

Web Application Security Testing

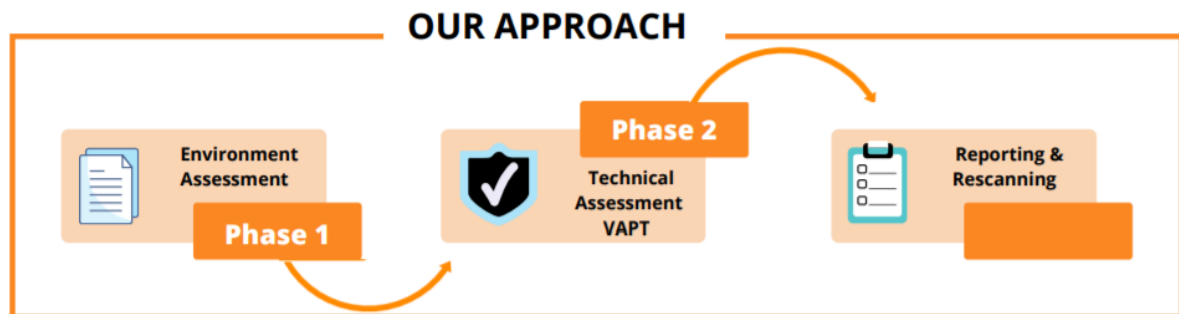
Web applications are unique constructs, mixing various forms of technology and providing an interactive front for others to use. Some web applications are made public, while others might be internal applications existing on an intranet. No matter the location, there are always security vulnerabilities. How well does your application handle input? Does it work with backend servers in a secure manner? Will your session management scheme hold up to penetration testing?

Web application penetration testing at Securze tests for the following:

- Application logic flaws
- Forced browsing
- Access and authentication controls
- Session management
- Cookie manipulation
- OWASP Top 10
- Horizontal escalation
- Vertical escalation
- Brute-force password guessing
- Poor server configuration
- Information leakage
- Source code disclosure
- Response splitting
- File upload/download attacks
- Parameter tampering
- URL manipulation
- Injection attacks for HTML, SQL, XML, SOAP, XPATH, LDAP, Command
- Cross-site scripting
- Fuzzing
- Cryptographic Issues
- Memory Corruption
- CVE

- Secure Design
- Manual tests

Methodology:



GREY-BOX TESTING

This one is the most common approach in security testing. With it, some information (like the credentials) is provided, but the rest is to be discovered by the tester.



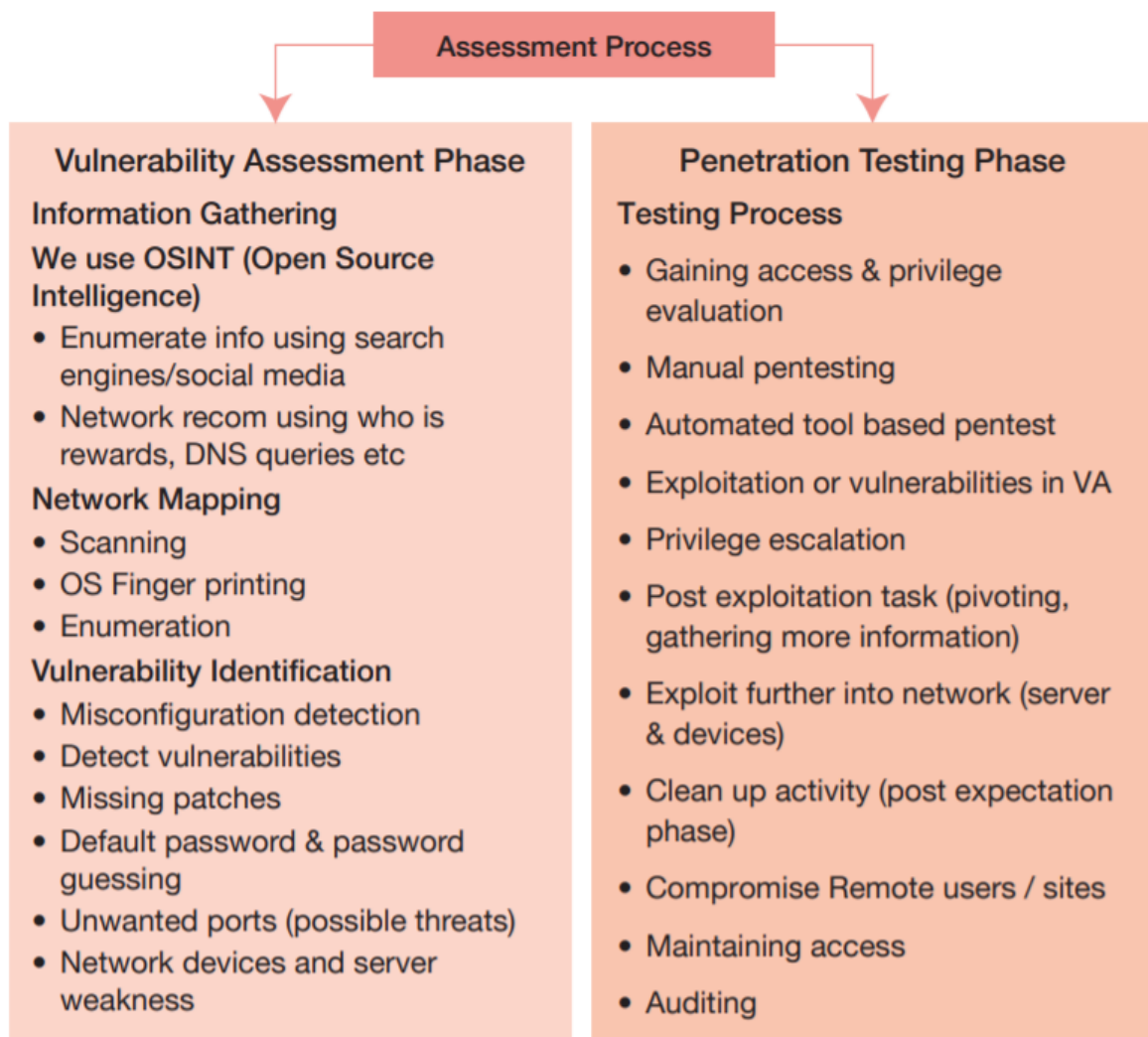
BLACK-BOX TESTING

With this approach, the tester has no prior knowledge of the app, which allows them to behave like user (or hacker) and exploit the publicly available info.

















WHITE-BOX TESTING

This method implies that the tester knows the app's ins and outs and has access to the source code and various documentation. White-box testing allows for faster testing and more sophisticated test cases.



Package Details & Pricing:

	Start-up Package \$– 1 Time	Corporate \$– 1 Time	Corporate Pro \$ – 1 Time
GDPR			
Managed vulnerability scan	 (Basic)	 (Advance)	 (Advance)
OWASP Top 10			
SANS Top 25 detection			
Application logic testing			
Web Application Firewall bypass			
Target Scope	Up to 1 Web Application	Upto 1 Web Application	Up to 1 Web Application
Zero false-positives guaranteed			
CWE, CVE and CVSS compliance			

GDPR			
Different user roles testing			
Pentest Reports			
Dedicated Consultant			
Customizable			

[Click Here](#) to inquire more about our other services.



Email: contact@securze.com

Phone Number: +91 8454051344 / +91 8451073938

Website: <https://securze.com>