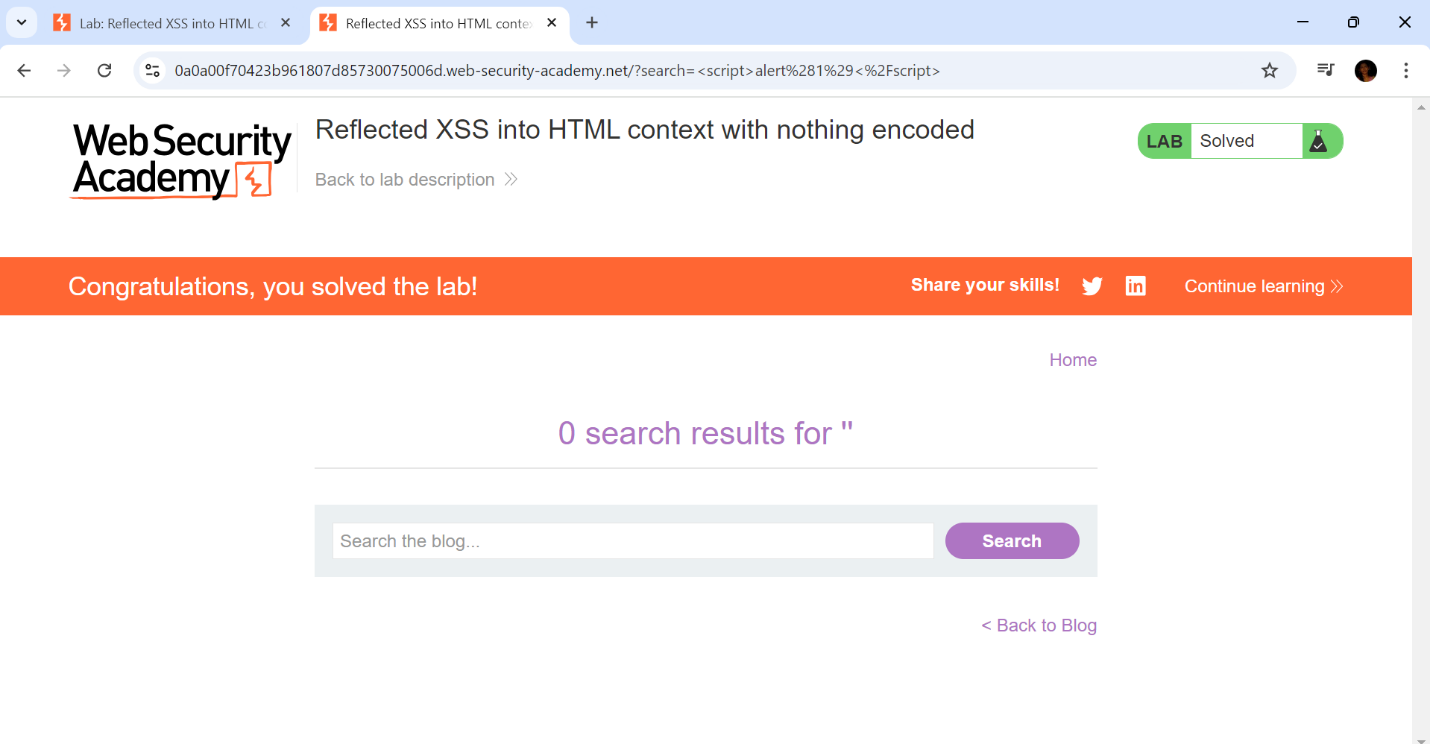
**1.SQL injection vulnerability allowing login bypass**



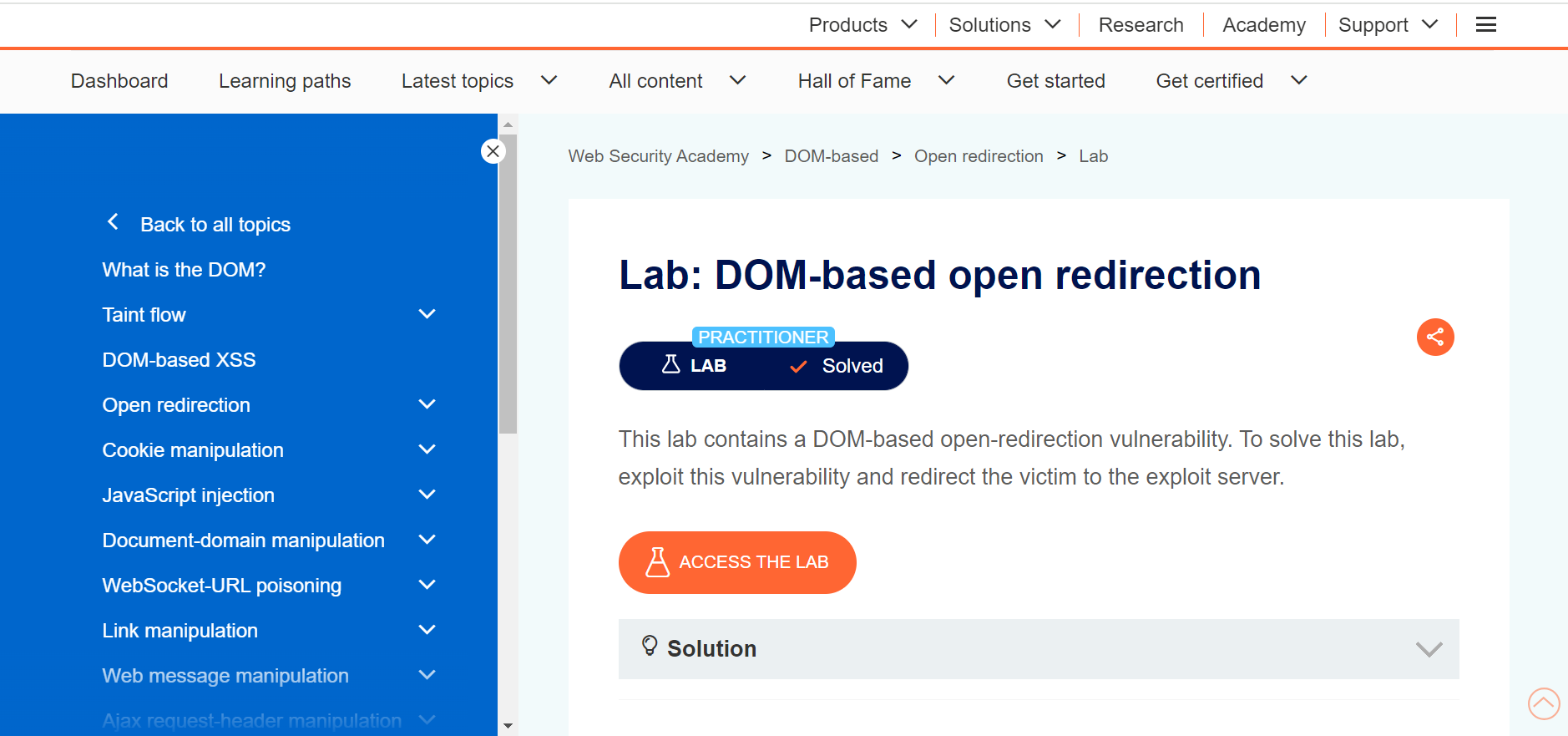
2. **Cross-site scripting**

* **Reflected XSS into HTML context with nothing encoded**



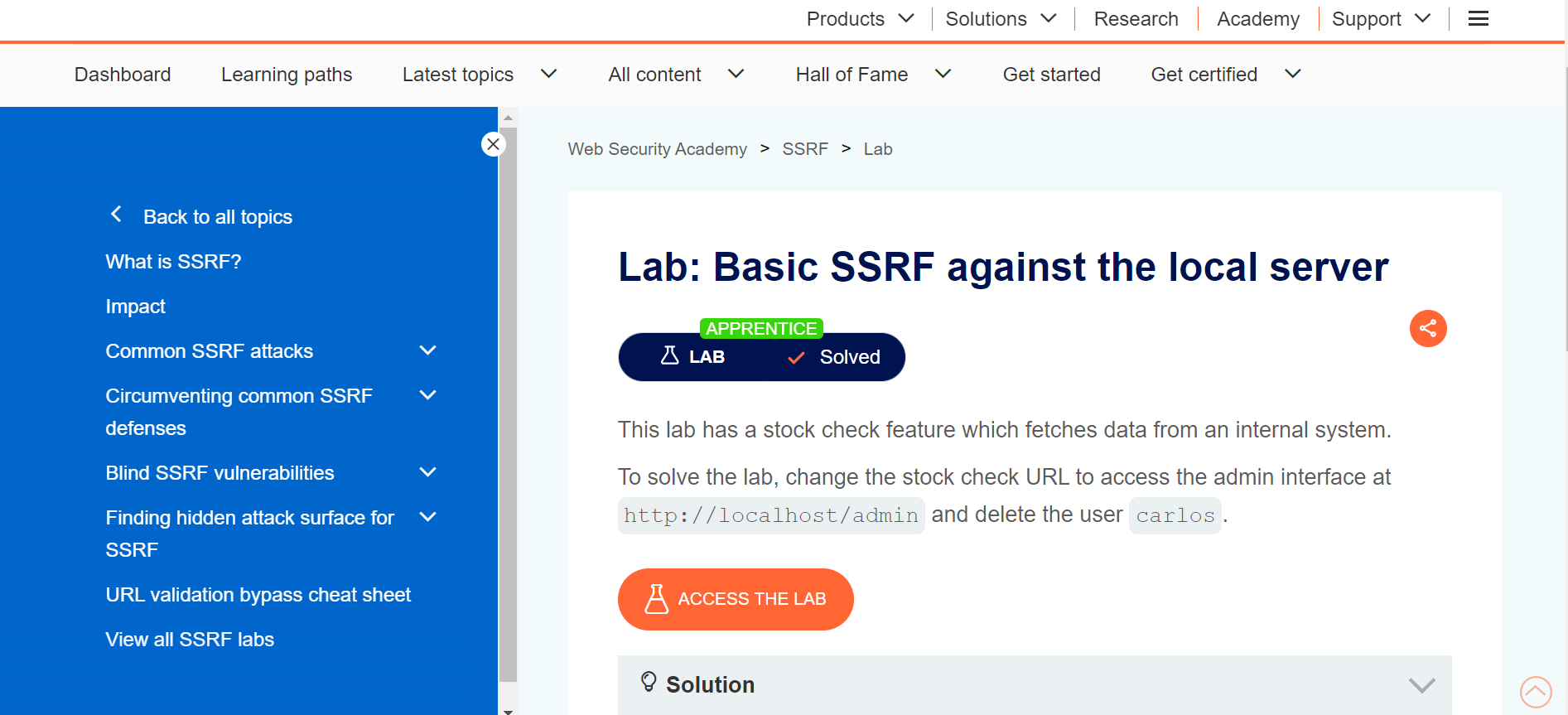
3. **DOM-based vulnerabilities**

* **DOM-based open redirection**



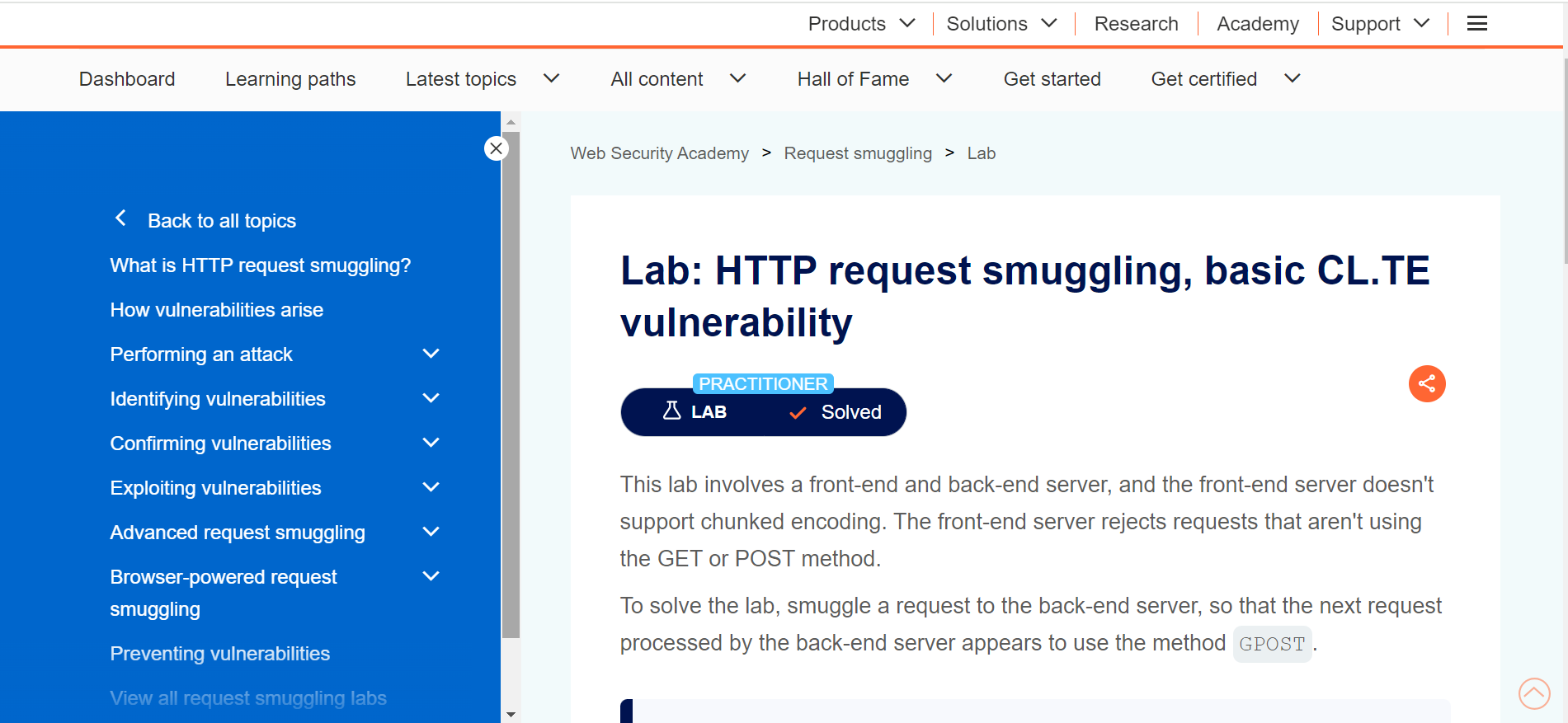
4. **Server-side request forgery (SSRF)**

* **Basic SSRF against the local server**

****

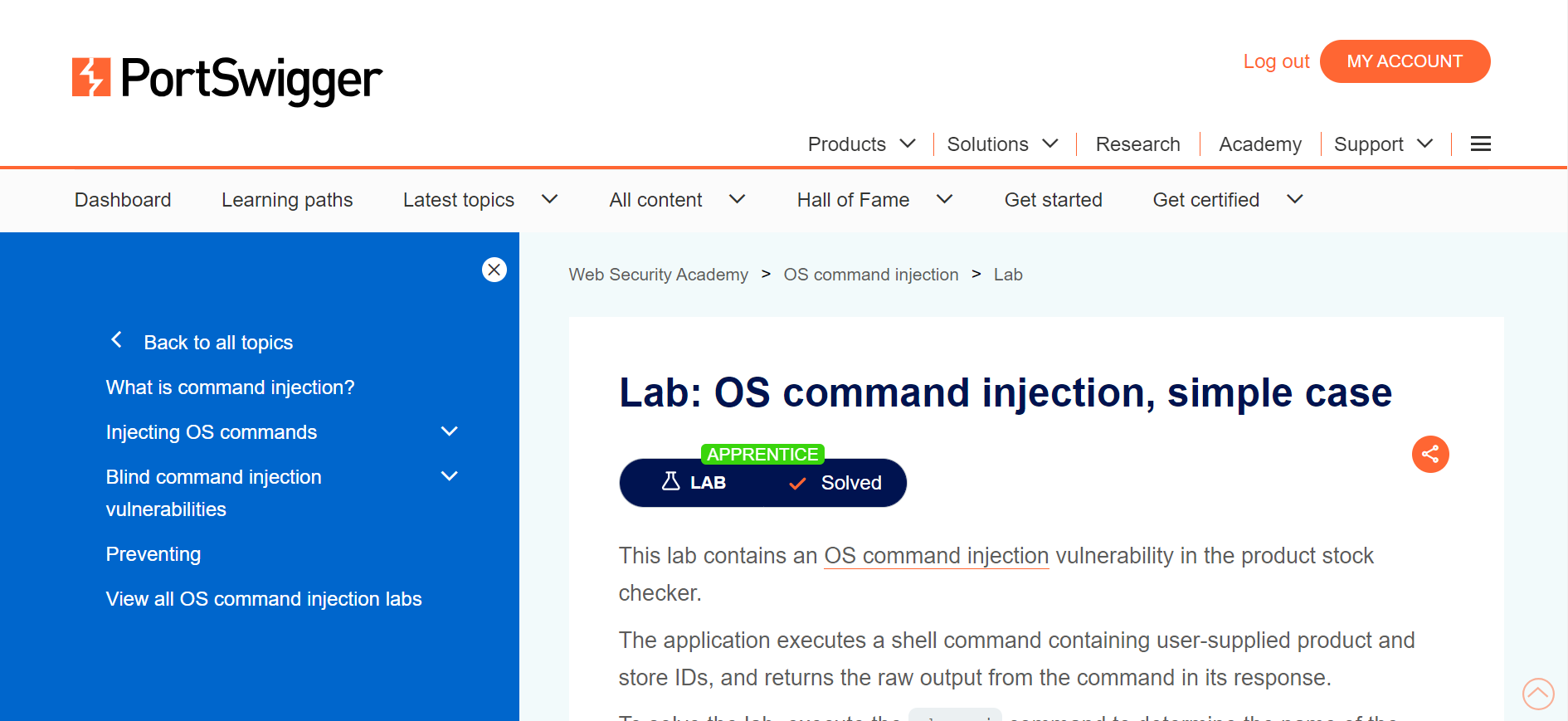
5. **HTTP request smuggling**

* **HTTP request smuggling, basic CL.TE vulnerability**



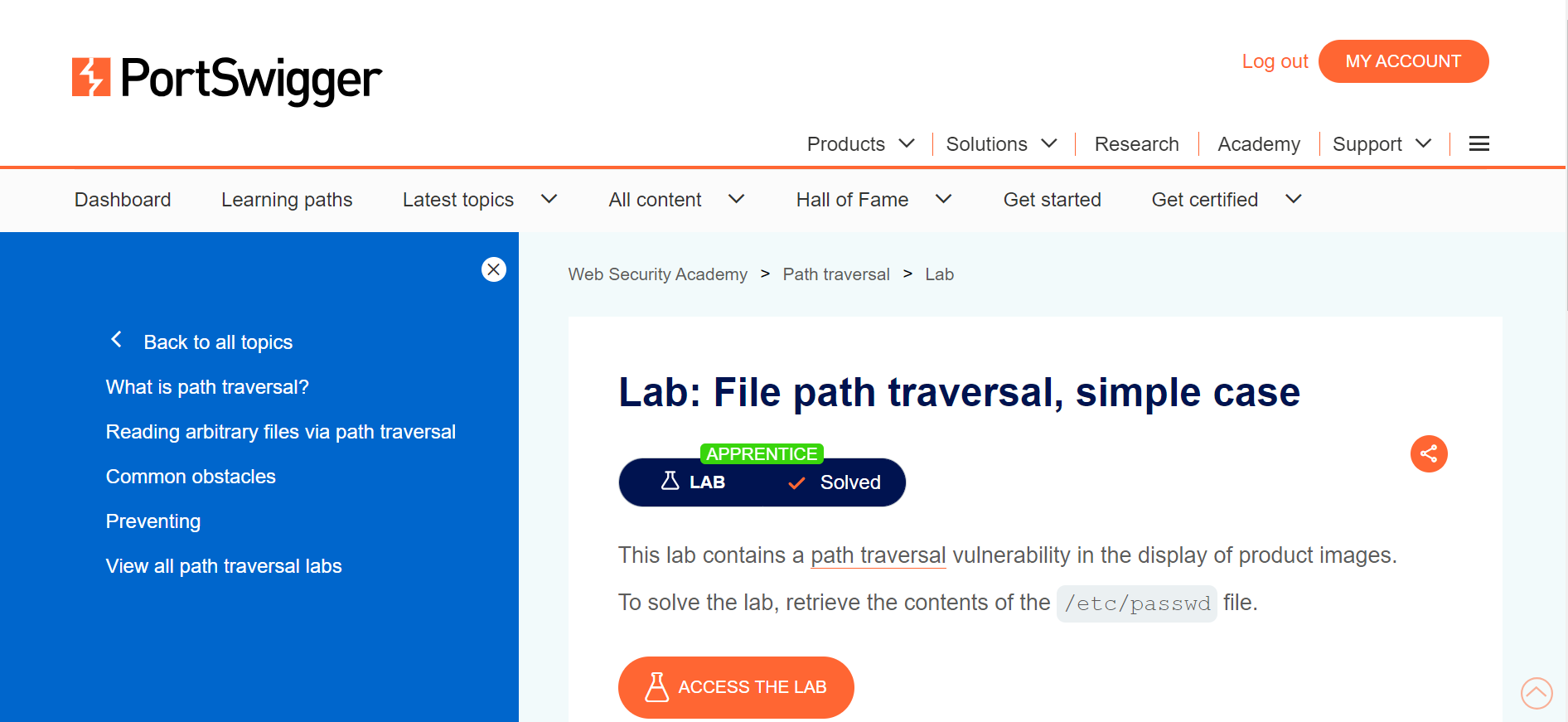
6. **OS command injection**

* **OS command injection, simple case**



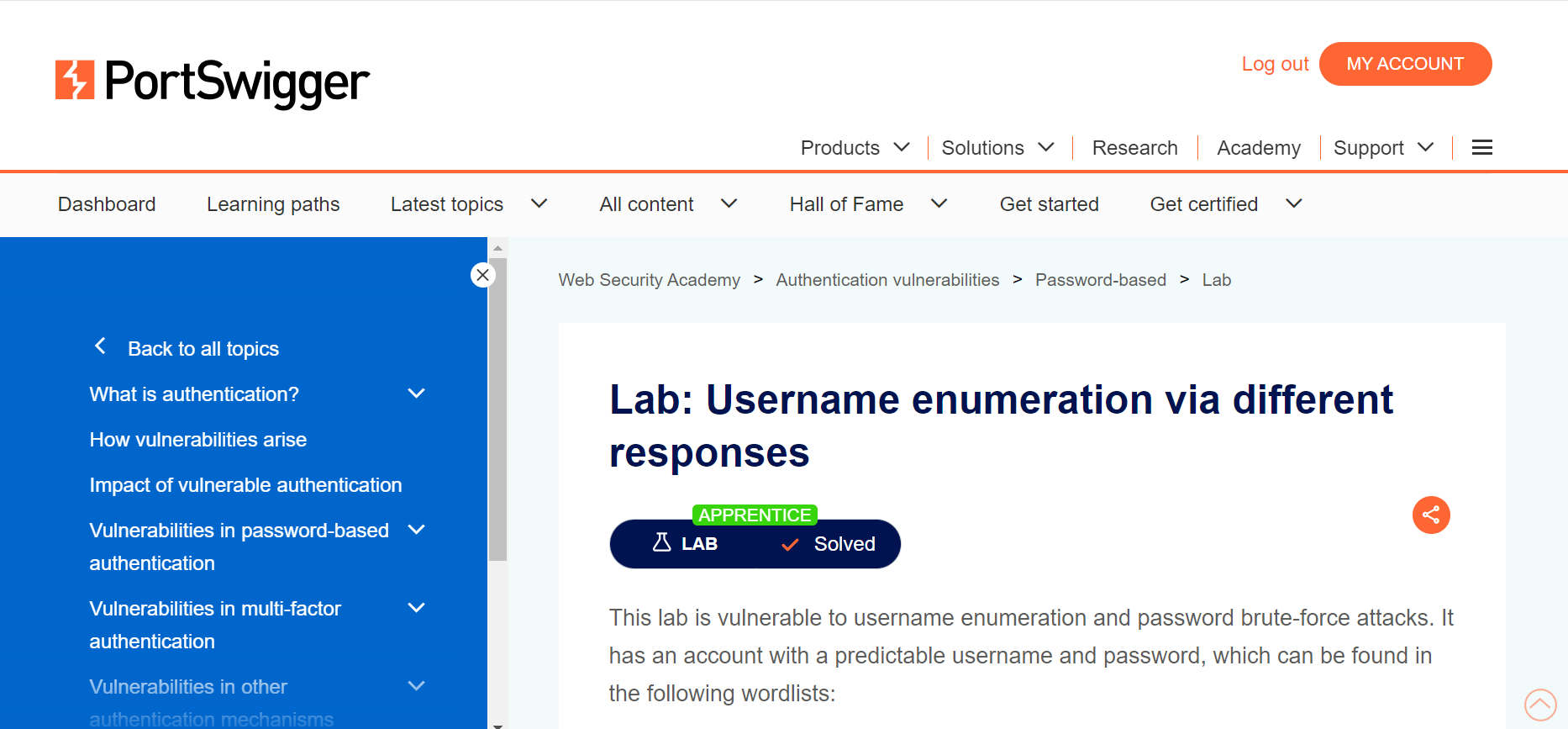
7. **Path traversal**

* **File path traversal, simple case**



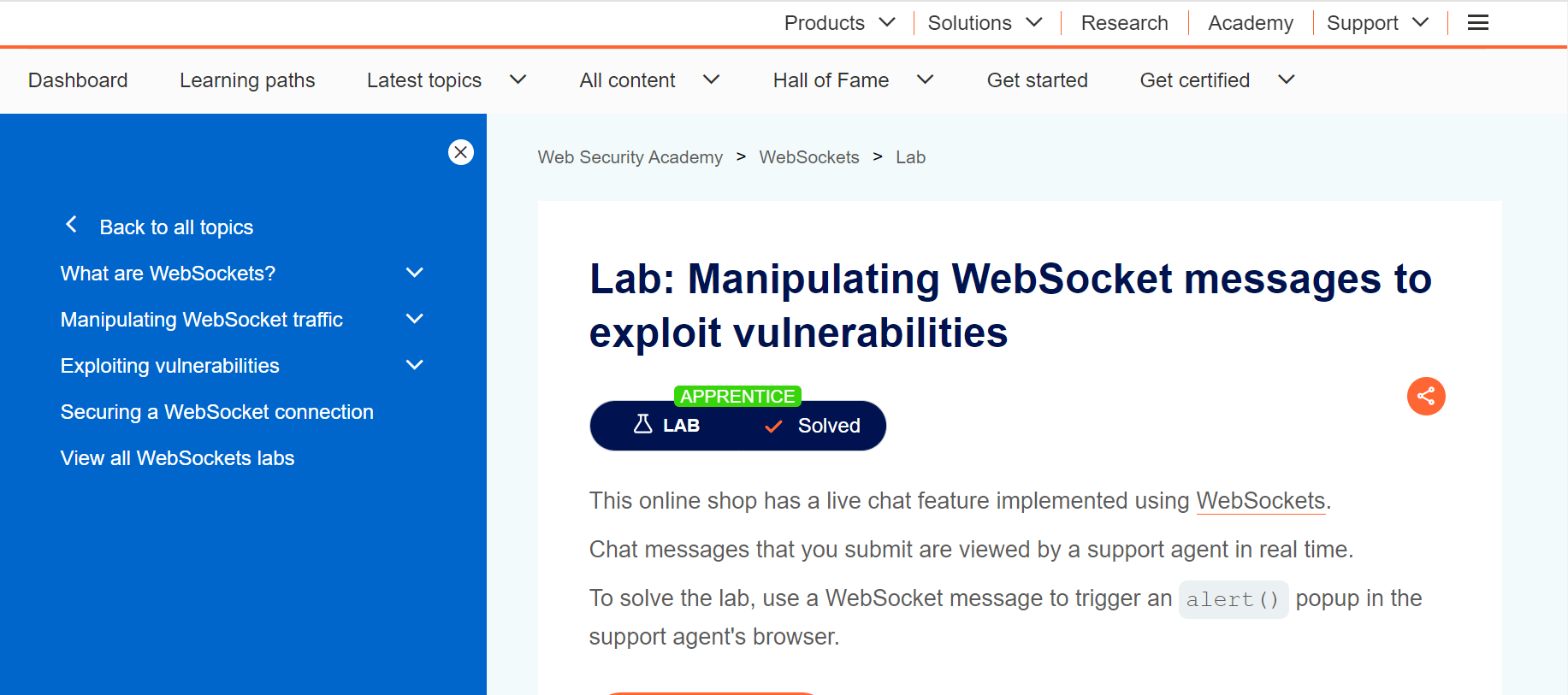
8. **Authentication**

* **Username enumeration via different responses**



9. **WebSockets**

* **Manipulating WebSocket messages to exploit vulnerabilities**



10. **File upload vulnerabilities**

* **Remote code execution via web shell upload**

