Our Web Application testing methodology is aligned with OWASP (the Open Web Application Security Project).

A list of the major testing categories that Secarma will attempt to locate can be seen below:

1. Authentication attacks

a) Brute force
b) Insufficient authentication
c) Weak password recovery validation
d) CAPTCHA abuse
e) Cleartext credentials
f) User enumeration

2. Authorisation

a) Credential/session prediction
b) Insufficient authorisation
c) Insufficient session expiration
d) Session fixation/hijacking
e) Session replay
f) Cross-site requests forgery

3. Client side attacks

a) Content spoofing
b) Cross-site scripting
c) HTTP splitting

4. Command execution

a) Buffer overflow
b) Format string attack
c) SQL/XPATH/LDAP injection
d) OS Command Injection
e) Local/Remote File Inclusion

5. Email abuse

a) Open mail relay
b) Virus proxy
c) Virus sending
d) List recipient disclosure

6. Information disclosure

a) Directory indexing
b) Information leakage
c) Path traversal
d) Predictable resource location
e) Print/PDF information disclosure

7. Logical attacks

a) Abuse of functionality
b) Logical flaws
c) Logic bombs
d) Backdoors

8. Denial of service

a) Resource exhaustion
b) Host OS vulnerabilities
c) Thread deadlocking
d) Network configuration

9. Insufficient input/output validation

a) Client side only validation
b) Multi form consistency
c) Viewstate abuse

10. Invalid server configuration

a) Surplus modules
b) Proxying/caching
c) Application port scanning
d) Surplus/insecure/demo code running

Assessment will include both unauthenticated and authenticated assessment unless otherwise specified. Secarma recommends this to capture the risks of an opportunistic attacker without any access, and any rogue users.

We use a mixture of automated scanning and manual assessment. On request we can remove the automated part for sensitive applications which may have stability concerns.

Secarma provides world class application testing. Our consultants are active in the wider community and maintain or contribute to open source projects in this space. We also believe in passing knowledge on by speaking at events such as Defcon and OWASP.

Pre-Requisites

An application assessment is an easy project to facilitate. The following lists the prerequisites required to facilitate the engagement:

- Knowledge of the URL
- Access to two copies of all levels of user (to facilitate privilege escalation)
  - If your application has complex roles based privileges then consider providing access as: "Standard User", and as "Administrator".
  - Alternatively, if you have a "nightmare" scenario such a user in group A being able to access data from another user in group B. Then ensure that access is given for accounts in both group A and B.
- Consider providing access to the source code of the application.
  - This is an optional pre-requisite and you do not need to do so.
  - Experience has shown us that a higher quality of project is possible with access to the source code.
  - We would not be conducting a full review of the code (though we also sell that as a service).
  - Some flaws are easier to confirm with access to the source code. Or we can improve our remediation advice to tailor it to your environment.
- Disable any Web Application Firewall (WAF) or Intrusion Prevention System (IPS) for traffic from our source IP addresses.
  - By disabling protections our process can find underlying security exceptions. Secarma recommend addressing the root problems rather than relying on a filter which could be disabled.
  - The engagement will trigger significant alerts and doing this will prevent the operator being burned out by alerts.