Security Built-in

Modified on: Fri, 22 Jan, 2021 at 2:49 PM

Security

DNS Level

- Zone lockout for protected parts of the Exchange such as Admin Panel
- Anti-DDOS protection using HTTP Flood, UDP Flood, TCP Flood, Error based Detection, and QUIC Flood.
- Automatic HTTPS writes helps fix mixed content by changing “http” to “https” for all resources or links on your web site that can be served with HTTPS.
- Use of DNSSEC that protects against forged DNS answers. DNSSEC protected zones are cryptographically signed to ensure the DNS records received are identical to the DNS records published by the domain owner.
- SSL/TLS certificates at origin to provide End to End Encryption
- HTTP Strict Transport Security (HSTS)
    - Status: On, Serves HSTS headers with all HTTPS requests
    - Max-Age: 1 month, Specifies the duration HSTS headers are cached in browsers
    - Include subdomains: On, Every subdomain below this will inherit the same HSTS headers
    - Preload: On, Permit browsers to preload HSTS configuration automatically
    - No-Sniff Header: Send the “X-Content-Type-Options: nosniff” header to prevent Internet Explorer and Google Chrome from MIME-sniffing away from the declared Content-Type.
- Web Application Firewall’s Managed rules for common known CMS attacks.
- OWASP Hacker Proof, OWASP Core Ruleset (2013) provides protection against common attack categories, including SQL Injection and Cross-Site Scripting. These rules present a Challenge page when triggered.
- Bot Fight Mode, Challenge, and/or block requests matching patterns of known bots before they can access your site.

Code Level

1. Request Rate Limits e.g. 10 requests per second per IP address.
2. Self Hosted Server-side Captcha Validation
3. Brute force attack prevention: We block the requesting IP for an hour as soon as the 10th invalid request is detected for an endpoint. e.g. HackerSpray
4. Strong Password Policy, can be customized using a custom Regular Expression. Passwords are stored as Hash Strings in DB.
5. CORS Enabled for specific domain only: Use of same domain CORS policy helps to restrict access from one domain to resources belonging to another domain.
6. XSS Attack prevention:
    1. Use of Regular Expressions to validate data & only store validated data.
    2. XSS can be prevented by Encoding URL parameters using URLEncoder.
7. Use of LINQ & ORM for SQL Injection attack prevention
8. Use of HttpOnly cookies. Httponly flag is very important to avoid any XSS attack and has other benefits

9. KYC profiles are encrypted with machine keys.
10. Use of custom response headers (Appended below)

HTTP Response Headers

- **x-content-type-options:** nosniff
- **x-frame-options:** DENY
- **x-xss-protection:** 1; mode=block
- **strict-transport-security:** max-age=0; includeSubDomains; preload
- Content-Security-Policy=script-src 'self' object-src 'none'

JWT Bearer Token for User Session

- IP Specific
- AES Encrypted
- Single-use allowed with max 5 retries
- Disable all token issued prior to password change, after logout, and after every IP whitelist change
- Tokens are renewed every 5 minutes to mimic the server-side session timeout behavior.

Transactional OTPs or Email Verification Links

- Single-use tokens
- No retry allowed
- Google 2FA required after Email verification
- Google 2FA required for address whitelisting

User profile & KYC Data

- Email OTP required for Email Change, OTP from both old and new emails.
- Email verification required for a Password reset
- KYC Profile, file upload sanitization
- File uploads to AWS S3 or Azure Storage using a pre-signed URL to prevent any foreign object from reaching the server where the object code executes.

Role-Based Authorization

- Custom role definitions to suit any situation
- Supports granular security permissions
- A full suite of role administration (list, get, create, update, delete)

Auditing

- Complete enterprise access and data auditing to meet compliance requirements
- HTTP Request / Response logging to track user activity (anonymous and authenticated users)

- Database change logging to track manipulation of data over time (anonymous and authenticated users)