Netsparker is a web application security solution that can be deployed on premise, on demand or a combination of both. Unlike other web application security scanners, that lack scalability, Netsparker was designed with enterprise in mind.

Netsparker’s web application security solution is packed with enterprise features such as workflows, integrations, SSO support, 2FA support, and proprietary technology that confirms false positives. The combination of these features allows Netsparker to scale scanning from 100 to 1000’s of websites in a short period of time.
The Need To Ensure **Your Web Applications & Web APIs are Secure**

Today’s businesses heavily rely on web applications because they allow employees to access critical data and collaborate with partners easily, at any time and from anywhere. Though more often than not web applications are susceptible to vulnerabilities that can be automatically detected and easily exploited.

Beat malicious hackers by identifying and fixing vulnerabilities in your websites and web APIs before they find and exploit them. Emulate them by using an automated web application security scanning solution to identify exploitable vulnerabilities and security flaws that can leave your business exposed.

Enter Netsparker, well known for its ease of use and high vulnerability detection rate and accuracy.

”

We believe that security tools should be easy to use and allow you to automate more, as opposed to complicating an already difficult process. That is why we've built an easy to use and automated web security scanner which automatically verifies identified vulnerabilities.

*Ferruh Mavituna, Netsparker Founder & CEO*
Netsparker Detects and Vulnerabilities

Netsparker was the only solution that identified all the vulnerabilities in third-party independent benchmark tests**. Also, it was one of the two scanners that did not report any false positives. These results are further proof that the Netsparker scanner has the most advanced and accurate crawling & scanning technology with the highest web vulnerabilities detection rate. So why settle for the second best?

<table>
<thead>
<tr>
<th></th>
<th>Netsparker</th>
<th>WebInspect</th>
<th>AppSpider</th>
<th>Acunetix</th>
<th>Burp Suite</th>
<th>AppScan</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Command Injection</td>
<td>100</td>
<td>N/A</td>
<td>99.11</td>
<td>78.57</td>
<td>93.3</td>
<td>N/A</td>
</tr>
<tr>
<td>Remote File Inclusion/SSRF</td>
<td>100</td>
<td>100</td>
<td>82.67</td>
<td>64.22</td>
<td>74.67</td>
<td>N/A</td>
</tr>
<tr>
<td>Path Traversal</td>
<td>100</td>
<td>91.18</td>
<td>81.61</td>
<td>94.12</td>
<td>78.31</td>
<td>100</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>100</td>
<td>98.46</td>
<td>95.39</td>
<td>100</td>
<td>97</td>
<td>100</td>
</tr>
<tr>
<td>Reflective XSS</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>97</td>
<td>100</td>
</tr>
<tr>
<td>Unvalidated Redirect</td>
<td>100</td>
<td>95.51</td>
<td>100</td>
<td>100</td>
<td>76.67</td>
<td>36.67</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>100%</strong></td>
<td><strong>97.0%</strong></td>
<td><strong>93.1%</strong></td>
<td><strong>89.5%</strong></td>
<td><strong>86.2%</strong></td>
<td><strong>84.2%</strong></td>
</tr>
</tbody>
</table>

Is Easy to Use

You can launch a web application security scan in just a few seconds. Netsparker will automatically detect custom 404 error pages, URL rewrites and scan websites with Anti-CSRF tokens, so you do not have to get bogged down in the details.

As Easy As 1-2-3

1. Enter URL
2. Configure credentials*
3. Launch security scan

* You have to configure credentials if you are scanning a password protected website.
Netsparker has unique self-tuning technology so you do not have to configure URL rewrite rules or scan policies before every scan. It is all automated so you can scan 100s & 1000s of websites without having to get bogged down in configuring the scanners for hours. This unique high level of automation gives you actionable and dead accurate insight without the need for manual verification, so your team can start working on the remedies straight away.

**Automatically Scan** HTML5, Single Page Applications & Web APIs

Netsparker can automatically parse, execute and analyze the output of JavaScript. This means it can automatically crawl, interpret and scan any type of HTML5, Web 2.0, Single Page and other modern web applications. Netsparker can also identify vulnerabilities in WSDL & REST APIs.
Automatically Verify Identified Vulnerabilities

It’s not possible to truly scale up and manage thousands of web applications if you have to manually verify the results of vulnerability assessments. Netsparker uses their proprietary Proof-Based-ScanningTM technology to automatically verify false positives and save you hundreds of man hours. Scale up your efforts without scaling up your team.

Netsparker is Stable, Accurate and Versatile, with a lot of thought put into each of its features. An excellent product in the arsenal of any security professional.

Shay Chen
Information Security, Analyst & Speaker

As we are faced with perpetual evolving security threats and vulnerabilities, Netsparker brings a level of assurance to our business as it is included as part of our development lifecycle to help identify and mitigate such threats prior to deployment. With Netsparker being able to provide zero false positives, it ensures that time is not wasted deciphering whether a vulnerability is legitimate or not.

Chris Evans
ISACA
Can **Easily Scale Up** & Encourage Team Collaboration

Netsparker is a multi-user web security scanning solution that can **scan thousands of websites simultaneously** with minimum configuration and effort. Packed with workflow enterprise tools such as Website Groups, Tasks Management and Trend Matrix Reports, Netsparker **encourages team collaboration** and allows you to **ensure that all vulnerabilities and security flaws are fixed before an application is launched in a live environment.**

In my years as a security specialist I’ve used many different tools for DAST and Netsparker has consistently been at the forefront of both experience and results. It’s simple to use without sacrificing capability.

**Scott Helme**  
Security Researcher & Entrepreneur

“I’ve long been an advocate of Netsparker without incentivisation simply because I believe it’s the easiest on-demand, do it yourself dynamic security analysis tool for the audience I speak to.”

**Troy Hunt**  
Microsoft MVP for Developer Security & International Speaker
Create a **Closed Loop Vulnerability Assessment Solution**

Netsparker can easily integrate with CI/CD and other systems found in the SDLC and DevOps environment, allowing you to build a fully customizable workflow in which vulnerability assessments, triaging and verification processes of vulnerabilities are all automated. Upon code commits, scans are launched automatically, verified vulnerabilities are automatically posted on your bug tracking system and assigned to the developers, and developer fixed are automatically scanned and verified, thus automating all of the web application security management.

Other **Noteworthy Features**

- Out of the box integration with systems such as JIRA and Github
- OWASP Top 10, PCI, HIPAA and other compliance report templates
- Automatic scanning of password protected areas
- Custom Reports API to build personalized security reports
- Automated retests of vulnerabilities fixes
- Built-in proxy for manual crawling and controlled scanning
- Exploitation engine to show the real impact of exploited vulnerabilities
- Single Sign-On support