Invicti

Web application security buyer's checklist

REQUIREMENT & IMPORTANCE	YES	NO
Discovering web applications MEDIUM		
Can the tool discover existing web assets?		
Can the tool discover new web assets as soon as they appear?		
Can the tool automatically treat discovered assets as scan targets?		
Discovering inputs (crawling) CRITICAL		
Can the tool parse SPAs with complex HTML5/JavaScript?		
Can the tool recognize/support frameworks such as React, Angular, Vue?		
Is the tool crawler based on Chromium or an equivalent recognized engine?		
Discovering unlinked assets (IAST) MEDIUM		
Can the tool discover additional files and directories from the server side?		
Can server-side discovery provide information to the crawler?		
Authenticated scanning HIGH		
Can the tool automatically recognize typical authentication schemes?		
Can you record a macro to enter areas that require custom authentication?		
Business logic support HIGH		
Can you record a macro to follow business logic (e.g. multi-level forms)?		
Scanning web services and APIs CRITICAL		
Can the tool import WADL, WSDL, Swagger, OpenApi, GraphQL definitions?		
Can the tool import data from a proxy such as Fiddler or Paros?		
Can the tool import data from API development platforms like Postman?		

REQUIREMENT & IMPORTANCE	YES	NO
Scanning for web vulnerabilities and more CRITICAL		
Can the tool detect and prove out-of-band/blind vulnerabilities?		
Can the tool detect web server misconfigurations?		
Can the tool detect vulnerable client-side libraries (dynamic SCA)?		
Can the tool detect other types of issues related to web application security?		
Reducing or eliminating false positives CRITICAL		
Can the tool provide direct evidence for vulnerabilities such as SQLi/RCE?		
Can the tool provide proof of concept for vulnerabilities such as XSS?		
Does the tool provide a confidence rating for issues that can't be proven?		
Confirming and finding vulnerabilities from the server side (IAST) MEDIUM		
Can the tool find more vulnerabilities by also scanning from the server side?		
Can the tool provide additional server-side information about vulnerabilities?		
Is the IAST module processing overhead no more than 5%?		
Developer support CRITICAL		
Does the tool provide a dedicated developer report that includes all details?		
Does the tool provide easy-to-read HTTP request and response content?		
Does the tool highlight the payload in the request/response to explain the attack?		
Does the tool provide the file and line of code or a stack trace for the issue (IAST)?		
Does the tool explain the vulnerability?		
Does the tool suggest best practices for fixing vulnerabilities?		
Does the tool provide external links to additional information?		
Do your developers like the reports provided by the tool?		
User interface and reporting MEDIUM		
Do future users of the UI like the look-and-feel and presented information?		
Do future report consumers like the look-and-feel and presented information?		

REQUIREMENT & IMPORTANCE	YES	NO
Flexibility in the SDLC HIGH		
Does the tool have a proven track record of shift-left deployments?		
Does the tool have a proven track record of being used even in production?		
Out-of-the-box integration capabilities HIGH		
Can you integrate out-of-the-box with issue trackers like Jira?		
Can you integrate out-of-the-box with CI/CD platforms like Jenkins?		
Can you integrate out-of-the-box with communication tools like Slack?		
Custom integration capabilities (RESTful API) HIGH		
Is the API designed using an industry standard like OpenAPI?		
Does the API provide access to as many functions as the UI (or more)?		
Is the API documentation easy to read?		
Does the maker have a track record of custom integrations?		
Can the maker design a custom integration for me?		
WAF automation (temporary protection) CRITICAL		
Can the tool create WAF-compatible rules for discovered vulnerabilities?		
Can I manually export WAF rules to import them to my WAF?		
Can I automate WAF export using the API?		
Compliance support HIGH		
Can the tool generate compliance reports in required formats?		
Does the tool have both generic and specific compliance reports?		
Does the maker work together with auditors to support compliance?		
Does the maker have a compliance-related track record?		
Product renown CRITICAL		
Has the product been on the market for at least 10 years?		
Is the product still developed with the help of the original team?		

REQUIREMENT & IMPORTANCE	YES	NO
Product renown (continued) CRITICAL		
Are new functions introduced into the product at least every 3 months?		
Is the maker rated in the current Gartner Magic Quadrant?		
Is the product rated in the current Gartner Peer Insights?		
Best-of-breed specialization HIGH		
Does the maker specialize exclusively in web application security?		
Does the maker prioritize web application security products?		
Did the maker enter the market first with web application security?		
Is there a dynamic growth roadmap for the web application security solution?		