Whiteboard doc for suggesting improvements to the web app testing section of http://www.crest-approved.org/wp-content/uploads/Cyber-Essentials-Test-Specification.pdf
Namely:

> The following tests cases are required for any web applications identified. Note – test cases should only be performed WITHOUT authentication credentials.
>
> - SQL Injection
> - Command Injection
> - Forced browsing to bypass authentication
> - Injection attacks that may allow host compromise or exfiltration of data

So … what do we think it should cover??
Add your suggestions here:

- Web systems (web servers, application servers, database servers, etc) included in port and vulnerability scans (as per tests 3 and 4)
- Missing security headers
- Publicly exposed web admin interface login screens (e.g. content management system, control panels, database interfaces like phpmyadmin) (NB, the kind of thing I'm thinking here is the stuff covered by tools like Nikto, so shouldn't be super expensive to do)
- TLS (to a certain standard?) missing from any page or form that requests or receives personal data, usernames, passwords, session identifiers, or other business sensitive data
- Backup content. So things like .bak, .old, subversion and git content. Easy to scan for. In a lot of cases not that serious but can be really bad if something like creds are present)
- Debug interfaces or debug content on system. For example ASP.NET trace.axd can reveal very sensitive information (I've seen full CC details) if enabled, again an easy hit for web app/CGI scanners. This would also include information leakage through error messages (e.g. stack traces).
- Using known vulnerable versions of application frameworks and libraries (ones that can be easily detected, eg JS libs with version headers in, again easy to scan for)
- Mobile apps?