Introduction Web Application Security Testing

The evolution of increasingly immersive, collaborative online technologies has transformed the way we communicate with the web-and also increased and introduced new security threats. Additional user feedback, linked databases, and quickly executed code bring new attack vectors into existence - from basic injection vulnerabilities to sophisticated, multi-stage attacks.

With decades of cumulative expertise, Infopercept is at the forefront of safety and penetration testing for applications. With a seasoned team of subject matter specialists, you can be confident that any resource is an authority in their profession.

Application Testing Beyond the OWASP Top 10

Application protection problems are not only the most common form of vulnerability, they are also increasing in scope. Although the OWASP Top 10 is seen as a benchmark for detecting device security bugs, this is only a starting point, and many specialized vulnerabilities are not included in that chart. Automated vulnerability scanners and OWASP-focused intrusion testers would lag behind emerging challenges, leaving the program vulnerable to unknown risks.

At Infopercept, we're going far beyond the OWASP Top 10, consistently stretching the device security limits and explaining how special architectures can be compromised – and how to repair them.

Code Review – Identify Flaws Earlier in Development

Though 'Blackbox' framework reviews offer a decent insight into the strengths and tactics of potential threats, especially sensitive systems need a more rigorous audit. Secure code checks detect vulnerabilities before they are pushed to development applications – and detected by attackers.

With Infopercept Security penetration testing and Code Review evaluation reviews, you will make sure the applications are ready for launch. In addition to technological vulnerabilities and remediation information, each study includes an executive overview for non-technical management.

Assessment Details and Methodology

At Infopercept, our penetration testing tool targets the full spectrum of bugs in your web app or API. Using the same tactics as professional hackers, we sometimes intentionally skip automated tools with specific access to security threats. To ensure good quality, repeatable commitments, our form of penetration testing meets the following steps:

Information gathering on the target environment

1.Reconnaissance

As with malicious hackers, any penetration test starts with the collection of information. To detect vulnerabilities, collecting, parsing, and correlating information on the target is essential.

Identify and map vulnerabilities

2.Vulnerability Detection

If the goal has been thoroughly listed, Infopercept uses both vulnerability scanning software and manual inspection to find security vulnerabilities. With decades of experience and custom-built equipment, our security engineers have found several unique and innovative ways of finding and fixing vulnerabilities.

Although code scanning tools may be helpful in detecting low-hanging threats, they are no substitute for professional engineers. By using the previous mapping and scanning techniques, we concentrate on the most vulnerable areas of the code – and discover weaknesses that automated services have overlooked.

Safe and controlled exploitation of vulnerabilities

3.Attack and Post-Exploitation

At this point of the evaluation, our experts will analyse all prior data to detect and securely exploit known bugs in the program. Once critical access has been achieved, the emphasis will be on escalation and movement to determine technological risks and the overall market effect.

During each step of the compromise, we keep client stakeholders updated about progress testing, maintaining asset protection and stability.

Detailed, risk- prioritized report with remediation steps

4.Assessment Reporting

If the engagement has been completed, Infopercept will include a concise review and vulnerability report, including remedial action. Our advisors set industry standards for transparent and succinct reviews, prioritizing the highest risk vulnerabilities.

The appraisal shall contain the following:

- Executive Summary.
- Strategic strengths and weaknesses.
- Identified vulnerability and risk rating.
- Detailed risk remediation.
- Assets and Data Committed during the assessment

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint
© Infopercept Consulting Pvt. Ltd.

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta
Hotel, Navrangpura, Ahmedabad, Gujarat
380009, INDIA

Contact
sos@infopercept.com
www.infopercept.com/knowledge/datasheets