undertakes:
		1. Ensure the performance of the Platform's functions 24/7, round-the-clock availability of the System, except for the time of preventive, technical and emergency maintenance.
		2. Notify the User of changes and additions made to this Agreement.
		3. Pay remuneration to the User in accordance with the terms of each individual program.
3. **Financial conditions and payment procedure**
	1. The Operator shall pay remuneration to the User in the manner, term and amount provided for in the Agreement, in a separate provision on the Operator's Client's program page.
	2. The fee is paid after passing the verification stage, filling in the details for receiving payment and signing by the parties of the Act of work performed/services rendered in the form provided by the Operator.
	3. Remuneration to the User may be paid with the help of a third party. When settling accounts with the User by a third party, the Operator's obligations to pay remuneration shall be deemed to have been fulfilled.
	4. The remuneration paid to the User under this Agreement shall be paid minus the amount of taxes, fees, deductions, and other mandatory payments established by the current legislation of the Republic of Kazakhstan.
	5. The Organizer pays remuneration to the User on the basis of the specified bank details by the User on the Platform, accordingly, the Operator is not responsible for the correctness and correctness of the details specified by the User. The Organizer shall be deemed to have fulfilled its obligations to pay the reward for the confirmed vulnerabilities in full if the User has no claims and is notified within 14 (fourteen) calendar days from the date of payment of the remuneration by the Organizer to the User.
4. **Liability of the Parties.**
	1. The User is responsible for:
		1. violation, non-fulfillment or improper fulfillment of obligations under the Agreement, including for violation of the Regulations and requirements published on the Operator's Website and in the Platform.
		2. for all actions performed on the Platform under the User's login.
		3. inaccuracy of the information provided to the User during registration in the System.
		4. for the distribution and use of vulnerabilities at their own discretion.
		5. failure to read the notifications sent to the Personal Account and/or to the e-mail specified during registration with the User.
		6. violation of the Operator's copyright and intellectual property rights.
		7. violation of the terms of the Agreement, as well as the copyright and intellectual rights of the Operator, the User is obliged to pay the Operator a fixed amount of money equal to the value for the actual damage caused to the Operator out of court. The cost of the actual damage caused to the Operator as a result of the violation of the Agreement, as well as the copyright and intellectual property rights of the Operator, shall be assessed by the Operator. The Operator has the right to demand the execution of this clause in court in accordance with the terms of this Agreement.
		8. dissemination of false information about the Operator and the Platform, committing deceptive, fraudulent, and other illegal actions falling under the Criminal Code of the Republic of Kazakhstan and the Code of Administrative Offenses of the Republic of Kazakhstan.
		9. committing deceptive, illegal, or unethical actions that may cause/have caused property or reputational damage to the Operator, the Platform.
		10. Violation of the Affiliate Program in accordance with the terms of the Partnership Agreement and the current legislation of the Republic of Kazakhstan.
	2. Under no circumstances shall the Operator be responsible for:
		1. unavailability of the Platform for reasons beyond the control of the Operator, if the unavailability of the Platform depends on the services of third parties provided to the Operator, including, but not limited to: colocation services, hosting, Rent a Rack, provision of VPN channels, in case of malfunction of communication channels or data centers, actions/omissions of third parties ensuring the provision of a communication channel, Internet, electricity, as well as information systems of participants, owners of payment systems, and in other circumstances beyond the control of the Operator and affecting the provision of the Platform under the Agreement.
		2. untimely reading by the User of the notifications sent to the Personal Account and to the e-mail specified by him during registration in the Platform.
		3. inability of the User to use the Platform due to the User's non-compliance with the provisions of the Agreement, the Regulations, the User's lack of Internet connection, the functioning of the Platform on a faulty computer and other reasons beyond the control of the Operator.
		4. loss of the User's data stored in the System in the event of force majeure (force majeure) determined in accordance with the legislation of the Republic of Kazakhstan and in the Agreement.
		5. any damage, any loss of income, profit, information or savings, for direct or indirect losses, including lost profits of the User, related to the use or inability to use the Platform, including in the event of prior notification by the User of the possibility of such damage, or for any claim of a third party.
		6. improper fulfillment of the terms of the Agreement, for any damage, any loss of income, profit, information or savings, for direct or indirect losses, including lost profits of the User, related to the use or inability to use the System, including in the event of prior notification by the User of the possibility of such damage, or under any claim of a third party in the case of free use of the Platform by the User, and the User is not entitled to impose any penalties (penalties, penalties), lawsuits, claims, etc. against the Operator.
		7. Loss or inability to receive tax deductions or benefits from the User related to the services provided by the Operator.

5.4. The aggregate amount of the Operator's liability under the Agreement, including the amount of penalties (penalties, penalties) and/or reimbursable damages, for any claim or claim against the Operator/Contract or its performance, is limited 100 MCI and on the date on which the claim was brought.

* 1. The Parties shall be exempt from liability for partial or complete non-fulfillment of obligations under this Agreement, if this failure was the result of force majeure circumstances determined in accordance with the legislation of the Republic of Kazakhstan and in the Agreement.
	2. The User shall indemnify and hold harmless the Operator from any and all claims, losses, damages, costs, lawsuits, debts, demands, fees, proceedings, causes of such proceedings, encumbrances, privileges, withholdings and expenses, including attorneys' fees, related to damage to or destruction of property, whether movable or personal, or otherwise, in the beneficial or absolute possession of the Operator/third parties, or under his/her responsibility, as a result of any act or omission of the User, whether or not the damage or loss is caused in whole or in part by any act, omission, fault, negligence or lack of due diligence on the part of the User, whether at common law or at law.
	3. The User hereby releases the Operator from any and all liability to third parties, including for any and all claims, losses, damages, costs, lawsuits, debts, demands, fees, proceedings, causes of such proceedings, encumbrances, privileges, withholdings and expenses, including attorneys' fees, as well as those related to: (a) personal injury, including death; (b) loss suffered by a third party, including property damage, arising out of or related in whole or in part to the Contract.
1. **Consent to the collection, processing and storage of personal data, confidentiality**
	1. The conditions for the collection, processing and storage of personal data are provided for in Appendix No. 2 to the Agreement.
	2. Confidential information includes: trade secrets, information (data) about persons, objects, facts, events and/or processes, regardless of the form of their provision, directly or indirectly related to the Operator, its affiliates and/or customers, namely, including: on the signing of Contracts by the Operator and their execution, information on cooperation and projects of the Operator, information on the implementation of specific projects, information regarding the Operator's activities, any information about the methods, technologies, ideas, concepts, tools, components, technologies, recipes, computer programs used or developed by the Operator, information about the organizational aspects of the Operator, information about the accounting rules of both accounting and management, the provisions of the Operator's accounting policy, the charts of accounts used by it, the procedures for entering and storing accounting information, information about information systems, software products of the Operator and service personnel, as well as any information that has become known in connection with the provision of the Services.
	3. Trade secret includes:
		1. on the cost of production, profitability;
		2. on the property of the Operator, its composition, value;
		3. contracts (commercial, civil and other contracts with clients and third parties) and on the terms and conditions of all concluded contracts;
		4. on the structure of production and technological processes;
		5. on the organization of the Operator's security, communication and signal system;
		6. internal documents of the Operator (all internal regulations of the organization);
		7. personal and business correspondence with clients and third parties;
		8. constituent documents of the Operator and clients, as well as third parties;
		9. personal, contact information, phone numbers and information of the Customer's clients and partners.
	4. The User undertakes not to disclose confidential information, information constituting a trade secret of the Operator, which will be entrusted to the User or become known as a result of the provision of the Services.
	5. The User undertakes not to transfer to third parties and not to publicly disclose information constituting a trade secret of the Operator without his written consent.
	6. The User undertakes to comply with the requirements of the Customer's instructions and regulations to ensure the safety of trade secrets.
	7. In the event of an attempt by unauthorized persons to obtain trade secret/confidential information from me, the User undertakes to immediately inform the Customer.
	8. The User undertakes to keep trade secrets/confidential information and personal data of the Operator's customers and/or partners.
	9. The User undertakes not to use/transfer/disclose/copy confidential information for any purpose, regardless of the current relationship with the Customer.
2. **Miscellaneous Provisions**
	1. The platform is provided on an “as is” basis. The Operator does not guarantee the compliance of the Platform or its components with the goals and expectations of the User.
	2. The Parties shall be exempt from liability for non-fulfillment or improper fulfillment of the terms of this Agreement in the event of force majeure circumstances determined in accordance with the current legislation of the Republic of Kazakhstan, if they provide evidence that these circumstances prevented the fulfillment of obligations under this Agreement. Force majeure includes natural disasters (earthquakes, floods, mudflows, other natural disasters and catastrophes), fires, including server equipment on which the System and all data stored in the System are located, circumstances that cannot be foreseen or prevented (or can be foreseen, but cannot be prevented), as well as the issuance by state bodies of the Republic of Kazakhstan of acts prohibiting and/or preventing the Parties from fulfilling their obligations. obligations under this Agreement, other decisions of the supreme state bodies of the Republic of Kazakhstan (prohibition of import or export, currency restrictions, etc.), blockades, wars, military conflicts, strikes, revolutions, services of third parties provided to the Operator, including colocation, malfunctions of communication channels or data centers, action/inaction of third parties providing the provision of a communication channel, the Internet, electricity, as well as service participants of information systems, owners of digital signature holders, payment systems, circumstances beyond the control of the Operator and affecting the fulfillment of obligations by the Parties under the Agreement, etc. The deadlines for the performance of obligations under the Agreement shall be proportionately shifted to the duration of force majeure if they significantly affect the terms of the provision of services under the Agreement or that part thereof that is subject to performance after the occurrence of force majeure circumstances. From the moment of elimination of force majeure circumstances, this Agreement shall operate in the usual manner. In the event of force majeure: a) the User shall send a notice to the Operator within 5 calendar days; b) the Operator informs about it on its official Website; c) The Operator informs about it in the personal account of the Platform.
	3. The Parties have agreed and agreed that all legal disputes will be considered in the Court at the location of the Operator.
	4. The Agreement is valid throughout the territory of the Republic of Kazakhstan and another state of the User (if the User is a citizen of another state).
	5. The Agreement comes into force from the moment of the User's Acceptance of the Offer and is valid indefinitely. Registration on the Platform in the manner provided for in this Agreement means the Participant's full and unconditional consent to all the terms of the Program, the Agreement and the Appendices.
	6. This Agreement is published on the Operator's Website.
	7. In the event that any part and terms of this Agreement are held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

**Appendix No. 1 to the Public Offer Agreement for the provision of services for the provision of access to the web resource located on the Internet at:** [**https://tumar.one/**](https://tumar.one/)

**REGULATIONS**

**for work on the Platform**

**Getting started with TumarOne:**

1. The user must register in the system in order to start using the TumarOne BugBounty platform. When registering, the user needs to create an account as a researcher.
2. It is necessary to go through the onboarding process, where the system collects data about user's experience as a researcher, interests and time that the User is willing to devote to research on TumarOne information systems.
3. After successful registration, the User will receive instructions for using the platform, which will help the User fill in personal and contact data, as well as show how to send reports, monitor rewards and receive payments in case of successfully confirmed reports.
4. Before sending vulnerability reports, the User should carefully read the terms of use of the platform in the "Rules" section.

**Vulnerability Disclosure Policy:**

The program is limited to searching for technical vulnerabilities in the company's services. Vulnerabilities are flaws in the system, the use of which can intentionally violate its integrity, confidentiality, or cause malfunctioning.

• Not to disclose or disseminate information about the vulnerability found to the public or to third parties until it is fixed.

• If the User follows the established Bug Bounty rules, the Operator will not pursue or take any legal action related to the research.

• Interact only with own accounts or with the explicit permission of the account owner.

**Private and Public Programs:**

Private software is software that is not intended to be shared. This implies that the User can search for vulnerabilities in such programs only after receiving a special invitation to hack them. All reports on identified vulnerabilities in these programs remain confidential, and the User has no right to publicly discuss the vulnerabilities detected.

All programs start their journey as private, but as they become more proficient in processing reports, they can become publicly available to a wide audience if desired.

Public programs are programs that are available to all researchers on the platform. This means that all researchers on the platform, working with public programs is a great way to learn how to identify vulnerabilities and increase the user's reputation on the platform.

**Personal account:**

1. After successful registration, the user needs to enable the two-factor authentication function to protect the account and report on vulnerabilities found. To enable two-factor authentication, the User can go to the personal account and activate it after installing the application (detailed instructions appear when connecting two-factor authentication).
2. Then, the User can fill in the account with personal data, including: contact information, social networks and payment information for the successful implementation of payouts.

**Vulnerability reporting:**

1. In order to send a report on programs from TumarOne, the User needs to go to the “My reports” tab and click on the “Add report” button.
2. Next, the User can select a program from the list of available programs and click on the “Submit vulnerability” button. Before submitting any vulnerability, the user needs to read the description of the program, which includes a list of domains available for scanning, acceptable vulnerabilities, and scoring by vulnerability severity levels.
3. Types of vulnerabilities that are not paid for (low-level vulnerabilities that do not have critical consequences if exploited, including):
* IDOR (reports on this type of vulnerability are accepted only if the severity level is high; the severity level is determined by our specialist when the vulnerability is confirmed);
* Any type of XSS vulnerability other than Stored XSS (reports on the Stored XSS vulnerability are accepted depending on the significance of the web resource);
* Clickjacking;
* Insecure Redirect URI;
* Directory Listing Enabled (depending on the data being disclosed; reports on this vulnerability are accepted if critical data (passwords, backups, etc.) are detected);
* Sensitive data exposure (depending on the data being disclosed; reports on this vulnerability are accepted if critical data is detected);
* Enabled debug mode, which does not disclose critical data;
* CSRF vulnerabilities found in functionality that is not critical;
* Disclosure of the admin panel (If the bug hunter finds the admin panel, but is not able to take over the account or receive other critical information);
* User Enumeration without disclosure of critical data;
* Security Misconfiguration, if there is no evidence that the threat has materialized;
* Denial of service;
* Spam;
* Social engineering directed against employees, contractors, or customers;
* Any physical attempts to gain access to property or data centers
* Owner of the system;
* Report with automated tools and scans;
* Errors in third-party software;
* No security headers that don't directly lead to the vulnerability;
* SSL/TLS Trust Breach;
* Vulnerabilities that affect only users of outdated or non-proprietary browsers and platforms;
* Password and account recovery policies, such as expiration of the reset link or password complexity;
* An outdated DNS record that points to a system that does not belong to the owner of the system.
1. When submitting a report, the user needs to make sure that they have all the additional supporting files. Thanks to them, the moderation team can fully verify the correctness of the report, which will have a positive impact on the probability of rewarding the submitted vulnerability.
2. After the report is successfully submitted, the report status moves to "under review". In the next section, the User can get acquainted with the status of reports on the TumarOne platform.
3. Researchers have the option to retract the report in the "My Reports" section if incorrect data was entered when submitting the report or the vulnerability is not up-to-date. This feature is available only when the status of the report is “under review”, that is, when the report has not yet been reviewed by the security analysis team.

**Report status:**

1. The process from receipt of reports to payment of remuneration is not quick and the processing of requests is carried out up to 3 months. Since the Operator sends reports to system owners on a weekly basis, some system owners (in public programs) may not accept the submitted vulnerabilities, or vulnerability processing may take a long time. The platform's teams try to speed up the process of processing vulnerabilities, and upon successful acceptance of the report, the Operator immediately issues rewards, if any.
2. The reports generated by the User are sent to the bugbounty collection system, after which they are assigned the status “**pending”**.
3. In the next step, the reports are pre-analyzed and assigned to a specific security analyst. After that, the report is assigned the "sorted" status**.** This means that the report has been reviewed by a security analyst but has not yet been submitted by the system owner.
4. The security analyst, in turn, conducts full monitoring and assigns one of the following statuses to the report:
	1. “**Rejected by moderator**”: If the security analyst does not find a vulnerability in the report, the report will be rejected;
	2. “**Need more information”**: If there is not enough information to confirm the vulnerability, the security analyst sends a report to the User for revision and the report processing process is carried out again;
	3. **“Duplicate”**: If the report contains vulnerabilities that were previously discovered by another user, the report will be considered duplicate. In this case, points and rewards are not awarded;
5. **“Sent to Owner”**: A security analyst confirms the existence of the vulnerability and sends it to the organization specialist. The specialist prepares an official letter with a vulnerability certificate (report) attached and sends it to the relevant organizations on whose information systems the vulnerabilities were detected.
6. Reports sent for confirmation to the owners of information systems (sites) may be **accepted** or **rejected** by a reasoned refusal. In case of rejection, the User will be provided with the answers received from the site owners. In case of acceptance of the report, the User may be allocated an award (for the rules for awarding reports, see the "Payments" section).
7. If the owner does not respond to the vulnerability report within 30 days after it is sent, the report goes to the “**No response from the owner”** status and the User will be awarded the corresponding points without paying a reward.
8. **“Informative”**: This status means that the vulnerabilities identified in the report are only a non-critical bug and the User can only be awarded the corresponding points without paying a reward.
9. For accepted reports, the owners of information systems can assign a certain amount of remuneration. In case of payment of remuneration, the report is assigned the final status “Paid”**.** “Paid” **status is displayed in** the “Payouts” section of the researcher's personal account, where the User can track their rewards for confirmed vulnerabilities (for more information on the rules for awarding reports, see the “Payouts” section).
10. If the owner of the system accepts, but does not assign a reward or after 2 months, no response will be received from the owner of the information systems, the report is assigned the **status “Accepted”,** the User is awarded the appropriate points and the report will be closed.
11. Private programs may request a re-check for the success of the vulnerability, in which case the report is assigned the **“Retest” status.** A request for retesting is sent to the researcher's personal account, which the User can accept, in which case he/she is awarded additional points.
12. After passing the re-check, the User can indicate in the response whether the vulnerability has been successfully patched by assigning the statuses **“Fixed”**  and **“Not fixed”.** The status changes  **to “Fixed” if the** User confirms that the vulnerability is serviceable, and to  **“Not fixed”**  if the User confirms that the vulnerability is in good working order, and the User has exactly 2 weeks from the appearance of the application, after the expiration of the period, the application for retesting will be automatically rejected.
13. After passing the retest, the report is assigned the status **“Accepted”** and then the report process goes through points 6, 9 and 10.

**User Verification:**

1. To increase the level of ethics of the research community, there is an account verification process. Since the reward process does not include the signing of other contracts, Users must go through a verification process.

2. The verification process includes the provision of an electronic version of the researcher's identity document. Also, providing a photo where the user's face with the document is clearly visible.

3. Upon successful uploading of the documents, the Operator confirms the identity of the user.

4. Upon successful verification of the user, the researcher will have access to the payout function in the personal account. This process will significantly speed up the process of rewarding researchers for vulnerabilities found, reducing the number of supporting contracts and other documents.

5. It is important to note that the platform's administrative team does not share your data with third parties.

6. The administrative team of the platform/Operator is not responsible for incorrectly provided data of researchers.

**Payouts for confirmed vulnerabilities:**

1. After the report has been assigned the **“Accepted”** statusand a quantitative payment has been specified, the report is automatically transferred to the “Payouts” section, where it will be credited with remuneration. **Important note**: in order to receive a reward, the User needs to go through the verification process in his personal account. For more information, see the “User Verification” section. The Operator will contact the User personally to make payments and sign documents. Users, in turn, are required to familiarize themselves with the public offer and sign the EDS as a closing document.
2. The user can view the rewards for public and private programs by selecting the “Public Payments” or “Private Payments” section.
3. Each payout has 5 statuses:
	1. The payout is assigned the status "**Under consideration**" when the payout is allocated to the User and waiting for confirmation of this payment by the Operator (the administrator of the platform).
	2. The payout is assigned the “**Signature Required**” status when the reward has been confirmed and the user needs to accept the terms of the public contract by clicking on the “I agree with the terms of service” button in the lower right corner of the page.
	3. After agreeing to the terms of service, the User must choose a payment method. Payment is made by bank card. Next, the User needs to specify the details and save the data. The Operator does not store or transfer the User's data to third parties, the payment system is only engaged in collecting details and sending rewards.
	4. Next, the payout is assigned the “**Processing**” status, which means that the payout process is confirmed by the bank service.
	5. Upon successful identity verification, agreement with the terms of service, confirmation of the payment method and acceptance of the reward, the payment status changes to “**Paid**” or “**Rejected**”.
	6. In the case of the “Rejected” status, the status and the reason for the error are displayed in the user's personal account, in the “Notifications” section. Next, in order to eliminate the error, the user needs to change the details or payment method in the “Payment Information” section by going to “Personal Data”.
	7. If the “Rejected” status is assigned due to an error on the service side, the Operator immediately proceeds to eliminate it and contacts the User. In any case, the user can contact technical support at info@tumar.one.
4. If agreeing to the terms, the User should carefully read their content and detailed instructions.
5. Researchers are provided with a Public Agreement for the provision of services for the provision of access to a web resource. This agreement is public, accordingly, the consent and acceptance of the terms is expressed through the form of the site (checkbox), by clicking it.

**Additionally:**

**Guidelines:**

* If a vulnerability is detected, it is necessary to inform the Operator about it as soon as possible so that the platform team can make every effort to quickly resolve this problem
* The user needs to be able to stop in time. For example, with SQLi, it is enough to output version() or similar information and stop, rather than dumping (dumping) the entire user base.
* The user must act reasonably and responsibly to avoid breaches of confidentiality, destruction of data, and interruption or deterioration of services.
* Do not use automatic scanning tools, this will definitely not add points to the User when reviewing the report.

**Rules of participation**

1. Do not disseminate information about the vulnerability until it is fixed.

2. Make every effort not to cause damage to our users and services (act in good faith).

3. Be sure to use own accounts, phone numbers, etc., to conduct the research. Do not attempt to access someone else's accounts or any confidential information. If access to the account is required to search for vulnerabilities, the User undertakes to use his/her personal account.

4. If, in the course of the research, the participant accidentally gained access to personal data, the Operator strongly requests that all information related to them, including connection codes, personal data, etc., be deleted from its media, after notifying the platform team about this.

5. Make all reasonable efforts to avoid violations of the privacy and work of other users, including unauthorized access to data, destruction of data, interruption or deterioration of services, etc.

6. The Operator deems it unacceptable and the reward will not be paid if it is discovered that in the course of testing and vulnerability search by the User:

* Physical interference with data centers or offices was committed.
* Social engineering methods were used to target the company's employees.
* The company's infrastructure was hacked and the information obtained was used to report vulnerabilities.
* Attempts have been made to gain access to other users' accounts or data.

7. Automatic scanning tools should be limited to no more than 5 requests per second (300 requests per minute) per target host and should not exceed the limit of 3 concurrent requests at the same time (5 threads).

8. Aggressive security checks are prohibited. It should be remembered that the User is testing a production environment that is functioning, maintained and controlled. To prevent negative consequences, the user needs to conduct research responsibly and reasonably control the impact of their tests on users, moderators, and system administrators.

Aggressive security checks and tests can trigger security mechanisms and generate an information security incident, which in turn can lead to other enforcement measures, such as blocking an account, phone number, or IP address.

**Types of vulnerabilities by severity levels for public programs:**

**Vulnerability severity scores are awarded as follows:**

1) For a low level of criticality - from 0 to 30 points;

2) For the average level of criticality - from 31 to 60 points;

3) For a high level of criticality - from 61 to 100 points.

Path Traversal -- 40-70 Medium/High

Directory Listing Enabled -- 10-40 Low/Medium

Insecure Redirect URI -- 5-10

Clickjacking -- 5

Brute Force -- 5

SQL Injection -- 50 - empty base, 70 - payload

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. High level of criticality:**

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. Medium level of criticality:**

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. Low Criticality:**

Cross-site Request Forgery

Sensitive Data Exposure Insecure

Redirect URI

Clickjacking

Brute Force

Reflected XSS

SMS flood

Open Redirect URI

It should be borne in mind that the severity level depends on what the identified vulnerability can lead to. Consequently, security analysts individually evaluate each vulnerability report. Also, it should be remembered that vulnerability assessments differ from one program to another, so before sending a report, the User should familiarize himself with the description of the program and follow their rules.

**Appendix No. 2 to the Public Offer Agreement for the provision of services for the provision of access to a web resource located on the Internet at:** [**https://tumar.one/**](https://tumar.one/)

* + - 1. **COLLECTION AND PROCESSING OF PERSONAL DATA**
	1. The Operator collects and stores only those Personal Data that are necessary for the provision of the Services by the Operator and interaction with the User.
	2. Personal data may be used for the following purposes:
		1. provision of Services to the User;
		2. identification of the User;
		3. interaction with the User;
		4. sending advertising materials, information and requests to the User;
		5. conducting statistical and other research;
		6. User verification.
	3. Among other things, the Operator processes the following data:
		1. Surname, first name and patronymic
		2. e-mail address;
		3. Telegram account and/or phone number (including mobile number);
		4. biometric data for verification;
		5. bank details;
		6. identity documents;
		7. other personal data (if necessary);
	4. The User is prohibited from specifying personal data of third parties on the Platform (except for the condition of representing the interests of these persons, having documentary evidence of third parties to carry out such actions).
1. **PROCEDURE FOR PROCESSING PERSONAL AND OTHER DATA**
	1. The Operator undertakes to use Personal Data in accordance with the Law "On Personal Data" of the Republic of Kazakhstan and the Operator's internal documents.
	2. In relation to the Personal Data and other Data of the User, their confidentiality is maintained, except for cases when the specified data is publicly available.
	3. The Operator has the right to keep an archival copy of the Personal Data. The Operator has the right to store Personal Data and Data on servers outside the territory of the Republic of Kazakhstan.
	4. The Operator has the right to transfer Personal Data and User Data without the User's consent to the following persons:
		1. state bodies, including bodies of inquiry and investigation, and bodies of local self-government upon their reasoned request;
		2. in other cases expressly provided for by the current legislation of the Republic of Kazakhstan.
	5. The Operator has the right to transfer Personal Data and Data to third parties not specified in clause 2.4. of this Privacy Policy, in the following cases:
		1. The User has expressed his/her consent to such actions;
		2. the transfer is necessary as part of the User's use of the Site or the provision of Services to the User;
	6. The Operator carries out automated processing of Personal Data and Data.
2. **PROTECTION OF PERSONAL DATA**
	1. The Operator shall ensure proper protection of Personal and other data in accordance with the Legislation and shall take necessary and sufficient organizational and technical measures to protect Personal Data.
	2. The applied protection measures, among other things, make it possible to protect Personal Data from unauthorized or accidental access, destruction, modification, blocking, copying, distribution, as well as from other illegal actions with them by third parties.
3. **MISCELLANEOUS**
	1. The law of the Republic of Kazakhstan shall apply to this Privacy Policy and the relations between the User and the Operator arising in connection with the application of the Privacy Policy.
	2. All possible disputes arising from this Privacy Policy shall be resolved in accordance with the current legislation at the place of registration of the Operator. Before applying to the court, the User must comply with the mandatory pre-trial procedure and send the relevant claim to the Operator in writing. The deadline for responding to a claim is 30 (thirty) business days.
	3. If, for any reason, one or more provisions of the Privacy Policy are found to be invalid or unenforceable, this does not affect the validity or enforceability of the remaining provisions of the Privacy Policy.
	4. The Operator has the right to change the Privacy Policy (in whole or in part) unilaterally at any time without prior agreement with the User. All changes come into force from the moment it is posted on the Site.
	5. The User undertakes to independently monitor changes to the Privacy Policy by familiarizing himself with the current version.
	6. All suggestions or questions regarding this Privacy Policy should be communicated by email: info@tumar.one.