# Вступ

E-corp дуже серйозно ставиться до безпеки своїх систем та приватності клієнтів, але ми усвідомлюємо, що наші зусилля з захисту ввірених нам секретів потребують зовнішньої незалежної перевірки. З цією метою E-corp регулярно замовляє повномасштабні тести на проникнення (Penetration Tests) у найдосвідченіших та найбільш кваліфікованих постачальників таких послуг. Але разом з тим, ми розуміємо, що періодичного незалежного тестування недостатньо для повної впевненості в найвищому можливому рівні захисту.

Саме тому, E-corp прийняла рішення щодо поліпшення рівня захищеності системи шляхом надання дозволу на дослідження вразливостей її систем усіма бажаючими, за умови додержання учасниками правил відповідального розкриття інформації про вразливості (Responsible Disclosure).

З цією метою E-corp розробив та опублікував цю Програму повідомлення про вразливості, кожен учасник якої може взяти участь у процесі підвищення рівня безпеки систем, що мають велике суспільне та економічне значення.

E-corp залишає за собою право змінювати умови цієї Програми. Будь ласка, слідкуйте за оновленнями.

# Винагорода

Ця Програма використовує стандартні положення BugCrowd Vulnerability Rating Taxonomy (<https://bugcrowd.com/vulnerability-rating-taxonomy>) для визначення рівня ризику знайдених вразливостей.

Учасники Програми можуть розраховувати на матеріальну винагороду за перевірені вразливості, знайдені в системах в Області дії. Форма винагороди: грошова премія та внесення імені або псевдоніму учасника у Зал слави Програми на офіційному веб-сайті системи: <https://bounty.e-corp.com.ua>

Розмір винагороди:

|  |  |
| --- | --- |
| **Priority (VRT)** | **Bounty, USD** |
| P1 | 500-1000 |
| P2 | 250-500 |
| P3 | 150-250 |
| P4 | 50-150 |
| P5 | Не винагороджується |

У випадках знайдення вразливості критичного рівня ризику, E-corp залишає за собою право збільшити розмір виплати відповідно до важливості знахідки. Також, E-corp робить деякі виключення з вразливостей, які можуть претендувати на винагороду. Докладніше дивіться розділ Пріоритети.

# Пріоритети

E-corp найбільше зацікавлена в отриманні звітів щодо таких вразливостей:

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

E-corp навмисно виключає такі вразливості з Програми:

* **Accessible non-sensitive files and directories**
* **Descriptive non-sensitive error messages**
* **Potential for social engineering and phishing attacks**
* **Potential for dictionary or brute force password attacks**
* **Potential for Denial of Service attacks**
* **Email/username enumeration**
* **Self XSS**
* **Text injection**
* **Email spoofing**
* **Fingerprinting of public services**
* **Clickjacking and issues only exploitable through clickjacking**
* **Low-impact CSRF, such as logout or publicly available forms**
* **Lack of Secure and HTTPOnly cookie flags**
* **Lack of HTTP security headers**
* **HTTPS mixed content**
* **Low risk SSL/TLS issues**
* **Out-of-date software versions**

Всі перелічені вразливості-виключення може бути винагороджено в разі їх присутності в критичних системах або демонстрації дослідником високого рівня відповідного ризику.

# Область дії та виключення

Дозвіл щодо здійснення дослідження вразливостей поширюється на такі домени, що знаходяться у розпорядженні E-corp:

**\*.e-corp.com.ua**

Дозвіл ***не поширюється*** на такі домени, які E-corp орендує у відповідних постачальників послуг:

**support.e-corp.com.ua  
crm.e-corp.com.ua  
marketing.e-corp.com.ua  
mail.e-corp.com.ua  
autodiscover.e-corp.com.ua**

У разі виникнення запитань щодо належності системи E-corp до області дії Програми, будь ласка, зверніться до нас по роз’яснення.

# Контакти

<https://security.e-corp.com.ua>   
[security@e-corp.com.ua](mailto:security@e-corp.com.ua)  
[bounty@e-corp.com.ua](mailto:bounty@e-corp.com.ua)

# Умови та обмеження

Програма встановлює такі умови:

* Винагороду отримує перший дослідник, який повідомив про вразливість.
* Вразливість повинна існувати в актуальній версії системи.
* Дослідник повинен надати фактичні докази існування вразливості (Proof of Concept) у формі текстового опису кроків відтворення вразливості, порцій мережевого трафіку або HTTP сесій, знімків екрану та/або відео демонстрації.
* Дослідник повинен повідомити про вразливість власнику системи та додержатися умов відповідального розкриття інформації: публічне розкриття інформації про вразливість дозволяється лише після її виправлення та повинно бути узгоджене з власником.
* Дослідник повинен надати додаткові відомості про вразливість, які можуть знадобитися власнику системи для її виправлення. Також, дослідник повинен здійснити перевірку виправлення вразливості в разі отримання такого звернення від власника системи.
* Дослідник повинен додержуватися норм етичної поведінки: використовувати лише тестові облікові записи, що належать досліднику, а також утримуватися від отримання доступу до чутливих даних та облікових записів інших користувачів.

Дослідникам забороняється здійснювати атаки відмови в обслуговуванні (DoS/DDoS) на системи в Області дії, а також використовувати системи автоматичного тестування, які генерують масивні об’єми мережевого трафіку та можуть вплинути на працездатність систем.

Працівники та підрядники E-corp, та інші особи, які могли брати участь в розробці та підтримці систем в Області дії, не мають права брати участь в цій Програмі.

# Форма звіту

1. Назва вразливості.
2. Класифікація вразливості згідно з VRT.
3. Суб’єктивна оцінка рівня ризику вразливості.
4. Пояснення щодо рівня ризику (необов'язково).
5. Демонстрація вразливості.

* Опис кроків з відтворення вразливості.
* HTTP-сесії, що демонструють вразливість.
* Знімки екрану, що демонструють вразливість.
* Відео-демонстрація відтворення вразливості (необов'язково).

# Доступ до систем

Доступ до систем, які дозволяють публічну реєстрацію користувачів, здійснюється із спеціальними обліковими записами, сформованими за схемою:

**username+hacker@e-corp.com.ua**