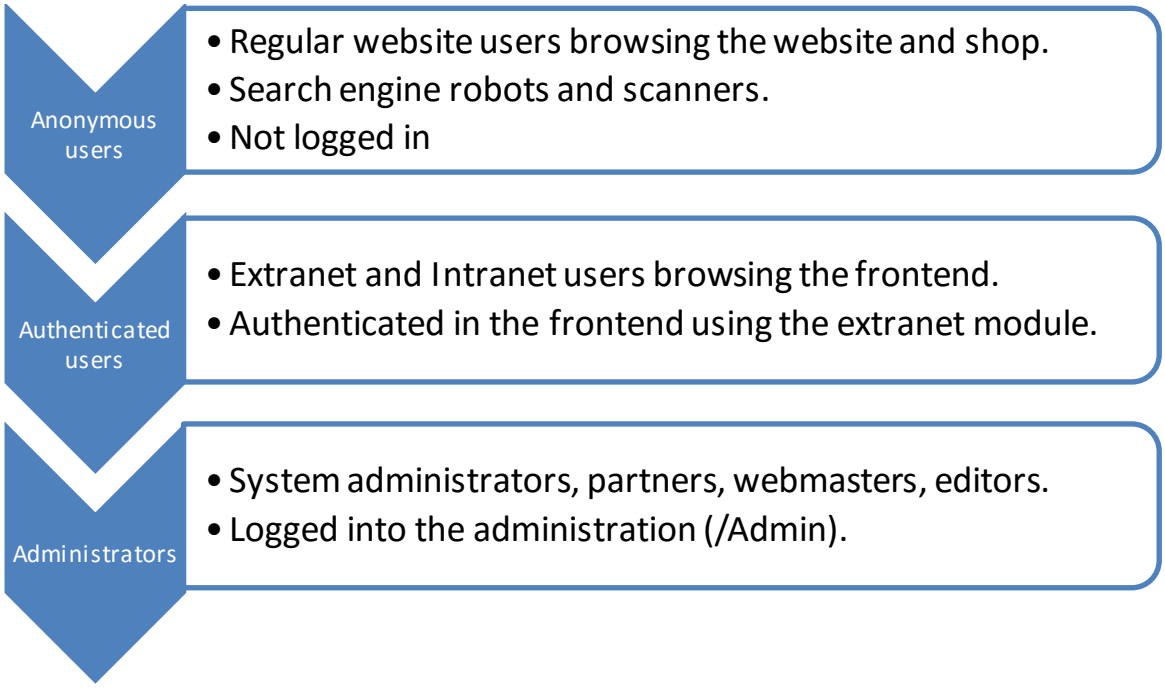
Dynamicweb 8 Security

Dynamicweb is a web application serving web pages on a webserver. Overall there are 2 areas of security when hosting a Dynamicweb solution – the security of the infrastructure tier (Firewall, Windows, IIS, SQL-Server, ASP.NET and related technologies) and the application tier security (The Dynamicweb application).

This document covers the application tier security. For infrastructure security, please refer to the hosting provider.

The Dynamicweb application makes use of various different approaches to ensure that the software cannot be compromised making it possible to post unintended content, get access to data, gain access to restricted areas of the website and Denial of Service attacks (DOS).

Dynamicweb has 3 layers of different user access control (UAC).



Anonymous and Authenticated users can only browse the frontend of the website (/Default.aspx) – they have access to everything not placed in /Admin and in /CustomModules subfolders with the exception of /Admin/Public folder.

Administrators have access to the frontend and the backend (/Admin).

The Dynamicweb application security handles various types of attacks.

- XS attacks (Cross script attacks)
- HTML injection attacks
- SQL Injection attacks
- HTTP Header injections
- Cookie injections
- Data input validations

Dynamicweb has a number of checks to handle these types of attacks.

1. Check if the current user have access to the specific area of the software. That would be either the administration (/Admin) or pages in the frontend with permissions. This check is made before any process of the request or incoming data is handled. The check is global and covers all requests going through the .NET engine. This is not applicable for i.e. files, i.e. /Files/Images/Picture.jpg.
    a. If user does not have access, show a login dialog.
2. Scan incoming data (Post, Get and Cookies) for SQL injection. A number of tests are executed against ALL the data being send to the application layer. This check is made before any process of the request or incoming data is handled. The check is global and covers all requests going through the .NET engine.
    a. If one of the test fails, Dynamicweb bans the IP for 5 minutes giving a 403.1 http status for all subsequent requests in that time period.
3. Scan incoming data (Post, Get and Cookies) for XS and HTML injection.
    a. If one test fails, Dynamicweb returns a 404 http status for the request and stops all further processing of the request.
4. Data is validated and converted to the proper data type to avoid bad data in the application.

Check 1-3 is done for all data going into the system regardless of how things are developed and covers both standard and custom modules and cannot be bypassed. Level 2+3 can be disabled by the system administrator though. Check 4 is done by each functionality or module in the system, and needs to be manually implemented in custom modules etc.

DOS prevention

Dynamicweb does not contain DOS prevention mechanisms. This should be handled by the security of the infrastructure tier.

Data Security

The data in a Dynamicweb solution is located in the database and Dynamicweb uses a single account with CRUD and DDL rights to access and maintain the data and the data model. End user permissions for the data in the database is handled by the application tier and not by the data model.

Security scanning

The above security mechanisms are tested on regular basis (with every minor release) using the http://sqlmap.org/ tools to check for vulnerabilities.