vumetric
CYBERSECURITY

OWASP Top 10 Vulnerabilities

Explore the critical security risks that shape the cybersecurity landscape. Understanding these vulnerabilities is essential for protecting web applications and staying ahead of emerging threats.

Vulnerability #1: Injection

This vulnerability occurs when untrusted data is sent to an interpreter as part of a command or query. It can lead to data loss or unauthorized access to data.

Vulnerability #2: Broken Authentication

This involves weaknesses in session management and authentication functions. Attackers can impersonate users and gain unauthorized access.

Vulnerability #3: Sensitive Data Exposure

This occurs when an application doesn't adequately protect sensitive information, such as passwords and credit card numbers, making it accessible to attackers.

Vulnerability #4: XML External Entities (XXE)

This vulnerability allows attackers to exploit vulnerable XML processors. They can disclose internal files and execute remote code.

Vulnerability #5: Broken Access Control

This happens when users can perform actions or access data they aren't supposed to due to inadequate or entirely missing access restrictions.

Vulnerability #6: Security Misconfiguration:

This is the most commonly seen issue where default configurations are not changed, unnecessary features are not disabled, and patches are not updated.

Vulnerability #7: Cross-Site Scripting (XSS):

This vulnerability allows attackers to inject malicious scripts into web pages viewed by other users, which can lead to various types of attacks like stealing cookies or defacing websites.

Vulnerability #8: Insecure Deserialization:

This allows attackers to execute arbitrary code or perform unauthorized actions by exploiting insecure deserialization processes.

Vulnerability #9: Components with Known Vulnerabilities:

This involves using libraries, frameworks, or other software components that have known vulnerabilities, putting the application at risk.

Vulnerability #10: Insufficient Logging & Monitoring:

This vulnerability makes it difficult to detect or respond to attacks in a timely manner due to inadequate logging and monitoring.

READY FOR A CUSTOM PENTESTING SOLUTION?

Use our efficient scoping tool to quickly receive a tailored quote with all-inclusive costs for your specific penetration testing needs, directly in your

GET A QUOTE

Explore tailored solutions for your specific needs. Our pentesting projects typically range from $6,000 to $25,000, offering comprehensive security assessments to protect against the vulnerabilities listed above.

ABOUT VUMETRIC

Vumetric is a leading cybersecurity company dedicated to providing comprehensive penetration testing services. We pride ourselves on delivering consistent, high-quality services backed by our ISO 9001 certified processes and the most recognized industry standards. Our world-class cybersecurity services are trusted by clients of all sizes, from Fortune 1000 companies to startups and government organizations.

Why Partner with Vumetric?

Here are some key differentiators that set Vumetric apart from the competition:

- **Certified Professionals**
  Our team of experienced and certified in-house ethical hackers hold the most recognized industry certifications including OSCP, OSCE, OSWE, GWAPT, GPEN, OSEP, CISA, CISSP and more.

- **Actionable Results**
  We deliver accurate, documented results and actionable recommendations. Our professional reports are suitable for both executive and technical stakeholders.

- **Industry Standards**
  Our penetration testing services are designed to help clients meet regulatory requirements, including SOC 2, ISO 27001, HIPAA, PCI DSS, and more.

- **Proven Methodologies**
  Our in-house team of ethical hackers provides advanced manual penetration testing using proven testing methodologies such as OWASP, OSSTMM, CREST and others,

- **Consistent Processes**
  Our company culture is firmly rooted in structured and efficient ISO 9001 certified processes. From project management workflows to penetration testing playbooks, we have formalized quality assurance and oversight to consistently deliver high quality results.

- **No Outsourcing**
  Our penetration testing services are delivered by full-time, in-house staff based in North America. We perform every project in-house, with a firm commitment to never outsource.

- **Experience & Reputation**
  Having completed thousands of client engagements across multiple industries, we're positioned as one of the most reputable cybersecurity assessment firms in the industry.

- **Responsive Team**
  We are known for our fast turnaround times and transparent communication at every stage of our projects, facilitating effective collaboration with our clients.