Договір приєднання
про надання послуг з пошуку вразливостей

м. Київ від 30.12.2024

ТОВ “СМАРТ ЮНІТ” (надалі - Координатор), в особі директора Папариги Джоржа Юрійовича, який діє на підставі Статуту, з однієї сторони, цим документом пропонує необмеженому колу фізичних осіб/фізичних осіб – підприємців (надалі - Учасник або Хантер) з іншої Сторони (надалі разом - Сторони), які прийняли пропозицію приєднатись до договору про надання послуг з пошуку вразливостей Системи.

Цей Договір приєднання укладається відповідно до ст. 634 Цивільного кодексу України (далі - ЦКУ), його умови однакові для всіх Учасників. Даний договір пропонується до укладення невизначеному колу осіб шляхом розміщення на сторінці https://prozorro.gov.ua/bugbounty в мережі інтернет Публічної оферти згідно зі ст. 641 ЦКУ. Беззастережне прийняття всіх умов даної Публічної оферти без будь-яких винятків та/або обмежень вважається акцептом даної Публічної оферти (далі - Договору) Координатором і Учасником, а сам Договір автоматично вважається укладеним (акцепт Публічної оферти рівнозначний укладенню Договору на умовах, викладених в Оферті).

1. Визначення основних термінів

Договір приєднання – це правочин, який встановлює однакові для всіх Учасників умови надання цих послуг на умовах публічної оферти з моменту її акцептування Учасником, про отримання послуг від Учасника шляхом участі у тестуванні та пошуку вразливостей Системи (далі - Проект).

Система – тестовий продукт, який не містить персональних даних, конфіденційної інформації та іншої інформації, розголошення якої заборонено законодавством України.

Вразливість - помилка, несправність або інший збій (зрив) у програмах, системах, алгоритмах роботи тощо Системи, що може вплинути на функціонування Системи в цілому або окрему її частину (компонент).

Публічна оферта (пропозиція) - пропозиція Координатора, адресована будь-якій фізичній особі/фізичній особі-підприємцю (Учаснику або Хантеру) відповідно до статті 641 Цивільного кодексу України, укласти з ним договір на умовах, визначених у ній.

Акцепт (прийняття пропозиції) - повне й беззастережне прийняття Учасником умов Публічної оферти, викладених в цьому Договорі. Договір, укладений Учасником за допомогою акцепту публічної оферти, має юридичну чинність з моменту направлення Учасником на електронну адресу disclosure@prozorro.ua, вказану в Договорі, звіту про знайдену вразливість, згідно зі статтею 642 Цивільного кодексу України і прирівнюється до укладання договору сторонами у письмовій формі.

Адміністратор електронної системи закупівель (надалі по тексту - Адміністратор) – Державне підприємство «ПРОЗОРРО» – юридична особа, що в порядку, передбаченому законодавством України, визначена відповідальною за забезпечення функціонування та наповнення веб-порталу Уповноваженого органу з питань закупівель.

Авторизований електронний майданчик (надалі по тексту - Майданчик) - авторизована Уповноваженим органом інформаційно-телекомунікаційна система Майданчика, яка є частиною електронної системи закупівель та забезпечує реєстрацію осіб, автоматичне розміщення, отримання, передавання інформації та документів під час проведення процедур закупівель, користування сервісами з автоматичним обміном інформацією, доступ до якого здійснюється за допомогою мережі Інтернет.

Учасник або Хантер - фізична особа/фізична особа-підприємець, яка виявила вразливість в Системі, повідомила про цю вразливість у спосіб, вказаний цим Договором, та має право на встановлену цим Договором винагороду.

Однотипні вразливості - це вразливості, виникнення яких викликане одним механізмом обробки запитів (певним елементом функціоналу). Тобто, якщо виправлення одного механізму призведе до неможливості застосування усіх однотипних вразливостей.

Electronic Procurement System Bug Bounty Program - проект, який створено з метою посилення захисту інформаційної безпеки та кібербезпеки в ІТС “PROZORRO” та ІТС Майданчиків із залученням (надання дозволу) Хантерів до пошуку вразливостей на тестовому середовищі (staging area) електронної системи закупівель (далі - Проект).

Організатори проекту – Координатор, Майданчик, Адміністратор.

Санкціоновані особи - особи, які підпадають під санкції (обмеження) України, або інших країн чи організацій.

Сторони - для цілей цього Договору під Сторонами розуміють ТОВ “СМАРТ ЮНІТ” та Учасника або Хантера, який своїми конклюдентними діями на виконання умов цієї Оферти надав згоду та здійснив акцепт запропонованої оферти і набув статусу верифікованого учасника Проекту.

2. Загальні умови

2.1. Цей Договір укладається між Учасником і Координатором у формі договору приєднання відповідно до ст. 634 Цивільного кодексу України та діє до закінчення Проекту, про що оприлюднюється відповідне повідомлення на сайті Адміністратора чи Координатора.

2.2. Публікація (розміщення) тексту Договору на сайті Координатора Проекту та Адміністратора Системи є офіційною пропозицією (Публічною Офертою) Координатора, що адресована невизначеному колу осіб відповідно до статті 641 Цивільного кодексу України укласти з ним договір про надання послуг на умовах договору приєднання.

2.3. У випадку прийняття умов даної Оферти, Учасник погоджується з усіма умовами цього Договору і підтверджує, що йому зрозумілі всі його положення.

2.4. Ця Оферта є відкритим і загальнодоступним документом.

2.5. Координатор має право змінювати або доповнювати Договір в будь-який момент без попереднього або наступного повідомлення Учасників, що оприлюднюється за 1

день до набрання змінами чинності і які доводяться до загального відома за допомогою публікації на Сайті.

2.6. Кожна Сторона гарантує іншій Стороні, що володіє необхідною дієздатністю, а також всіма правами і повноваженнями, необхідними і достатніми для укладання і виконання Договору відповідно до його умов. Координатор також підтверджує, що не існує будь-яких обставин, через які можна було б визнати такий договір нікчемним.

2.7. При приєднанні до даної Публічної оферти Учасник надає згоду Координатору на збір, використання та обробку його персональних даних та право вчиняти дії, передбачені Законом України «Про захист персональних даних».

2.8. Учасник підтверджує, що прочитав і погоджується з усіма умовами Договору та Програми беззастережно та зобов'язується виконувати.

2.9. Участь у Проекті є вільною та добровільною. Учасник не має отримувати будь-які попередні дозволи та погодження при умові дотримання вимог цієї публічної оферти та умов Проекту. За умови дотримання положень цієї публічної оферти, пошук вразливостей в Системі буде вважатися суспільно корисною справою та не може вважатись правопорушенням чи злочином.

У разі переслідування Учасника, який не порушує умови цієї публічної оферти, правоохоронними органами, Організатори нададуть докази його невинуватості.

2.10. Організатори Проекту мають право зменшувати обсяг Договору та загальну суму винагороди за цим Договором, шляхом внесення змін до цього договору. У разі зменшення об'єму договору, оплата знайдених вразливостей здійснюється в залежності від фактичних фінансових можливостей організаторів Проекту.

2.11. Організатори Проекту мають право переглянути розмір винагороди, визначиненний у Таблиці 1 даного договору, та мають право зменшити розмір винагороди за знайдені вразливості, шляхом внесення змін до цього договору.

2.12. Організатори Проекту мають право відмовити учаснику у виплаті винагороди у разі завершення Проекту, закінчення фінансування Проекту або зменшення об'ємів такого фінансування, про що оприлюднюється відповідне повідомлення на сайті Адміністратора чи Координатора.

3. Предмет договору, оплата послуг та заохочувальні бали

3.1. Предметом договору є надання Учаснику доступу до Системи для здійснення пошуку вразливостей за умов, передбачених цим договором.

3.2. Фінансова винагорода Учаснику встановлюється відповідно до рівня складності (критичності), виявленої в роботі Системи Вразливості.

Під винагородою розуміється заохочення, виражене у грошовій формі в національній валюті України, у розмірах, в залежності від категорій Вразливості, що наведені в таблиці 1, на банківський рахунок, або у інший спосіб, не заборонений законодавством України:

Таблиця 1

Категорія вразливості згідно з BugCrowd Vulnerability Rating Taxonomy:

Категорія	Винагорода*	Вразливості для відповідної категорії
P1	28 000 грн	File Inclusion, RCE, SQL Injection, XXE, Authentication Bypass, Critically Sensitive Data, Command Injection, Hardcoded Password
P2	14 000 грн	XSS (P2 specific), SSRF, CSRF (Application-Wide), Application-Level DOS (NOT DDOS), Hardcoded Password, Weak Password Reset Implementation
P3	8 400 грн	HTTP Response Manipulation, Content Spoofing, Session Fixation, XSS and SSRF (P3 specific)

** Виплата винагороди здійснюється з дотриманням податкового законодавства України*

За визнані Вразливості P1, P2, P3 Учаснику виплачується фінансова винагорода та нараховуються заохочувальні бали. За Вразливості P4 Хантерам нараховуються лише заохочуванні бали.
Таблиця нарахувань заохочувальних балів за Вразливості:

Критичність	Кількість балів	
	За перший репорт	За дублікат
P1	100	25
P2	50	12
P3	25	5
P4	12	2

3.3. Листування щодо отримання фінансової винагороди здійснюється Учасником виключно з електронної адреси, з якої направлено звіт щодо вразливості.

4. Умови та правила участі в Проекті

4.1. Для участі в Проекті Учасник повинен **відповідати таким вимогам**:

4.1.1. Учасник має бути не молодше 14 років. Якщо Учаснику менше 14 років та він вважається неповнолітньою особою за країною громадянства/проживання, він повинен отримати згоду від батьків чи законних опікунів, перш ніж вчинити дії, визначені цим договором, як Акцепт оферти та участі у Проекті. Організатори мають право вимагати від такого Учасника письмової (також нотаріально посвідченої) згоди представників Учасника (батьків чи законних опікунів/піклувальників про свою участь у Проекті) та за її відсутності Учасник втрачає право на отримання винагороди.

4.1.2. Учасник не брав участь у будь-якій частині розробки, адміністрування та/або виконання Системи.

4.1.3. Учасник не є зараз або не був протягом останніх шести місяців працівником

та/або надавачем послуг Адміністратору чи Майданчикам, що були пов'язані з розробкою, адмініструванням, підтримкою Системи тощо.

4.1.4. Учасник не є членом сім'ї або пов'язаною особою з будь-ким з переліку, наведеному в пп. 4.1.2 та 4.1.3.

4.1.5. Учасник не є працівником підприємства, установи, організації будь-якої форми власності, політика яких забороняє без надання дозволу роботодавця брати участь в таких Проектах.

4.1.6. Учасник не є особою, на яку поширюються санкційні заходи, введені в Україні або які містяться на сайті: sanctions.nazk.gov.ua.

4.1.7 Учасником може бути як фізична особа так і фізична особа - підприємець.

4.2. У випадку, якщо Учасника буде визначено таким, що порушує хоча б один із критеріїв, викладених у пункті 4.1, він втрачає право бути Учасником і не має права на винагороду.

4.3. Учасник зобов’язаний дотримуватися вимог конфіденційності - вся інформація, отримана за допомогою участі або під час участі у Проекті, вважається конфіденційною. Організатори залишають за собою право вжити юридичних дій щодо захисту від неправомірного використання або розкриття інформації, що стосується Проекту, або іншим чином розповсюдження такої інформації.

4.4. Учасник використовує лише власні персональні дані, а також власну електронну адресу під час взаємодії та участі в Проекті.

4.5. Учаснику **заборонено**:

4.5.1. здійснення цілеспрямованих атак, які можуть завдати шкоди чи іншим чином вплинути на надійність або цілісність даних Системи;

4.5.2. здійснення інших цілеспрямованих дій, що спричинять перебої в роботі Системи, використовувати її вразливість в пошуках власних вигод або порушувати цим законодавство України.

4.6. Винагорода Учаснику встановлюється відповідно до рівня складності (критичності), виявленої в роботі Системи. Умови оплати винагороди здійснюються відповідно до п.3.2 Договору - приєднання.

Не приймаються та не сплачується винагорода за виявлені потенційні загрози та вразливості без детального опису вектору атаки та доказів потенційного завдання збитку або шкоди, наприклад:

- відсутність безпечних HTTP-хедерів та флагів cookie;
- розкриття версії програмного забезпечення;
- раніше відомі вразливі бібліотеки;
- вразливості в конфігурації SSL / TLS.

Інформація про нараховані заохочувальні бали Учасника вноситься до Рейтингу Хантерів та оприлюднюється на сайті Координатора та/або Адміністратора ЕСЗ.

4.7. Нагороджуються лише вразливості, підтверджені листом Координатора, після підтвердження їх з боку Адміністратора та/або Майданчика.

4.8. При одночасному знаходженні однакових або однотипних вразливостей, право на

винагороду отримує Учасник, який першим повідомив у встановлений Договором спосіб, про виявлену в Системі вразливість.

4.9. Вразливість повинна існувати в актуальній версії.

4.10. Учасник повинен надати фактичні докази існування вразливості, ***та її практичного, а не потенційного використання*** у вигляді звіту (Proof of Concept). Вимоги до звіту зазначені в п. 5.2.

4.11. Учасник повинен повідомити про вразливість та дотриматися умов відповідального розкриття інформації: публічне розкриття інформації про вразливість дозволяється лише після її виправлення та за письмової згоди Координатора.

4.12. Учасник повинен надати додаткові відомості про вразливість, які можуть знадобитися для її виправлення. Також, Учасник повинен здійснити перевірку виправлення вразливості в разі отримання такого звернення від Координатора.

4.13. Учасник зобов'язується дотримуватись норм етичної поведінки та таких правил:

- не робити нічого, що порушує законодавство України; ;
- не надсилати спам;
- не займатися діяльністю, що вводить в оману;
- не займатися шкідливою діяльністю (наприклад, передача вірусів);
- не посягати на права інших осіб (наприклад, несанкціонований обмін матеріалами, захищеними авторським правом) і не займатися діяльністю, яка порушує конфіденційність інших осіб;
- не допомагати іншим особам порушувати ці правила та діючі норми законодавства України;
- регулярно перевіряти зміни на сайті Адміністратора або до цього Договору.

4.14. Учасникам забороняється здійснювати розподілені атаки відмови в обслуговуванні (DDoS).

4.15. Учасник погоджується надати Координатору свої особисті та контактні дані та іншу інформацію, що може бути кваліфікована як персональні дані відповідно до українського законодавства.

4.16. Персональні дані будуть використовуватися в тій мірі, в якій це потрібно для виконання умов цього Договору. Персональні дані, не можуть розголошуватися без згоди Учасника, за винятком випадків, встановлених законодавством України або умовами Договору.

4.17. Період зберігання даних учасника Програми становить 3 (три) роки, якщо юридичні акти не вимагають більш тривалого періоду зберігання.

4.18. Учасники, яким необхідно самостійно сплачувати податки, несуть персональну відповідальність за сплату всіх податків та обов'язкових платежів, пов'язаних з цим Договором.

4.19. Координатор Проекту залишає за собою право будь-коли припинити Проект та

виплату Винагороди за відповідним зверненням Адміністратора та Майданчиків.

5. Особливі умови. Вказівки щодо звітності

5.1. Після знаходження вразливості, виявленої в Системі, Учасник повинен направити опис виявленої вразливості (далі - Звіт) на електронну адресу: disclosure@prozorro.ua. Направленням Звіту учасник підтверджує беззаперечну згоду з умовами цього договору, підтверджує повну відповідність вимогам, що висуваються до Учасників та висловлює готовність виконувати його умови в повній мірі.

5.2. Звіт оформлюється у довільній формі, українською мовою та повинен містити таку інформацію:

- інформацію про Учасника;
- назва та опис вразливості;
- категорія вразливості згідно з BugCrowd Vulnerability Rating Taxonomy;
- пояснення вибраної категорії відповідно до практичного використання вразливості, а не потенційної можливості її використання;
- опис кроків з відтворення практичного використання вразливості, який може включати:

- HTTP-сесії, що демонструють вразливість;
- Знімки екрану, що демонструють вразливість;
- Відео-демонстрацію відтворення вразливості.

Приклад форми звіту про вразливості

Заголовок

- номер знайденої вразливості (особиста наскрізна нумерація Хантера);
- тип вразливості;
- домен чи ендпоінт;
- категорія вразливості згідно з BugCrowd Vulnerability Rating Taxonomy.

Опис (коротке пояснення вразливості)

- загальна інформація про тип виявленої вразливості та причини її виникнення;
- загальна інформацію про вразливий ендпоінт або компонент;
- необхідні привілеї (privilege required);
- необхідність додаткових дій з боку користувача (user interaction).

Відтворення

Детальний опис кроків з відтворення практичного використання вразливості, який може включати:

- інструменти та/або команди, що використовуються для виконання атаки;
- знімки екрану, що демонструють вразливість;
- відео-демонстрацію відтворення вразливості.

Вплив (impact)

Пояснення вибраної категорії відповідно до продемонстрованого практичного використання вразливості, зокрема:

- що може зробити зловмисник;
- до якої інформації він може отримати доступ;
- як це впливає на систему.

Рекомендації

- можливі рішення щодо усунення вразливості.

5.3. Координатор Проекту найбільше зацікавлений в отриманні Звітів щодо таких вразливостей:

- Remote Code Execution
- SQL Injection
- Cross-Site Scripting
- Cross-Site Request Forgery
- Authentication Bypass
- Privilege Escalation

5.3.1. Дозвіл щодо здійснення дослідження вразливостей поширюється виключно на такі домени з вказаними IP адресами:

- staging.prozorro.gov.ua 195.178.150.103
- auction-staging.prozorro.gov.ua 195.178.157.50, 195.178.157.60
- audit-api-staging.prozorro.gov.ua 195.178.157.50, 195.178.157.60
- public-api-staging.prozorro.gov.ua 195.178.157.50, 195.178.157.60
- public-docs-staging.prozorro.gov.ua 195.178.157.50, 195.178.157.60
- swift-staging.prozorro.gov.ua 195.178.157.50, 195.178.157.60
- sas-staging.prozorro.gov.ua 195.178.150.103
- amcu-staging.prozorro.gov.ua 195.178.150.103
- infobox.prozorro.org 195.178.150.108, 195.178.150.106
- risks-staging.prozorro.gov.ua 195.178.150.82 195.178.150.81
- exam-staging.prozorro.gov.ua 195.178.150.105
- exam-back-staging.prozorro.gov.ua 195.178.150.105

Електронні Майданчики:

- zakupivli.today 193.200.64.61
- my.zakupivli.today 193.200.64.61
- stage.e-tender.ua 94.131.241.154
- test.smarttender.biz 91.200.74.11
- api-test.smarttender.biz 91.200.74.11
- content-test.smarttender.biz 91.200.74.11
- smartid-test.smarttender.biz 91.200.74.11

НЕ ДОЗВОЛЯЄТЬСЯ сканування та пошук вразливостей, та не приймаються вразливості (out of scope) на наступних доменах:

- всі інші домени *.prozorro.gov.ua
- всі інші домени *.prozorro.org
- всі інші домени *.prozorro.ua
- *.openprocurement.org
- всі інші домени *.s3.zakupivli.today
- всі інші домени та субдомени *.e-tender.ua, *gov.e-tender.ua, *auction.e-tender.ua, *biz.e-tender.ua

- всі інші домени *smarttender.biz, *api.smarttender.biz, *content.smarttender.biz, *smartid.smarttender.biz

5.4. Координатор Проекту не вимагає жодних прав на результати віднайдення вразливості (ей), втім, надсилаючи звіт, Учасник:

5.4.1. надає Координатору, Адміністратору/Майданчику безвідкличний, безстроковий, безоплатний дозвіл щодо інтелектуальної власності у Звіті:

(i) використовувати, переглядати, оцінювати, перевіряти та іншим чином аналізувати Звіт;

(ii) відтворювати, змінювати, поширювати, показувати та використовувати публічно, комерціалізувати та створювати похідні твори, що випливає зі Звіту та весь його вміст, повністю або частково;

та (iii) розміщення Звіту та всього його вмісту або його частини у матеріалах, пов'язаних з маркетингом чи просуванням цього чи інших проектів (включаючи внутрішні та зовнішні, презентації, конференції, виставки тощо) у всіх засобах масової інформації (зараз відомі чи такі, що будуть створені пізніше).

5.4.2. Учасник погоджується підписати акти виконаних робіт по знайдених вразливостях та будь-яку документацію, яка може знадобитися Координатору для підтвердження прав, які було надано вище.

5.4.3. Учасник заявляє та гарантує, що Звіт та наведене в ньому - його власна робота, що він не використовував інформацію, що належить іншій фізичній чи юридичній особі.

5.4.4. Координатор вимагає, щоб Звіт Учасника залишався конфіденційним і не був розголошений третім особам до моменту усунення такої вразливості. До моменту отримання листа про усунення вразливості, Учасник буде вважатися таким, що не повідомлений про розгляд Звіту, а сам Звіт залишатиметься конфіденційним.

5.4.5. Після надходження Звіту та доданих матеріалів, його буде розглянуто відповідними спеціалістами та підтверджено його актуальність та придатність. Координатор, Адміністратор та Майданчик докладатиме всіх зусиль для якнайшвидшого розгляду Звіту.

5.4.6. Рішення щодо результатів розгляду Звіту є остаточним та не підлягає перегляду та/або оскарженню Учасником.

Якщо Ви, як потенційний або дійсний Учасник, не погоджуєтесь з будь-якими умовами цього Договору, інформацією, яка доводяться до загального відома за допомогою публікації на Сайті Координатора або Адміністратора Системи, не приймайте Оферту, не надавайте послуги щодо пошуку Вразливостей, не надсилайте Звіт та будь-які інші повідомлення в рамках Проекту.