Competitor Analysis Report:
PlexTrac and Cobalt's multi-tenant Functionality

Overview

The purpose of this report is to assess the multi-tenant functionality of PlexTrac and Cobalt, two competing products, in order to identify their key features for administrators and users, and to evaluate their approaches to handling multiple tenants. This will offer insights into our product "Capture the Bug", highlighting areas where we can adopt or improve upon.

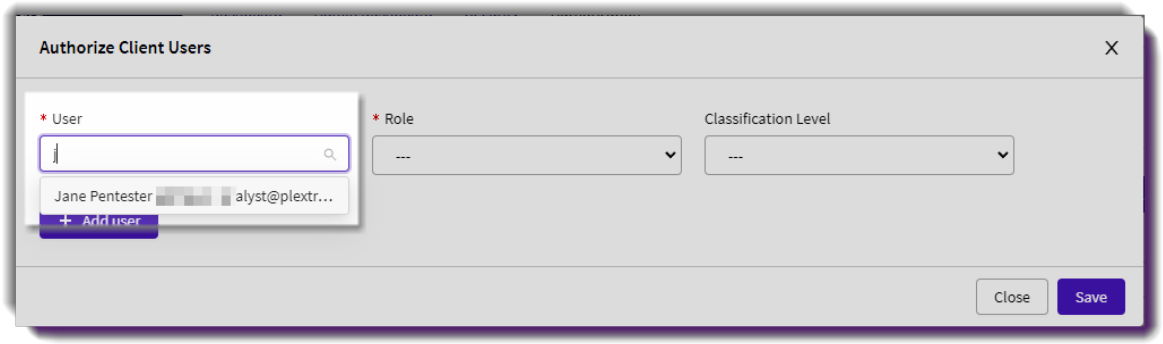
PlexTrac's Multi-Tenant Functionality Analysis

PlexTrac is a platform that assists cybersecurity teams in enhancing and centrally managing entire lifecycle workflows. It streamlines processes from preparation for offensive engagement, execution of evaluations, data analysis, reporting, prioritisation of critical issues, collaboration between teams, to communication with stakeholders.

Functional Modules:

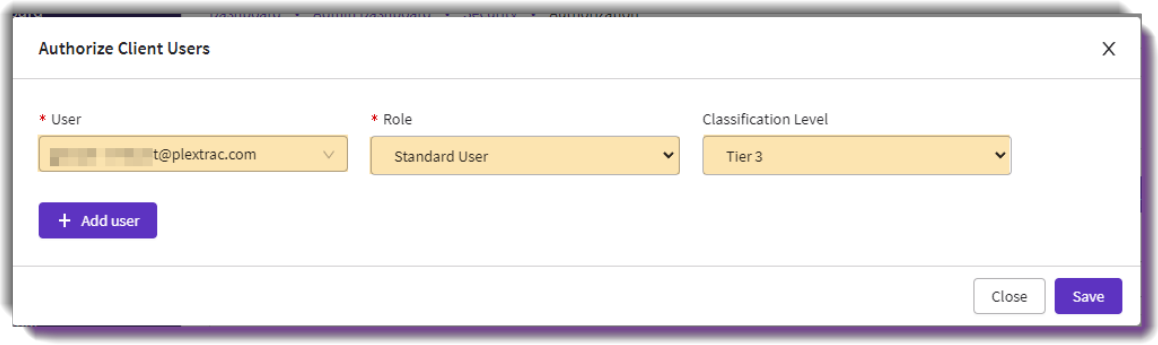
- Dashboard: The page users see first after logging in.
- Clients: Manage client information.
- Assessments: Conduct security assessments.
- Reports: Generate and view security reports.
- Priorities: Determine the priorities of tasks.
- Content Library: Store and manage security testing content.
- Analytics: Provide data analysis functions.
- Runbooks: Manuals that guide security operations.

- Adding Users to a Client by authorization page



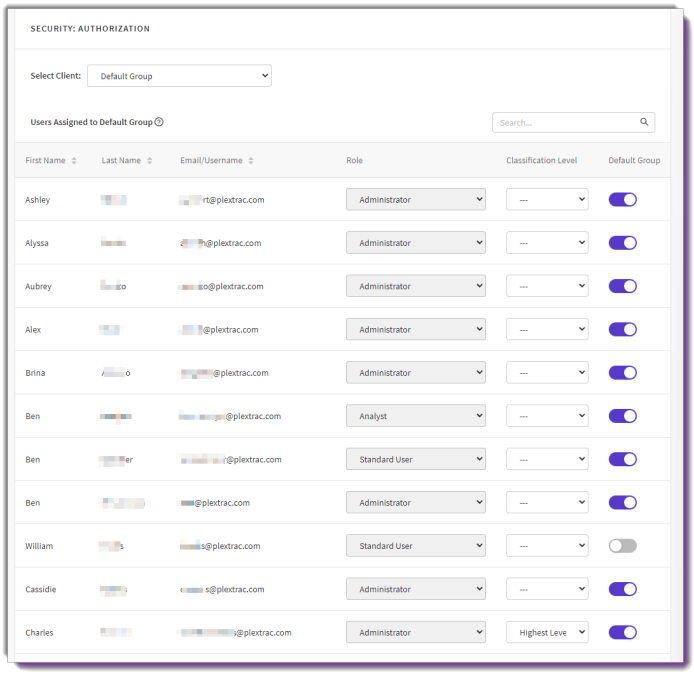
(Plextrac, n.d.)

- Assigning a role from the pull-down menu while authorizing an user.



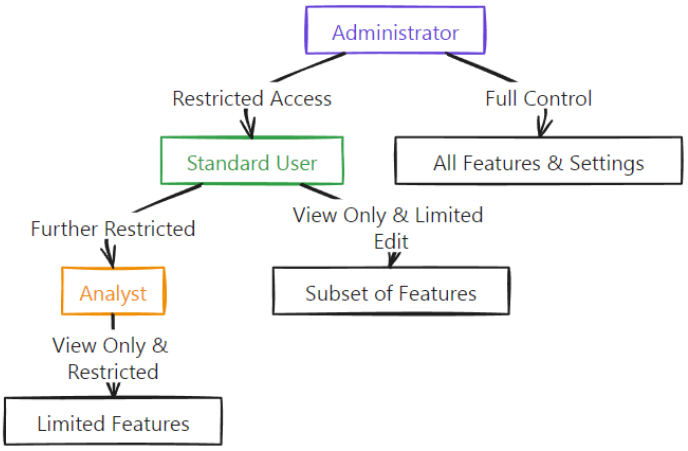
(Plextrac, n.d.)

- Managing Roles at authorization



(Plextrac, n.d.)

User Types



(Plextrac, n.d.)

PlexTrac supports two primary user types for business: standard users and administrators. Standard users have basic access necessary for performing daily tasks, whereas administrators possess broader permissions that allow them to manage tenant settings, user accounts, and advanced configuration options. This distinction helps maintain effective separation between operational and management aspects of the system, contributing to both security and operational efficiency.

Account Management

- Tenant Creation and Organisation: Administrators have the capability to create and organise multiple tenants hierarchically. This allows for efficient management of either clients or internal departments, ensuring each unit operates independently while maintaining a clear overall organisational structure.
- Customisation: Each tenant can be tailored with specific settings, branding, and integrations to meet unique operational requirements. This level of customization allows different tenants to have distinct appearances and functionalities tailored to their specific needs.
- User Management: Admins can add, remove, and manage users within each tenant, controlling access levels and permissions. This ensures precise control over access to sensitive data and simplifies the management process by providing a clear framework for user operations within the tenant.

Assignments and Roles

The *differences* between Standard User and Administrator roles:

- No access to Administration Access
- No access to Account information
- No access to Custom Templates
- No access to Email Settings
- No access to General Settings
- No access to Integration Settings
- No access to Parser Actions
- No access to License Management
- No access to Security
- No access to Style Guides
- No access to Tags Management
- View only permissions for client users (cannot create or delete client users)
- View only permissions on Customizations (cannot credit, edit, or remove)
- Cannot manage repositories in the Content Library
- View only ability on Priorities (cannot create, delete or edit)
- View only ability on priority scoring equations (cannot create, delete, or edit)

(Plextrac, n.d.)

- Role-Based Access Control: Specific roles are assigned to users, determining their access and functionalities within the system. This not only enhances security but also provides flexibility as administrators can adjust roles and permissions based on actual needs.
- Permissions: Detailed permission settings ensure that users access only the necessary information, thereby enhancing security and compliance. These permissions can be finely tuned to specific actions and data sets, ensuring each user's activities conform to the organization's security policies.

Relevance to Capture the Bug:

- **Customization and Hierarchical Management**: Adopting a similar approach can enhance scalability and user management in "Capture the Bug."
- **Role-Based Access Control**: Incorporate detailed roles and permissions to improve security and flexibility.

Cobalt's Multi-Tenant Functionality Analysis

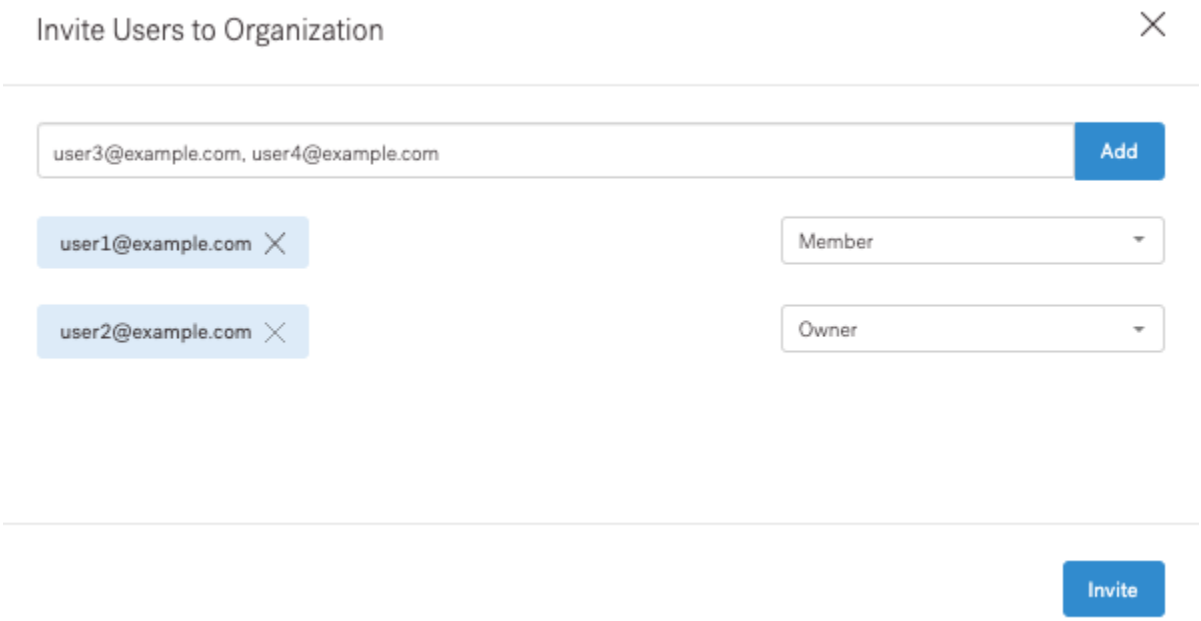
Cobalt provides a Pentest Management Platform that caters to both external and internal cybersecurity needs. The system is designed to support multiple roles, enhancing collaborative and individual testing efforts.

Functional Modules:

- **Pentests:** Setup and manage penetration tests.
- **Assets:** Define and organise assets for security testing.
- **Findings:** Document and track security vulnerabilities.
- **Reports:** Generate detailed security reports.
- **Integrations:** Connect with other tools like JIRA and GitHub.

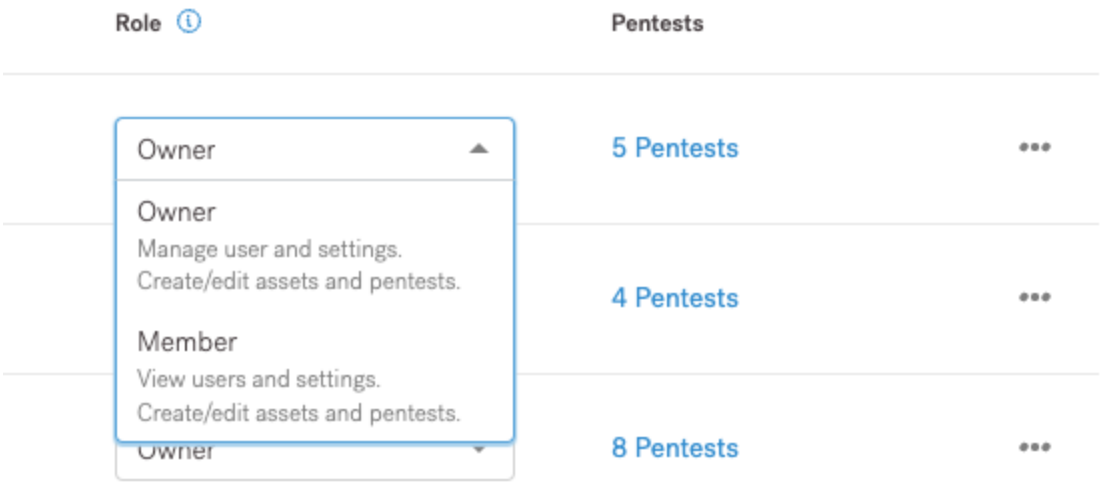
Joel:

- Invite users to the organization through email



(Cobalt, n.d.)

- Adding users by "Security & User Management"
- Change a user's role



(Cobalt, n.d.)

- Remove Users
- Manage Pentest Collaborators

User Types

There are three user types in Cobalt platform:

a. User Roles

- **Pentest Level:**
  - **Pentest Team Member:** Engages specifically in pentests, limited access to organizational settings unless combined with higher-level roles.
- **Organization Level:**

Permission	Organization Member	Organization Owner
Create assets and pentests, edit assets	✓	✓
Change the group an asset is associated with	–	✓
View all findings reported within an organization on the **Findings** page, within group permissions	✓	✓
View organization users and pentest collaborators on the **People** page	✓	✓
Manage integrations for an organization	✓	✓
Edit the organization profile	✓	✓
View the credits ledger	✓	✓
View the Insights page	✓	✓
Manage users for an organization	–	✓
Create and manage groups	–	✓
Manage security settings for an organization: two-factor authentication and SAML	–	✓
Enable co-branded reports (for Cobalt partners)	–	✓

(Cobalt, n.d.)

    - **Organization Owner:** Manages assets, user settings, and has comprehensive control over organizational configurations and pentests.
    - **Organization Member:** Participates in asset and pentest management with visibility into organizational settings but restricted control compared to the owner.
- **Pentest + Organization Level:**
    - Merges responsibilities across pentesting and organizational management, allowing for dual capabilities in managing settings and active pentests.

b. Pentester Roles:

- **Cobalt Pentesters:** Directly involved in conducting pentests for clients.
- **Customer Pentesters:** In-House Pentesters performing tests specifically for their organization.

c. Administrative Role:

- **Cobalt Staff:** Holds administrative oversight across the platform, supporting both organizational and pentest operations.

Comparison

Plextrac enhances operational efficiency by clearly differentiating the roles and access between standard users and administrators, ensuring only authorised personnel handle administrative tasks. This structure helps maintain a simple and effective user interface for regular users.

Cobalt employs a comprehensive role system that spans organizational and operational levels, offering detailed permissions tailored to specific roles such as Pentest Team Member, Organization Owner, and Organization Member, thereby supporting complex pentesting activities.

Recommendations for Capture the Bug

- **Defining Clear Roles and Permissions:** Establishing clear and distinct roles within the system, much like Plextrac's division between standard users and administrators, while considering Cobalt's approach to detailed role-based access at both organizational and operational levels.
- **Customising Access Control:** Implementing robust access control mechanisms that allow for customization depending on the role, ensuring that each user has access to the necessary tools and information for their specific responsibilities without compromising security.
- **Integration and Collaboration Tools**: Cobalt's integration strategies could be leveraged to boost collaborative efforts within "Capture the Bug."

Plextrac and Cobalt both have a Role Based Access (RBAC) approach to control over permissions for different roles. However, Cobalt's RBAC is more complicated and more suitable for clients who are large-scale organization. At this stage, we might only need to consider user roles at organization level, which is similar to Plextrax's RBAC approach.

Conclusion

PlexTrac and Cobalt showcase robust functionalities that can benefit the development of multi-tenant feature for Capture the Bug. By adopting those key features including Plextrac's customization features and Cobalt's detailed role-based system, we can significantly enhance user experience and administrative efficiency for Capture the Bug. We believe these adaptations will ensure that the platform meets current market standards.

Reference List

Plextrac. (n.d.). *Role-Based Access Control (RBAC)*. In *Plextrac Documentation*. Retrieved August 13, 2024, from https://docs.plextrac.com/plextrac-documentation/product-documentation-1/account-management/account-admin/security-and-user-management/rbac

Cobalt. (n.d.). *Manage users: Invite users*. In *Cobalt Documentation*. Retrieved August 13, 2024, from https://docs.cobalt.io/platform-deep-dive/organization/manage-users/#invite-users