The following points highlight the team's work on addressing **Rapid7 vulnerability findings**:

- Prevented browser caching on sensitive pages to mitigate cache-related data leakage
- Hardened sensitive fields and error handling
- Disabled autocomplete on sensitive fields
- Enabled custom error redirection
- Prevented SQL injection
- Addressed form resubmission vulnerabilities across server and client code
- Applied Content-Security-Policy to allow external sources (images, fonts, scripts) and trusted domains
- Set X-Content-Type-Options to nosniff
- Added httpCookies configuration in web.config