Possible threats

|  |  |
| --- | --- |
|  | Mitigations |
| SQL Injection | Escaping, parameterized sql statements, validate, sanitize |
| Password attacks (brute force) | Captchas, Strong passwords, account lockouts. |
| XSS |  |
| CSRF | tokens |
| Cookie Stealing | httpOnly, don’t set max age or expires; that way cookie expires after 1 hour. |
| Path Traversal |  |
| General Implementation | * HTTP security headers. E.g. X-XSS-Protection. Check this out: <http://www.dotnetnoob.com/2012/09/security-through-http-response-headers.html> * Folder permissions |

Security Controls

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Input valid.** | **Pre-pared**  **stmnts** | **Https** | **Secure authen-tication** | **Random tokens** | **Excep-tion han-dling** | **http sec. headers** | **Server harde-ning** | **Data encryp-tion** |
| XSS |  |  |  |  |  |  |  |  |  |
| SQLi |  |  |  |  |  |  |  |  |  |
| CSRF |  |  |  |  |  |  |  |  |  |
| Netw.att. |  |  |  |  |  |  |  |  |  |
| pwd.att. |  |  |  |  |  |  |  |  |  |
| Inf.leak. |  |  |  |  |  |  |  |  |  |
| unknown |  |  |  |  |  |  |  |  |  |