0.1 Path Traversal Attack

Utilização de .. e / para aceder a ficheiros e diretórios que não devem ser acedidos.

0.2 SQL Injection

Injeção e queries SQL a partir de dados de input.

0.3 Account Lockout

A aplicação contém bloqueio de contas que pode ser ativado facilmente (mecanismo usado contra ataques de força bruta).

Isto permite que os atacantes bloqueiem serviços aos utilizadores, bloqueando-lhes as contas.

0.4 Cross-Site Scripting (XSS)

Injeção de scripts malignos em sites.

0.5 Cross-Site Request Forgery (CSRF)

Um atacante cria links que levam para ações na página onde o utilizador já tem sessão iniciada.

0.6 Man in the Middle Attack

Intercetar comunicações entre dois sistemas.

Evita-se usando chaves públicas assinadas por uma certificate authority (CA).

0.7 Credential Storage

Passwords devem ser passadas ao servidor e só depois se faz uma hash, utilizando um salt variável.

Um salt deve ser gerado com um Cryptographically Secure Pseudo-Random Number Generator. Deve ser único para cada user. Tem que ser longo. O salt deve ser concatenado à password e, de seguida, deve ser criada uma hash. Tanto o salt como a hash devem ser guardados na base de dados.

0.8 Session Fixation

Obter ID de sessão válido, induzindo um utilizador a autenticar-se com esse ID e, posteriormente, roubar a sessão validada com o conhecimento do ID de sessão utilizado.

0.9 Session Hijacking

Ganhar controlo da sessão do utilizador roubando o ID de sessão.

0.10 Denial of Service

Tentativa de fazer uma máquina ou recurso de rede indisponível para os seus utilizadores.