(048) 770 10 70
Одесса, ул. Жуковского, 41

Програма Inweb з винагороди білих хакерів

Ми цінуємо увагу до нашого агентства, дбаємо про безпеку даних користувачів і завжди вдячні за допомогу. Дякуємо, що зайшли на сторінку про програму винагороди за знайдені недоліки в роботі inweb.ua.

Якщо ви помітили проблему в роботі сайту, будь ласка, напишіть нам. Але перш переконайтеся, що вона входить до переліку тих, про які нам варто знати, і у вас є всі дані, щоб повідомити нам (деталі в розділі «Як повідомити про проблему» нижче). Якщо недолік дійсно загрожує безпеці даних користувачів Inweb, ми з радістю усунемо його, а вам — виплатимо нагороду.

Рекомендуємо звернути особливу увагу на політику розкриття інформації.

Як повідомити про проблему

- Детально опишіть виявлену вразливість.
- Прикладіть приклади того, як «працює» несправність (використовуючи скриншоти, запис екрану).
- Опишіть список інструментів, яким ви користувалися для виявлення проблеми (наприклад, браузер, версія, сканер безпеки та інше).
- Всю інформацію надішліть на safety@inweb.ua.

Про проблему можна писати в тілі листа або в будь-якому, зручному вам, документі. Якщо ваш звіт буде містити дані, описані вище, можете бути впевнені — він не залишиться поза нашою увагою. В іншому випадку ми можемо його не аналізувати.

Як проходить аналіз звітів про проблему

- Ми вивчаємо всі правильно складені звіти.
- Визначимо пріоритетність.
- У разі, якщо знайдена проблема дійсно загрожує безпеці даних — усунемо її.
- Вам виплатимо нагороду.

Враховуйте, що нам потрібен час для вивчення вашого звернення. Ми залишаємо за собою право публікувати звіти.

Політика відповідального розкриття інформації

Коли будете повідомляти про проблеми, дотримуйтеся наступних рекомендацій, щоб уникнути ініціювання судових позовів проти вас і залучення правоохоронних органів для розслідування:

- Ні в якому разі не використовуйте виявлену проблему в системі безпеки в будь-яких цілях (в тому числі для демонстрації додаткових ризиків, включаючи спроби розкрити конфіденційні дані компанії або знайти інші проблеми).
- Уникайте порушень конфіденційності даних і роботи інших людей, в тому числі серед іншого, несанкціонованого доступу до даних, знищення даних і переривання або погіршення роботи нашого сайту.
- Надайте нам достатньо часу на аналіз і усунення проблеми, перш ніж опублікувати свій звіт у відкритому доступі або ділитися цією інформацією з іншими.
- Утримуйтеся від навмисних порушень будь-яких інших чинних законів або норм, в тому числі серед іншого, законів і норм, що забороняють несанкціонований доступ до даних.

Про розмір винагороди

Максимальна сума за одну знайдену проблему становить 50 доларів США.
Ми виплачуємо винагороду тільки в тому випадку, якщо це не суперечить чинному законодавству.
За виявлення проблем з дуже низьким рівнем ризику винагорода може не надаватися зовсім.
Одна винагорода виплачується тільки одній людині.

Проблеми, на які програма винагороди не поширюється

- Спам і техніки соціальної інженерії.
- Атаки на кшталт «відмова в обслуговуванні».
- Робота з інтегрованими сервісами.
- Помилкові результати.

(048) 770 10 70
Одесса, ул. Жуковского, 41

Программа Inweb по вознаграждению белых хакеров

Мы ценим внимание к нашему агентству, заботимся о безопасности данных пользователей и всегда благодарим за помощь. Спасибо, что зашли на страницу о программе вознаграждения за найденные недочеты в работе inweb.ua.

Если вы заметили проблему в работе сайта, пожалуйста, напишите нам. Но прежде убедитесь, что она входит в перечень тех, о которых нам стоит знать, и у вас есть все данные, чтобы сообщить нам (детали в разделе «Как сообщить о проблеме» — ниже). Если недочет действительно угрожает безопасности данных пользователей Inweb, мы с радостью устраним его, а вас — вознаградим.

Рекомендуем обратить особое внимание на политику раскрытия информации.

Как сообщить о проблеме

- Подробно опишите обнаруженную уязвимость.
- Приложите примеры того, как «работает» неисправность (используя скриншоты, запись экрана).
- Опишите список инструментов, которым вы пользовались для обнаружения проблемы (например, браузер, версия, сканер безопасности и тд).
- Всю информацию пришлите на safety@inweb.ua.

О проблеме можно писать в теле письма или в любом, удобном вам, документе. Если ваш отчет будет содержать данные, описанные выше, можете быть уверены — он не останется без нашего внимания. В противном случае мы можем его не анализировать.

Как проходит анализ отчетов о проблеме

- Мы изучим все правильно составленные отчеты.
- Определим приоритетность.
- В случае, если найденная проблема действительно угрожает безопасности данных — устраним ее.
- Вам выдадим вознаграждение.

Учитывайте, что нам нужно время для изучения вашего обращения. Мы оставляем за собой право публиковать отчеты.

Политика ответственного раскрытия информации

Когда будете сообщать о проблеме, придерживайтесь следующих рекомендаций, чтобы избежать инициирования судебных исков против вас и привлечения правоохранительных органов для расследования:

- Ни при каких обстоятельствах не используйте обнаруженную проблему в системе безопасности в каких-либо целях (в т. ч. для демонстрации дополнительных рисков, включая попытки раскрыть конфиденциальные данные компании или найти другие проблемы).
- Избегайте нарушений конфиденциальности данных и работы других людей, в т. ч., среди прочего, несанкционированного доступа к данным, уничтожения данных и прерывания или ухудшения работы нашего сайта.
- Предоставьте нам достаточно времени на анализ и устранение проблемы, прежде чем публиковать свой отчет в открытом доступе или делиться этой информацией с другими.
- Воздерживайтесь от намеренных нарушений любых других применимых законов или норм, в т. ч., среди прочего, законов и норм, запрещающих несанкционированный доступ к данным.

О размере вознаграждения

Максимальная сумма за одну найденную проблему составляет 50 долларов США.
Мы выплачиваем вознаграждение только в том случае, если это не противоречит действующим законам.
За выявление проблем с очень низким уровнем риска вознаграждение может не предоставляться вовсе.
Одно вознаграждение выплачивается только одному человеку.

Проблемы, на которые программа вознаграждения не распространяется

- Спам и техники социальной инженерии.
- Атаки по типу «отказ в обслуживании».
- Работа с интегрированными сервисами.
- Ошибочные результаты.

(048) 770 10 70
Одесса, ул. Жуковского, 41

Inweb white hat bounty program

We appreciate the attention to our agency, we care about the security of user data and always thank you for your help. Thank you for visiting the Reward program for flaws and loopholes found in the work of Inweb.ua.

If you notice a problem with the site, please write to us. But first, make sure that it is on the list of those that we should know about, and that you have all the data to tell us (details in the section "How to report a problem" - below). If a flaw really threatens the security of Inweb users' data, we will gladly fix it, and we will reward you.

We recommend that you pay special attention to the Information disclosure policy.

How to report a problem

- Describe the vulnerability that you have found in detail.
- Attach examples of how the loophole “works” (using screenshots, screen recording, etc.).
- Describe the list of tools that you used to find the problem (for example, browser, version, security scanner, etc.).
- Send all information to safety@inweb.ua.

You can write about the problem in the body of the letter or in any document that is convenient for you. If your report contains the data described above, you can be sure that it will not be left without our attention. Otherwise, we may not analyze it.

How problem reports are analyzed

- We will review all correctly prepared reports.
- Then we`ll define the priority.
- If the problem found really threatens data security, we will eliminate it.
- We will give you a reward.

Please note that we need time to review your appeal. We reserve the right to publish reports.

Information disclosure policy

When reporting an issue, follow these guidelines to avoid taking legal action against you and bringing law enforcement to investigate:

- Do not under any circumstances use the detected security issue for any purpose (including to demonstrate additional risks, attempts to disclose confidential company data or find other problems).
- Avoid breaching the confidentiality of data and the work of others, including, but not limited to, unauthorized access to data, data destruction, and interruption or degradation of our website.

- Allow us sufficient time to analyze and resolve the issue before publishing your report to the public or sharing this information with others.
- Refrain from knowingly violating any other applicable laws or regulations, including, but not limited to, laws and regulations that prohibit unauthorized access to data.

About the amount of the reward

The maximum reward amount for one problem found is $ 50.
We pay reward only if it does not contradict applicable laws.
There may be no reward at all for identifying very low-risk issues.
One reward is paid to only one person.

Issues not covered by the bounty program:

- Spam and social engineering techniques.
- “Denial of service” attacks.
- Working with integrated services.
- Erroneous results.