Description

Dunder Mifflin Paper Company Inc. (Dunder Mifflin) has engaged Shehzade Security Group (SSG) to perform a security assessment of their Infinity e-commerce platform. The Infinity application provides customers the ability to purchase various types and amounts of paper without relying on sales staff. The purpose of the assessment is to provide assurance that the application does not represent an unnecessary security risk to Dunder Mifflin or their customers in terms of the confidentiality, availability, and integrity of sensitive data.

The Dunder Mifflin Infinity application is a web application hosted on infrastructure consisting of an application server running Microsoft's Internet Information Services and a database server running Microsoft SQL Server 2017. The Dunder Mifflin Infinity application is accessible from the internet and allows users to authenticate using a username/password pair. MFA is not currently required but will be enforced in a future release. The application front-end and back-end is developed using ASP.NET Core and the application contains 24 pages.

The Infinity application is currently in the final testing phase, where it is being trialed by a small number of external customers and internal administrators. As such, there are currently two user roles supported, with plans to add additional roles in the future. The currently supported roles are as follows:

- Administrative User
  - Represents a Dunder Mifflin employee
  - This role should be able to access the administrative panel containing all customer, sales, and security log data
- External User
  - Represents a Dunder Mifflin customer
  - This role should only be able to access their data

The application handles various forms of sensitive data, such as names, emails, order histories, and payment information of Dunder Mifflin customers.

The assessment will be conducted remotely, from SSG systems via the internet, against a live, production environment. SSG consultants will make an active effort to avoid disruption of business activities. Dunder Mifflin has a hard requirement to have the final report delivered by the end of July.

SSG will utilize industry-standard methodologies such as those provided by OWASP to assess the application across areas including, but not limited to, the following:

- Authentication
- Authorization
- Session Management

- Input Validation
- Secure Communications
- Data Storage

Dunder Mifflin has requested that an emphasis be placed on testing the administrative panel and the resume upload feature as well as the security of the personally identifiable information (PII) of Infinity customers.

Effort

8 consultant days, including reporting

Deliverables

1 PDF report, to be delivered no more than three working days after the end of the assessment.

Requirements

- Confirmation of all in-scope URLs
- Allow-listing of SSG IP addresses from any firewall, IDS, or WAF that may be in place
- 2x (two) test accounts, each assigned a different user role within the application
- A demo call prior to the start of testing to walk consultants through application functionality
- A technical point of contact for the duration of the assessment to assist with any questions that may arise