EBC Web based 'v' OWASP application

Q - Is Passtrack is a web application, is it OWASP compliant?

- Passtrack is a web based appication. Not 'Open Worldwide Application Security Project' defined

Q - Supporting Answer.

To manage Appication security we depoly standard and recommended security protocols including

- DDoS mitigation
  - DDoS mitigation services between the server and the public Internet, using specialized filtration and extremely high bandwidth capacity to prevent surges of malicious traffic from overwhelming the server. These services are filter and remove malicious traffic
- Web Application Firewall (WAF):
  - Filtration of traffic known or suspected to be taking advantage of web application vulnerabilities.
  - These WAFs address new vulnerabilities
- API gateways
  - Identifies 'shadow APIs,' and blocks traffic known or suspected to target API vulnerabilities.
  - They also manage and monitor our API traffic
- DNSSEC:
  - This protocol guarantees our web application's DNS traffic is safely routed to the correct servers, so our users are are not intercepted by an on-path attacker.
- Encryption certificate management:
  - A third party manages key elements of the SSL/TLS encryption process, such as generating private keys, renewing certificates, and revoking certificates due to vulnerabilities.
  - This removes the risk of those elements going overlooked and exposing private traffic
- Bot management:
  - Small elements of machine learning and other specialized detection methods to distinguish automated traffic from human users, and prevent the former from accessing a web application.
- Client-side security:
  - We check for new third-party JavaScript dependencies and third-party code changes, which helps to catch any malicious activity quickly
- Attack surface management:
  - We have implemented some attack surface management tools to identify potential security risks, and mitigate risks with minimal operational activity

1. Q - **2FA**: The "System does support 2 factor authentication,
2. Q - **Audit trails:** including logs of all user, client and candidate activity. "Limited audit functionality. Plans to improve this in Q3 to capture all transactional activity and store for 7 days". Are there any plans to increase the stored duration of the logs as even 7 days may be too late to investigate once an issue becomes known and may be insufficient for effective accountability given the sensitive nature of the data?
   - *A – Comment noted and agreed. We will look to increase the Audit storage duration as a standard default setting of 6 months*
3. Q - **Encryption:** Please confirm algorithm used for data at rest and during transfer (AES-128 or AES-256)?
   - *A – AES-128 for 128-Bit key length for encryption, decryption and at rest storage*
4. Q - **Role-based access:** While the system does not support role-based access, is there an admin / super user role that can only make configuration changes, such as KPIs / reports (or are these not possible)?

- *A – Yes. The system has user and Admin (super user) access levels as standard*
- *Super user is sole authority for user access level control and configuration management*