

バグバウンティを用いた課題解決

株式会社フォーゼット
蒨 綾人

自己紹介: 部 綾人

Hacker / Pentester

2004年札幌生まれ

ベトナム Duy Tan大学 / レッドチーム講師

株式会社フォーゼット / Hacker

株式会社網屋 札幌研究所 / リサーチャー

得意分野: WEB・Linux・OSINT



バグバウンティ等の実績

IssueHunt 月間ランキング1位(2024年3月)

バグバウンティ累計報告数約25件

ゼロデイ攻撃発見数 20件

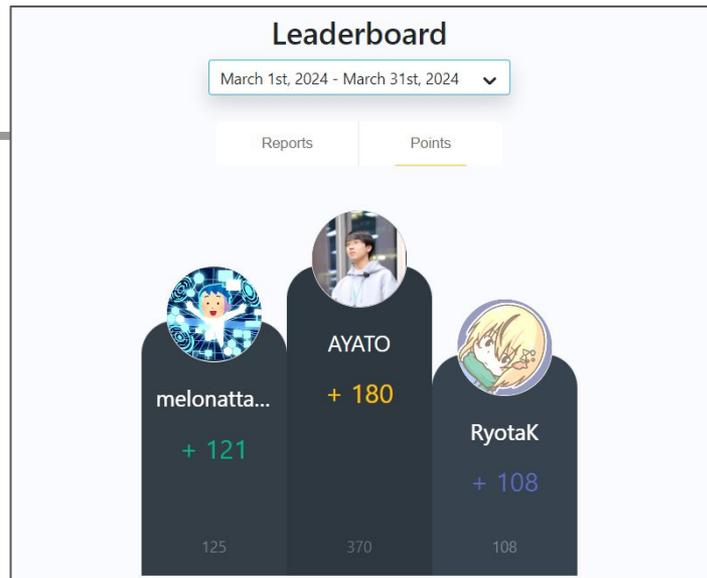
共通脆弱性識別子(CVE)

CVE-2024-46278 ファイル共有ソフト「Teedy」における格納型XSS

CVE-2024-47158 教習システム「N-LINE」におけるHTMLインジェクション

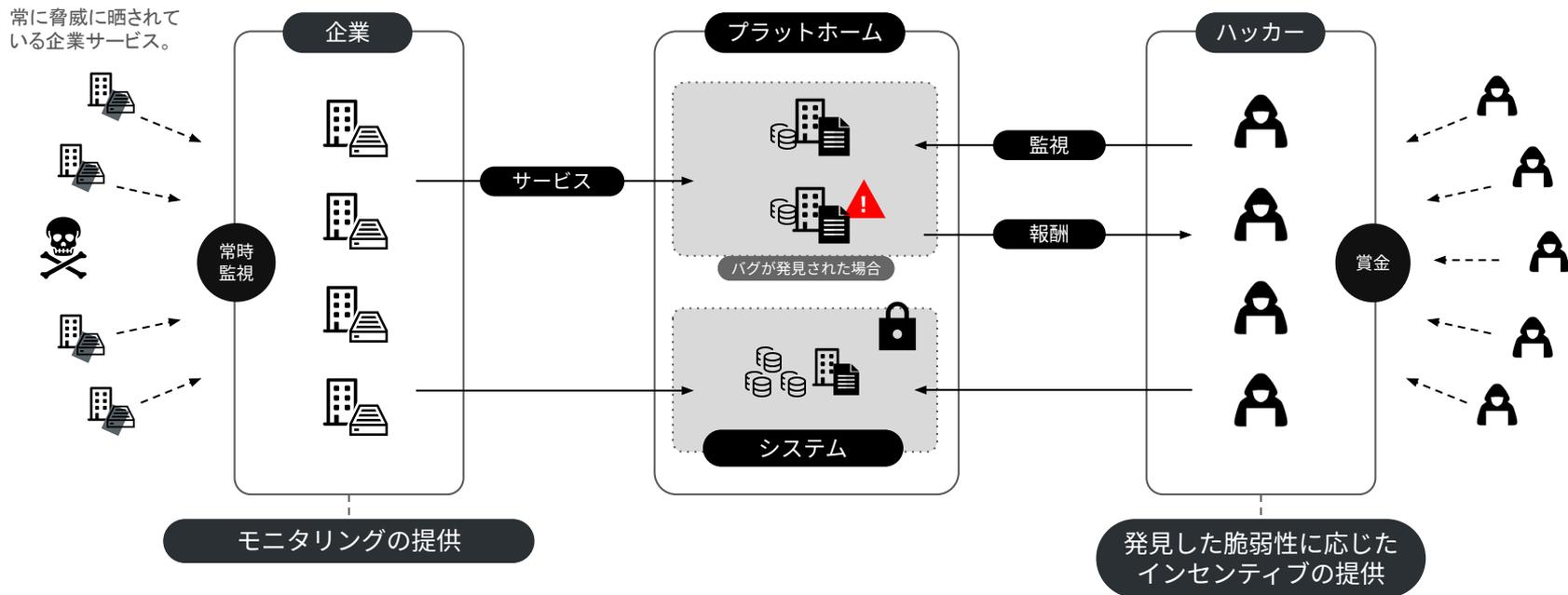
CVE-2024-46998 国産CMS「Baser CMS」における格納型XSS

CVE-2024-46996 国産CMS「Baser CMS」における格納型XSS



バグバウンティとは

👉 善意を持ったハッカーが企業の穴を見つけしてくれる プラットフォーム



代表的なバグバウンティプラットフォーム

HackerOne 世界最大のプラットフォーム

Google Bug Hunters Googleが運営する自社製品に対するプラットフォーム

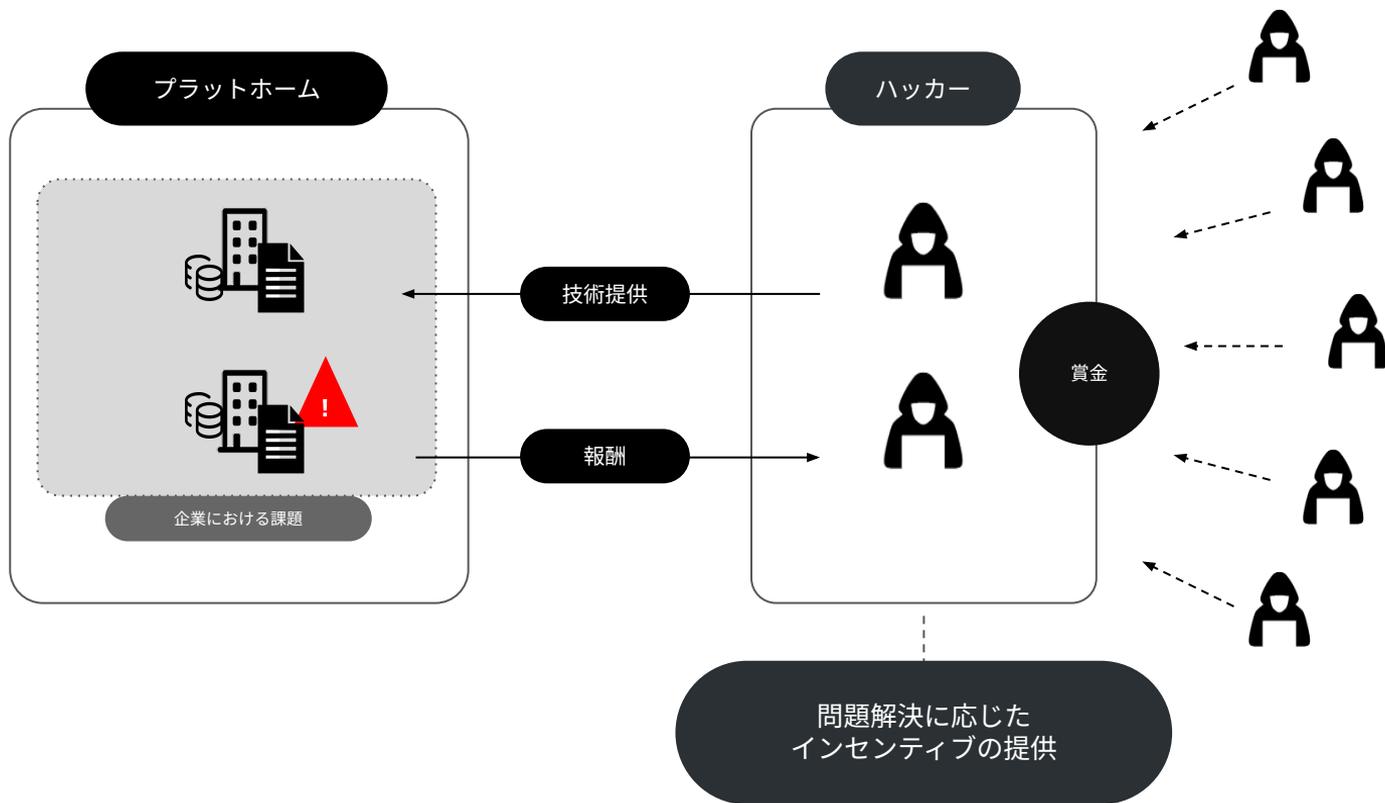
IssueHunt 日本企業向けプラットフォーム

ZoneZero 株式会社フォーアセットが提供するプラットフォーム

hackerone



ハッカーの力を借りて問題を解決する



例1)パスワードを忘れたzipファイルの解析

ハッカーに
ハッカーにフ
忘れたパス

```
(ayato@ayato) ~$ zip2johnn  
ver 1.0 efh  
b chk, TS_ch  
=8042 type=0  
  
(ayato@ayato) ~$ cat hash  
secret.zip/s  
042*40e8cb22  
t.txt:secret
```

ZONE ZERO ダッシュボード プログラム ランキング プロフィール 支払い 通知

株式会社フォアセット

特別プログラム [脆弱性を報告](#)

報酬が支払われた件数 3

平均支払額 (全期間) ¥254,200

対象範囲の数 2

今までの最大報酬 ¥300,000

プログラム情報 対象範囲 お知らせ/更新 アクティビティ レポート履歴

以下のURLに格納されているハッシュ値を解析してください

いずれのハッシュ値も報奨金プログラムの対象となります。

Program Rules

Our main rules are as follows:

例2)マルウェア解析

ハッカーにマルウェアを解析してもらう

解析業務のアウトソーシング

専門家が社内にいる必要がない

特にIoT、ブロックチェーンなど

マイナーな技術に対する策

The screenshot shows the ZONE ZERO dashboard for株式会社フォアゼット (Foreaset Co., Ltd.). The dashboard includes a navigation menu with options like ダッシュボード (Dashboard), プログラム (Program), ランキング (Ranking), プロフィール (Profile), 支払い (Payment), and a notification bell. The main content area is titled "株式会社フォアゼット" and "マルウェア解析プログラム" (Malware Analysis Program). A purple button labeled "脆弱性を報告" (Report Vulnerability) is visible. Below the title, there are several key metrics:

- 報酬が支払われた件数 (Number of payments made): 32
- 平均支払額 (全期間) (Average payment amount (all periods)): ¥474,000
- 対象範囲の数 (Number of target ranges): 2
- 今までの最大報酬 ¥600,000 (Maximum payment so far: ¥600,000)

The "プログラム情報" (Program Information) tab is active, displaying the following text: "以下のURLからIoT向けマルウェアの検体を取得して、C2サーバーに関する情報を取得・解析してください。ただしC2サーバーの解析に関して、対象範囲における要件を満たしてください。" (Obtain IoT malware samples from the following URLs, and obtain and analyze information related to C2 servers. However, regarding C2 server analysis, please meet the requirements in the target range.)

Below this text, there is a red bar. At the bottom of the dashboard, the "Program Rules" section is visible, stating: "Our main rules are as follows:"

まとめ:バグバウンティの導入後の拡張性

必要とする技術をスポットで利用することが可能

→ マイナーや超高度な技術に対するエンジニアの雇用が不要

成果ベースで成績が見える

→ 優秀な人材の発見が簡単に可能