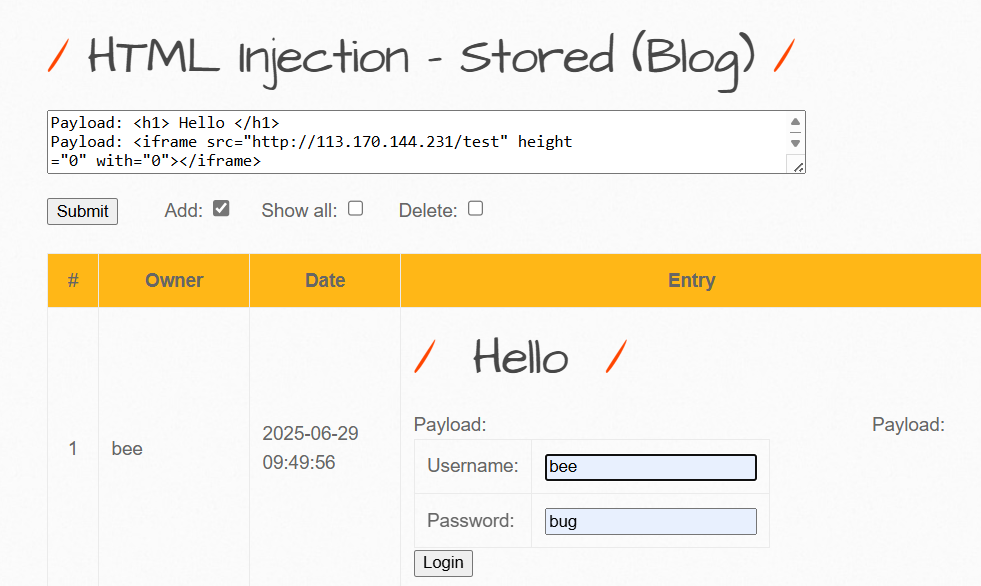
**Injection**



**HTML injection – Stored**

****

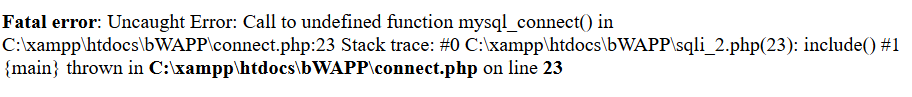
**PHP code injection**

****

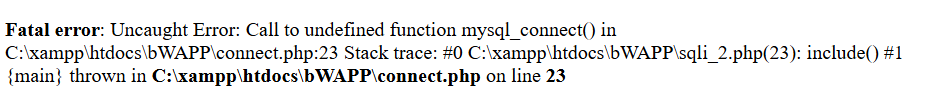
**OS Command injection**

****

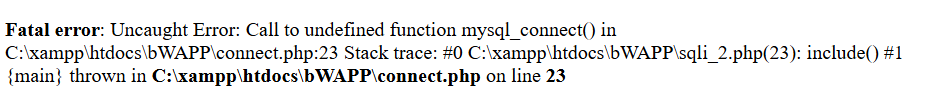
**SQL injection (Get/Search)**

****

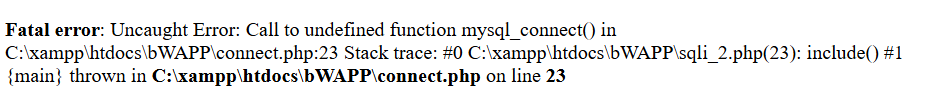
**SQL injection (Get/Select)**

****

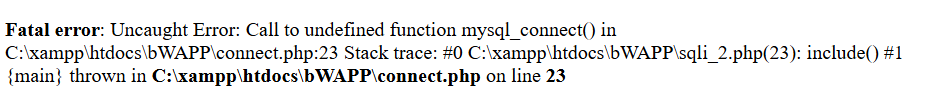
**SQL injection (Post/Search)**

****

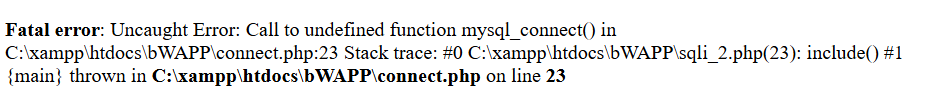
**SQL injection (Post/Select)**

****

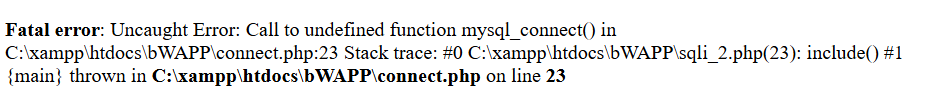
**SQL injection (Captcha)**

****

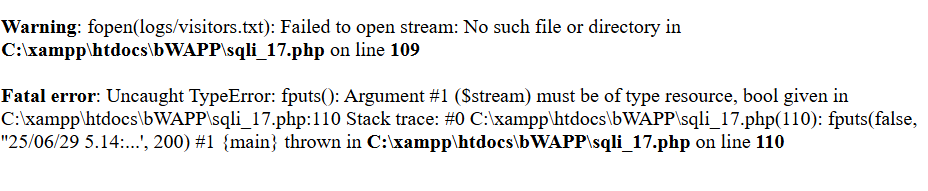
**SQL injection (Login Form/Hero)**

****

**SQL injection - Stored (Blog)**

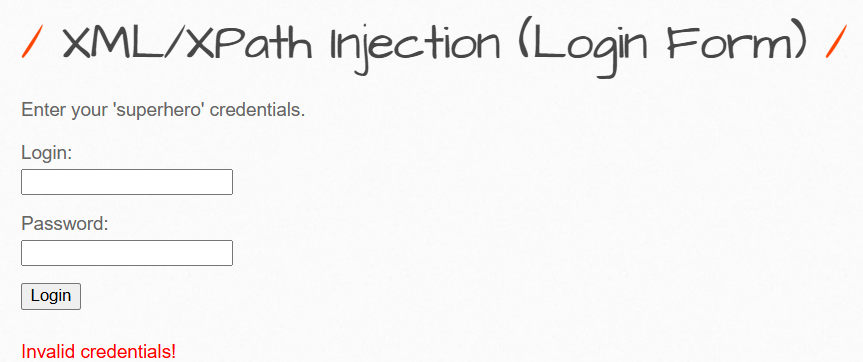
****

**SQL injection - Stored (User-Agent)**

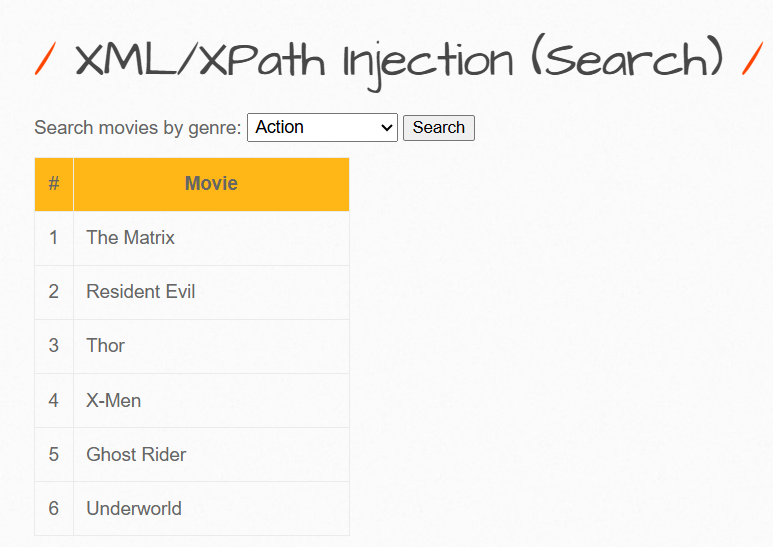
****

**SQL BỊ LỖI NÊN EM LƯỚT PHẦN SQL NHA THẦY**

**XML/XPath injection (Login Form)**

****

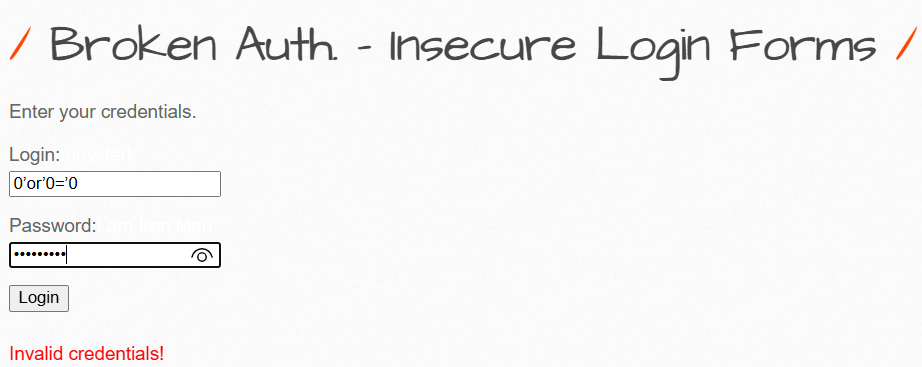
**XML/XPath injection (Search)**

****

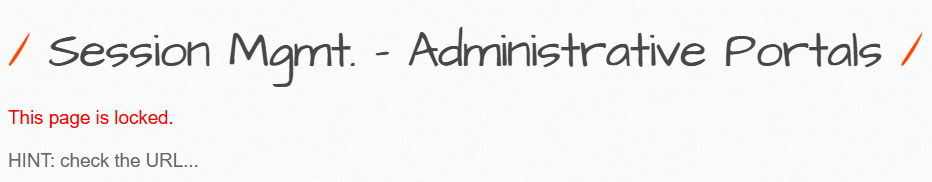
**Broken Authentication**

**“”**

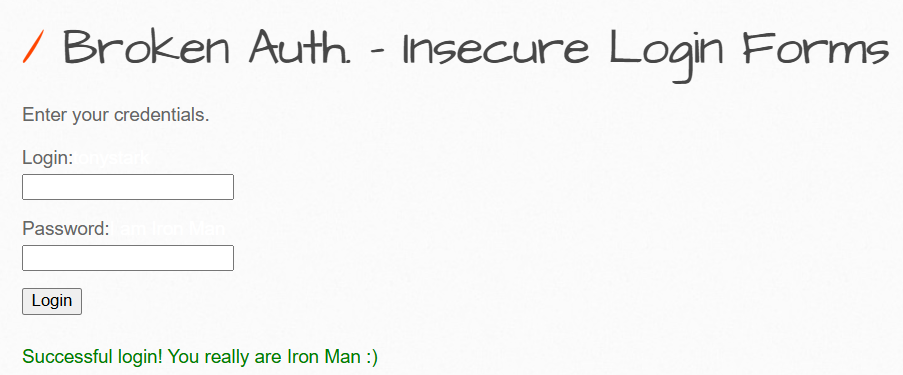
**Broken Authentication - Insecure Login Forms**

****

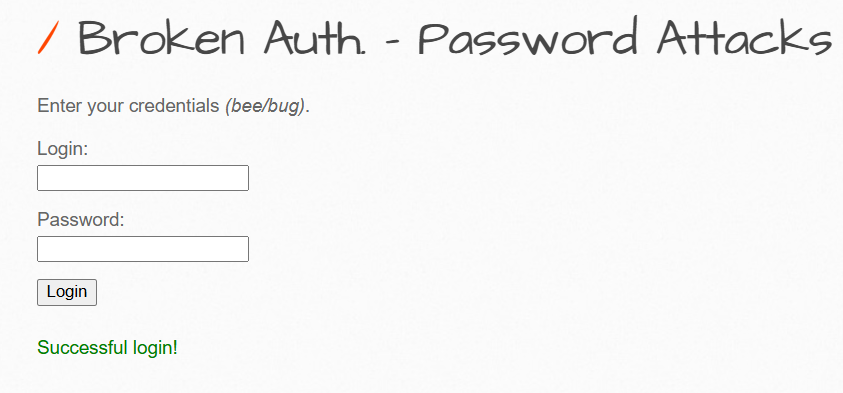
**Session Management - Administrative Portals**

****

**Broken Authentication - Insecure Login Forms**

****

**Broken Auth. - Password Attacks**

****

**HTML5 Web Storage (Secret)**

****

**Cross-Site Request Forgery (CSRF)**

**CMD**