

Acunetix

Acunetix is a web vulnerability scanner designed to identify and address security issues in web applications. It automates the detection of vulnerabilities like SQL injection, cross-site scripting (XSS), and other web threats.

The tool offers comprehensive reports, vulnerability management, and integrations with other security platforms, making it suitable for both developers and security professionals.

Acunetix is widely used for its speed, accuracy, and ability to scan complex web applications, ensuring robust security assessments for organizations.

The screenshot displays the Acunetix web interface during an active scan. The browser's address bar shows the URL `https://kali.3443/#/scans/c1bb9d13-5c9e-4f3e-9edd-c96115d32916/info`. The interface includes a sidebar with navigation options like Dashboard, Targets, Vulnerabilities, Scans, Reports, Users, Scan Types, Network Scanner, Issue Trackers, Email Settings, Engines, Excluded Hours, Proxy Settings, About, and Help. The main content area is titled 'Scan' and features a 'Scan Information' tab. A prominent 'Acunetix Threat Level 2' badge with a 'MEDIUM' rating is shown, accompanied by a message: 'One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.' Below this, key scan metrics are displayed: 'Scan Duration' (9m 5s), 'Requests' (47,088), 'Average Response Time' (23ms), and 'Locations' (548). The 'Target Information' section lists details such as Address (`https://bmsot.ac.in/`), Server (`nginx/1.10.3 (Ubuntu)`), Operating System (`Unix`), Identified Technologies (`Yes`), and Responsive (`Yes`). The 'Discovered Hosts (31)' section lists several domains with a 'Create Target' button for each. The 'Activity' section shows the 'Overall Progress' at 90% and lists recent events, including 'Scanning of bmsot.ac.in started' and 'Antivirus not found'. The 'Latest Alerts' section displays five alerts, such as 'Possible sensitive files', 'Password type input with auto-complete enabled', 'HTML form without CSRF protection', 'Possible internal IP address disclosure', and 'Email address found', each with a timestamp.