Data Theft Protection Usage

https://campus.barracuda.com/doc/98216234/

Data Theft Protection prevents unauthorized disclosure of confidential information, such as social security numbers, credit card information, and errors from web applications like Microsoft and MySQL. To avoid exposing this data, you can choose one of these options:

- Block – The entire response page is blocked, if it contains the data theft pattern, like a credit card number.
- Cloak – The response page is sent, but matching strings are partially overwritten with Xs, optionally displaying initial or trailing characters. You can see the pattern of the string, but cannot see the full value.

This protection can be applied to all or a portion of your application.

You must add elements that you want to block or cloak. Then, you can control options separately for each of the types of sensitive data.

Element types include:

- Credit cards
- Social security numbers
- Directory indexing
- Errors from Microsoft, Oracle, PHP, Postgres, and MySQL

Configure Data Theft Protection

To apply Data Theft Protection to all or a portion of your application, follow these steps:

1. From App Profiles, add Form Protection to the desired URL.
2. In the right side panel find **Data Theft Protection** and click on it.
3. Set **Enable Data Theft Protection** to **Enable**.