

Затверджено:
Наказом № 30/11/23 від 30.11.2023 року
директора ТОВ «ФІНТЕХ БЕНД»
Рогальського М.В.

Набрання чинності: 30.11.2023 року

ПРАВИЛА ХАКАТОНУ «Баг Баунті»

Організатор: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ФІНТЕХ БЕНД», ідентифікаційний код за Єдиним державним реєстром підприємств та організацій України 32388371, місцезнаходження якого зареєстроване за адресою: 49044, Дніпропетровська обл., м. Дніпро, вул. Січеславська Набережна, буд. 47, офіс 1, в особі директора Рогальського Михайла Вікторовича, який діє на підставі Статуту, пропонує резидентам України прийняти участь в Хакатоні «Баг Баунті», для чого публікує ці Правила Хакатону «Баг Баунті» (далі - Правила).

Правила - за своєю суттю є договором приєднання, який укладається в порядку, встановленому ст. 634 Цивільного кодексу України, а саме: публічна його частина встановлена Організатором та розміщена в мережі Інтернет на сайті <https://fintech.band/>. Приєднатися до Правил Учасник може тільки в цілому. У відповідності до ч. 2 ст. 642 Цивільного кодексу України, реєстрація Учасника за посиланням <https://forms.gle/KKG7hQqfqMTKaPAj7> та підписання Учасником та Організатором Заяви про приєднання до Правил є акцептом цих Правил, що прирівнюється до укладення договору на умовах викладених нижче по тексту.

Заява про приєднання підписується накладанням кваліфікованого електронного підпису Сторонами в порядку, передбаченому чинним законодавством України за допомогою Сервісу електронного документообігу «Вчасно» (<https://vchasno.ua/>).

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Хакатон «Баг Баунті» (далі — Хакатон) — змагання ІТ фахівців з пошуку вразливостей комп'ютерної програми - мобільного застосунку monobank для android та IOS.

1.2. Мета та завдання Хакатону:

- Пошук та повідомлення Організатора про вразливості мобільного застосунку monobank.

1.3. Організатор Хакатону - ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ФІНТЕХ БЕНД», ідентифікаційний код за Єдиним державним реєстром підприємств та організацій України 32388371, місцезнаходження якого зареєстроване за адресою: 49044, Дніпропетровська обл., м. Дніпро, вул. Січеславська Набережна, буд. 47, офіс 1.

1.4. Призовий фонд Хакатону - 1 000 000 грн. (один мільйон гривень), який розподіляється між переможцями - Учасниками Хакатону, які виконали завдання (повідомили Організатора про вразливості мобільного застосунку monobank) згідно з критеріями, визначеними нижче. У разі якщо кількість звітів переможців про вразливості перевищує розмір Призового фонду, то сплачується винагорода за вразливості, що знайдені першими виключно в межах суми призового фонду Хакатону.

1.5. Кількість переможців Хакатону та порядок їх визначення вказуються у відповідних розділах цього Положення.

1.6. Інформація про Хакатон розміщується у глобальній мережі Інтернет на офіційному сайті Організатора <https://fintech.band/>, а також у засобах масової інформації.

1.7. Під час проведення Хакатону обробка персональних даних учасників здійснюється з урахуванням вимог Закону України «Про захист персональних даних».

2. УЧАСНИКИ ХАКАТОНУ

2.1. Учасники Хакатону є резиденти України: фізичні особи, фізичні особи - підприємці та юридичні особи.

2.2. Учасники зобов'язані дотримуватись вимог прописаних в Положенні та норм етичної поведінки.

2.3. Заявник вважається учасником Хакатону після успішного проходження реєстрації для участі в Хакатоні. Правила вважаються акцептованими Учасником, а Учасник вважається зареєстрованим Організатором за умови підписання Заяви Учасником / уповноваженою особою Учасника та уповноваженою особою Організатора про приєднання до Правил.

3. ПОРЯДОК ПРОВЕДЕННЯ ХАКАТОНУ

3.1. Хакатон проводиться у категорії Баг Баунті.

3.2. Хакатон проводиться в один етап в онлайн форматі: з 17.11.2023 року по 08.12.2023 р. включно.

3.3. Для участі в Хакатоні необхідно зареєструватися до 30.11.2023 року включно шляхом подачі заявки за посиланням <https://forms.gle/KKG7hQqfqMTKaPAj7> та підписання Заяви про приєднання.

3.4. Організатор має право на власний розсуд прийняти рішення щодо:

- Відмови в реєстрації Учасника;
- Внесення змін до Правил Хакатону;
- продовження строку проведення Хакатону;
- продовження строків розгляду звітів Учасників;
- продовження строків розрахунків з Учасниками з числа переможців.

3.5. У разі виникнення ситуацій, що допускають неоднозначне тлумачення цих Правил, та/або питань, неврегульованих цими Правилами, остаточне рішення приймається Організатором відповідно до вимог чинного законодавства України. При цьому рішення Організатора є остаточним і не підлягає оскарженню.

3.6. Організатор залишає за собою право змінювати Правила Хакатону «Баг Баунті». Всі зміни будуть розміщені на офіційному сайті Організатора. Організатор не несе відповідальності за не ознайомлення Учасників Хакатону з такими змінами.

3.7. Організатор не несе відповідальності у разі виникнення форс-мажорних обставин, таких як стихійні лиха, пожежа, повінь, військові дії будь-якого характеру, в тому числі антитерористичні операції, блокади, суттєві зміни у законодавстві, що діє на території проведення Хакатону, інші непідвладні контролю з боку Організатора обставини.

4. ВИМОГИ ДО РОБІТ УЧАСНИКІВ ПІД ЧАС УЧАСТІ В ХАКАТОНІ

4.1. Учасник, який виявив вразливість, подає Організатору звіт, що буде розкривати висновки вразливості.

4.2. Звіт має містити інформацію про те:

- Де виявлено вразливість;
- на кого вона впливає;
- як її відтворити,
- параметри, на які вона впливає,
- надати допоміжну інформацію Proof-of-Concept. Для цього Учасник може завантажити будь-які файли або журнали як підтверджуючі докази. Це не тільки допомагає швидко відтворити проблему, але й швидше переносить заявку на розгляд без затримок через відсутність інформації.

4.3. Складовими частинами звіту є:

Заголовок звіту	Це буде заголовок вашого звіту. Він повинен надавати короткий огляд типу знайденої вразливості, місця її виявлення
-----------------	--------------------------------------------------------------------------------------------------------------------

	та загального впливу. Наприклад, «Віддалене включення файлу у форму завантаження резюме дозволяє віддалене виконання коду» є більш описовим і корисним, ніж «Знайдено ін'єкцію RFI».
Ціль	Визначає конкретну ціль, на яку впливає виявлена Учасником вразливість.
Технічна серйозність	Класифікація таксономії рейтингу вразливості визначає тип помилки, яку Учасник виявив, на основі нашої базової системи оцінки пріоритетів для типових вразливостей, визначеної у Правилах Хакатону. Важливо вибрати правильний тип, щоб Організатор усвідомлював ризик вразливості. Рейтинг технічної серйозності вразливостей, не гарантує, що рейтинг технічної серйозності буде застосований до вашого подання після розгляду впливу.
Деталі вразливості включають таку інформацію:	<ul style="list-style-type: none"> - URL-адреса/розташування вразливості: місце в програмі, де Учасник виявив вразливість. - Опис: Учасник має надати детальну інформацію про вразливість. Мають бути додані чіткі та описові кроки реплікації, щоб Організатор міг легко відтворити та підтвердити висновки Учасника. Також має бути опис ризиків і впливу. Учасник має надати ілюстративні докази у вигляді скріншотів або відео, які демонструють доказ уразливості. Це одна з найефективніших речей, які Учасник може зробити, щоб надати контекст навколо свого подання. Додатково можуть бути надані сценарії підтвердження концепції, знімки екрана, записи екрана тощо.

5. ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

5.1. Загальне керівництво підготовкою та проведенням Хакатону здійснюється Організаційним комітетом (надалі – Оргкомітет), склад якого затверджується наказом Організатора.

5.2. До складу Оргкомітету входять представники Організатора, а також профільні спеціалісти, які були залучені Організатором на договірних засадах.

5.3. У функції Оргкомітету входить:

- підготовка та розповсюдження інформації про Хакатон;
- забезпечення безпосереднього проведення Хакатону;
- підведення підсумків Хакатону.

6. ЖУРІ ХАКАТОНУ

6.1. Із метою забезпечення об'єктивності оцінювання учасників та визначення переможців запрошуються журі. Склад журі Хакатону затверджується наказом Організатора.

6.2. Журі Хакатону формується із числа представників Організатора, а також профільних спеціалістів, які були залучені Організатором на договірних засадах.

6.3. Журі очолює голова, який організовує роботу членів журі, проводить засідання журі, бере участь у визначенні переможців і призерів Хакатону, затверджує список переможців.

6.4. Члени журі забезпечують об'єктивність оцінювання під час проведення Хакатону, ведуть оцінювальні протоколи, визначають переможців та призерів.

6.5. Результати оцінювання оформлюються протоколами засідань журі. Протокол підписують Голова, відповідальний секретар і члени журі, які брали участь у засіданні.

7. ПОРЯДОК ВИЗНАЧЕННЯ ПЕРЕМОЖЦІВ

7.1. Переможцями є всі Учасники, які першими повідомили Організатора про конкретну вразливість мобільного застосунку топобank. Сума виплати винагороди переможцям з числа Учасників визначається, виходячи з критеріїв оцінювання, визначених у розділі 8 цих Правил.

7.2. Організатор направляє повідомлення Учаснику щодо статусу переможця одразу після завершення оцінки робіт.

7.3. Рішення журі перегляду, оскарженню, роз'ясненню не підлягає.

7.4. Усі Учасники, які направили Організатору звіт щодо вразливостей мобільного застосунку топобank, отримують винагороду у розмірі 4800 грн.

7.5. Під час виплати винагороди на користь Учасника - фізичної особи Організатор, виконуючи функцію податкового агента, утримує податки та обов'язкові платежі та перераховує їх до бюджету України в розмірі та порядку, визначеному чинним законодавством України.

8. КРИТЕРІЇ ОЦІНЮВАННЯ

8.1. Роботи учасників Хакатону оцінюються за такими критеріями:

Критерії	Максимальна кількість балів	Вартість, грн. за 1 одиницю знайденої вразливості (сплачується першому з Учасників, хто повідомив Організатора щодо конкретної вразливості)
P1 (Критична): Уразливості, які спричиняють підвищення привілеїв від непривілейованих до адміністраторів або дозволяють віддалене виконання коду, фінансову крадіжку тощо.	1000	60 000
P2 (Висока): Уразливості, які впливають на безпеку програмного забезпечення та процеси, які воно підтримує	750	40 000
P3 (Середня): Уразливості, які впливають на кількох користувачів і для активації яких потрібна незначна взаємодія з користувачем.	500	30 000
P4 (Низька): Уразливості, які впливають на окремих користувачів і вимагають взаємодії або значних передумов для запуску (MitM) до запуску.	250	10 000

Повна таблиця для детальної класифікації, яка буде застосована при оцінюванні <https://bugcrowd.com/vulnerability-rating-taxonomy>

8.2. За результатом перевірки звіту Учасника щодо вразливостей мобільного застосунку топобank Організатор повідомляє Учасника щодо:

- Підтвердження знайденої вразливості;
- Кількість отриманих балів за знайдену вразливість;
- Чи був Учасник першим, хто повідомив Організатора щодо конкретної вразливості.

9. ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

9.1. Оргкомітет залишає за собою право використовувати назви, логотипи та короткі описи проєктів, що беруть участь в Хакатоні, а також презентації Учасників.

9.2. Організатори залишають за собою право оприлюднювати повністю або частково роботи учасників Хакатону в засобах масової інформації із зазначенням авторів.

9.3. В період проведення Хакатону буде проводитися фото- та відео зйомка заходу. Організатори залишають за собою право використовувати фото- і відео матеріали на власний розсуд.

10. ПЕРСОНАЛЬНІ ДАНІ

10.1. Під час реєстрації для участі в Хакатоні, Учасник Хакатону надає Організатору Хакатону свою згоду на обробку наданих при реєстрації і / або згодом при проведенні Хакатону персональних даних, включаючи прізвище, ім'я, по батькові, РНОКПП, номери засобів зв'язку та адресу електронної пошти, для цілей організації і проведення Хакатону, що включає передачу персональних даних, а також, в разі обрання Учасника переможцем Хакатону, – публікацію його прізвища, імені та по батькові, інших наданих Учасником даних на Інтернет-ресурсах Хакатону.

11. УМОВИ ПРО НЕРОЗГОЛОШЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

11.1. В рамках участі Учасника в Хакатоні Учасник може отримати або іншим чином мати доступ до інформації, розкритої в письмовій, усній чи іншим способом, яку Організатор та його дочірні компанії або філії вважають конфіденційною, яка може включати, але не обмежуючись цим, кодова база, бази даних і мережу Організатора та його дочірніх компаній або філій, особисту інформацію, ділову, фінансову та технічну інформацію, процеси та процедури розробки та виробництва, плани, дослідження, інформацію про існуючу та майбутню продукцію, зразки, прототипи, методи випробування, інформацію про обладнання, проекти, дані, комп'ютерні програми та програмне забезпечення (включаючи вихідний та об'єктний код), списки клієнтів і потенційних клієнтів, алгоритми, торгові марки, ідеї, концепції, блок-схеми, діаграми, пристрої, винаходи, формули, зразки, інформацію про постачальників, звіти, прогнози, ціни, дані про витрати та персонал, проекти, методи, техніки, креслення, комерційні секрети, процеси та ноу-хау. (разом "Конфіденційна інформація" або "КІ").

11.2. ВИКОРИСТАННЯ ТА ОБОВ'ЯЗОК ЗАХИЩАТИ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ. Учасник погоджується використовувати КІ лише для Мети, захищати та підтримувати конфіденційність КІ Організатора. Учасник не має права використовувати КІ, за винятком випадків, коли це необхідно для досягнення Мети, і не має права продавати, передавати, публікувати, розголошувати чи іншим чином використовувати чи надавати будь-яку частину КІ третім особам. Зобов'язання Учасника щодо конфіденційності та невикористання за цим Договором триватимуть на невизначений термін.

11.3. ПРАВО НА ПОВІДОМЛЕННЯ. У випадку, якщо Учасник: (а) отримує запит на розкриття КІ відповідно до чинного законодавства з належно оформленим документом, Учасник повинен надати Організатору негайне письмове повідомлення, щоб дозволити Організатору отримати відповідний засіб правового захисту, що захищає його від розголошення КІ, і Учасник повинен максимально обмежити оприлюднення КІ усіма можливими за даних обставин способами.

11.4. ПРАВО ВЛАСНОСТІ на КІ. Отримана під час Хакатону Конфіденційна інформація є та залишатиметься виключною власністю Організатора. Жодної ліцензії чи інших прав інтелектуальної власності не переходять до Учасника. При цьому Учасник має право на використання творів (комп'ютерних програм), отриманих в процесі участі у Хакатоні, тільки шляхом їхнього відтворення без обмежень, доопрацювання, удосконалення, переробки та створення інших творів (комп'ютерних програм), в тому числі похідних, з використанням комп'ютерних програм без можливості розкриття, оприлюднення чи розголошення отриманого від Організатора вихідного коду комп'ютерних програм та технічної документації третім особам.

11.5. Відповідальність за розголошення КІ. У випадку порушення Учасником умов про нерозголошення КІ Учасник, зобов'язується протягом 3 (трьох) днів з дати отримання відповідного повідомлення від Організатора, сплатити штраф в розмірі 1000 000,00 (один мільйон) гривень. При цьому сплата штрафу не звільняє Учасника від належного виконання своїх зобов'язань і повного відшкодування завданих збитків.

12. ПОРЯДОК РОЗКРИТТЯ МАТЕРІАЛІВ ХАКАТОНУ (DISCLOSING SUBMISSIONS)

12.1. Будь-яке розкриття, розголошення, публікація матеріалів та результатів Хакатону, що стосуються вразливостей мобільного застосунку monobank, можливе виключно за письмовим погодженням з Організатором.