Web vulns:

* Injection

Basics:

Providing unexpected inputs to an application that then uses them to frame a statement that is then executed by the database. Most common being SQL queries that will take unsanitised input. Anything that accepts parameters as input can potentially be vulnerable to a code injection attack. Wordpress websites will probably be our main source of these vulns due to different plugins people add to them.

Other software to investigate:

[**Kiuwan**](https://www.kiuwan.com/)

Method:

In order to check for SQL injection, we must make the query always true. To do this we can use code such as:

‘ or 1=1;--

If the statement uses unsanitised user input, this code will make the query always true and we can add any code to the end that we want to execute

* Broken Authentication
* Sensitive Data Exposure
* XML external entities
* Broken access control
* Security Misconfig
* XSS
* Insecure Deserialisation