Security risks involved with a system

* You can find out list of controllers
* MD5 hashing is old and can be convereted online
* A user could find out if the system is using the old hashing system and find a password hashed in the dev tools and convert it to find the admin
* If a system displays what javascript libraries are used then they could attempt to hack the libraries instead
* URL manipulation – where you try and guess what an admin site would be by adding it to the end of the url for example [www.arnoldclark.com/administration](http://www.arnoldclark.com/administration) etc
* 3rd party dependencies – touching on libraries again as this could allow a hacker to mess with a used library
* A hacker could try and make a website unavailable
* An update could actually introduce defects to a system or break the systems
* A hacker could try and access data from a system
* You can get some OS security patches that are out of dat etht can leave a site open to attacks
* A hacker could access data and start deleiting the websites data or users date
* If a page returns a 500 error or 404 ensure there is no information leakage regarding SQL queries or table names or anything like that
* Verify there is no unsecured admin functionality – no url and stuff
* A distributed denial-of-service (**DDoS**) **attack** occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an **attack** is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.
* If a hacker could view a users information this would be breaching data agreements
* Man in the middle attack = where 2 systems think its talking encrypted but theres an attacker in the middle of the communications viewing everythign
* Tampering / theft of data – could change users access, could give access to unauthorised users etc
* Unhashed passwords / old hashing functions ( MD5) this could leave confidential information vulnerable to theft
* Persistant cookies on a machine could be a risk as an attacker couldl put a virus in there and it could persist across many sessions
* An attacker could view users data and then use their payment methods to buy goods
* Unexcrypted communications is another security risk