

Ultra-Coins での活動状況

2026-07-21 細島涼雅

@Ultra-Coins 総会

自己紹介

- 細島涼雅(ほそじまりょうが)
 - 情報科学類 B4
 - 言語処理系 / セキュリティ / GPGPU に興味があります
 - HCI の研究をしています
 - HPC の研究も少ししています

Ultra-Coins 入室により得られるもの

- 部屋
- 24h 稼働なマシン
- グローバル IP

特にグローバル IP があると、様々なことができる

Ultra-Coins 設置機材を活用した CTF への参加

- [IERAE CTF 2024] Great Management Opener
- [SECCON CTF 14 Quals] broken-challenge

これらの問題などで、Ultra-Coins に設置した機材およびグローバル IP を活用した。

例1:[IERAE CTF 2024] Great Management Opener

基本的な認証認可を備えたサービスがある

HTML のインジェクションが可能 & CSPにより外部とインラインのJavaScript実行は制限され、CSSは許容されている

→ CSS injection によりCSRF対策トークンを窃取し、CSRFを行う。

例2:[SECCON CTF 14 Quals] broken-challenge

Signed HTTP Exchanges(SXG) を行う問題

署名されたHTTPレスポンス(とそのリクエストURL)を含むパッケージを返すことで、全く異なるオリジンのコンテンツであっても、そのオリジンから配信されたかのように振る舞う

just for fun...?

Ultra-Coins 設置機材を活用した脆弱性調査

最近、とある大きなウェブアプリケーションにおける脆弱性を発見した。

脆弱性については然るべき機関を通じて報告済み。

調査・脆弱性の確認 (PoC) において、Ultra-Coins の設置機材とグローバル IP を活用した。

発見した脆弱性

※ 2026/07/21 時点でコードの修正が行われていることは確認したものの、まだ連絡が来ていないため、具体的なソフトウェア、報告した脆弱性については言及できません。

とある電子メールサービス

メールに対してサニタイザがいるが、とある入力によりバイパスが可能。

被害者がメールを開くだけで個人情報が流出する。

検証には Ultra-Coins に設置した機材 & グローバル IP を活用

発見した脆弱性

※ 2026/07/21 時点でコードの修正が行われていることは確認したものの、まだ連絡が来ていないため、具体的なソフトウェア、報告した脆弱性については言及できません。

とある電子メールサーバー

メールに対してサニ

Bounty ???? \$

能。

被害者がメールを開くだけで個人情報流出する。

Profit!

検証には Ultra-Coins に設置した機材 & グローバル IP アドレス

まとめ

- Ultra-Coins の環境は Web CTF においてかなり有利である
- 脆弱性調査も柔軟に行えて便利
- いろんなことができて嬉しい

Ultra-Coins for fun and profit