

Rakshitha K

19ITR071

OS COMMAND INJECTION AND HTTP REQUEST SMUGGLING

The screenshot shows the 'All labs | Web Security Academy' interface. At the top, there's a navigation bar with 'LAB' and 'EXERCISE' tabs. Below this, a list of labs is displayed. The first lab, 'Server-side pause-based request smuggling', is marked 'Not solved'. Below it, a section titled 'OS command injection' is shown. This section contains five labs: 'OS command injection, simple case' (Solved), 'Blind OS command injection with time delays' (Solved), 'Blind OS command injection with output redirection' (Solved), 'Blind OS command injection with out-of-band interaction' (Not solved), and 'Blind OS command injection with out-of-band data exfiltration' (Not solved). The interface includes a search bar, a list of suggested sites, and a taskbar at the bottom with various application icons and system status indicators.

LAB EXPERT Server-side pause-based request smuggling » Not solved

OS command injection

LAB APPRENTICE OS command injection, simple case » ✓ Solved

LAB PRACTITIONER Blind OS command injection with time delays » ✓ Solved

LAB PRACTITIONER Blind OS command injection with output redirection » ✓ Solved

LAB PRACTITIONER Blind OS command injection with out-of-band interaction » Not solved

LAB PRACTITIONER Blind OS command injection with out-of-band data exfiltration » Not solved

Server-side template injection

The screenshot shows the 'All labs | Web Security Academy' interface. At the top, there's a navigation bar with 'LAB' and 'EXERCISE' tabs. Below this, a list of labs is displayed. The first lab, 'Blind SSRF with Shellshock exploitation', is marked 'Not solved'. Below it, a section titled 'HTTP request smuggling' is shown. This section contains five labs: 'HTTP request smuggling, basic CL.TE vulnerability' (Solved), 'HTTP request smuggling, basic TE.CL vulnerability' (Solved), 'HTTP request smuggling, obfuscating the TE header' (Solved), 'HTTP request smuggling, confirming a CL.TE vulnerability via differential responses' (Solved), and 'HTTP request smuggling, confirming a TE.CL vulnerability via differential responses' (Solved). The interface includes a search bar, a list of suggested sites, and a taskbar at the bottom with various application icons and system status indicators.

LAB Blind SSRF with Shellshock exploitation » Not solved

HTTP request smuggling

LAB PRACTITIONER HTTP request smuggling, basic CL.TE vulnerability » ✓ Solved

LAB PRACTITIONER HTTP request smuggling, basic TE.CL vulnerability » ✓ Solved

LAB PRACTITIONER HTTP request smuggling, obfuscating the TE header » ✓ Solved

LAB PRACTITIONER HTTP request smuggling, confirming a CL.TE vulnerability via differential responses » ✓ Solved

LAB PRACTITIONER HTTP request smuggling, confirming a TE.CL vulnerability via differential responses » ✓ Solved

