T: +31 (0)30 63 36 260
E: support.digital@bdo.nl
www.bdo.nl

BDO Advisory B.V.
Postbus 4053, 3502 HB Utrecht
Van Deventerlaan 101, 3528 AG Utrecht
Nederland

Approach BDO security testing

BDO uses the following approach when performing penetration tests:

- Making an inventory of the goals determined in the scope; This involves investigating which (web) applications and (underlying) systems are present in the network.
- Identifying applicable services and open ports on the machine(s) or server(s) of the (web) application(s)
- Analysis and validation of vulnerabilities on the identified services/(web) applications.
- Filtering of false positives and classifying the risk using CVSS.
- Logical testing (ethical hacking) of the environment.
- Documentation of the findings, including clear evidence, classified risks, and recommendations for correcting them.

Methodologies

To perform the penetration test successfully and to be able to deliver maximum quality, BDO applies a combination of vulnerability assessment and penetration test methodologies that are based on international standards, recommendations, and guidelines. We supplement the methodologies with the experience and knowledge of our experts in the field. These methodologies include **OWASP ASVS, PTES, OSSTMM,** and **NIST 800-115.**

Our experience shows that this combination of methods yields the best approach and results. We have now used this for more than 100 clients, to the complete satisfaction and surprise of the depth of our findings.

Approach and methods used in infrastructure testing

For the optimal output and predictable results of infrastructure testing, we follow the approach below as a guideline to be able to test it in its entirety. This methodology is based on the PTES methodology with its additions. In addition to our expertise, we use both open-source and commercial tools. The tools used vary per test scenario to achieve the best results. In the approach below, we list the tools that we expect to use as a minimum for the successful execution of the test:

1. Reconnaissance - Mapping all machines and offering services (and version numbers) within the infrastructure. It looks at hosts, IP addresses, routes, and infrastructure locations.
2. Network analysis - It examines what can be concluded from non-encrypted network traffic in the infrastructure. This information can potentially be used to support further attacks.
3. Vulnerability and misconfiguration - It is checked whether vulnerabilities in the offered services and misconfigurations can be abused.
4. Exploitation and privilege escalation - Existing vulnerabilities are exploited, and whether horizontal/vertical privilege escalation is possible is checked. This is mainly done with manual exploitation and known (custom) scripts.

5. Network access control analysis - It is checked whether (wireless) network segmentation/segregation and Network Access Control are in use, whether this has been implemented correctly and whether there are ways to circumvent this.
6. Data exfiltration - It will be examined whether it is possible to exfiltrate data from the environment through manual analysis and actions with tools available in the appropriate environment.

Approach and methods used in (web) application testing

For the optimal output and predictable results of web application testing, we follow the approach below as a guideline to be able to test it in its entirety. This methodology is based on elements from the OWASP Top 10 with its additions to test the application accurately and the landscape it is located. In addition to our expertise, we use both open-source and commercial tools. The tools used vary per test scenario to achieve the best results. In the approach below, we list the tools that we expect to use as a minimum for the successful execution of the test:

1. Reconnaisance - Mapping of web application, (obsolete/vulnerable) frameworks and underlying infrastructure. It looks at host, IP addresses, routes and the location of infrastructure.
2. Input validation - Various 'injection' methods are being tried on the server, such as XSS, XXE, SQL injections, and the following vulnerabilities, such as clickjacking. It also checks whether malware can be uploaded.

3. Error handling test - This looks at the behavior of the web application when it receives erroneous or malicious input. Error messages can contain sensitive data.

4. Infrastructure test - All (web) services are mapped through port scanning (e.g., SSL/TLS, HTTP testing, etc.) and whether there are exploitation possibilities of the services offered.
5. Authentication, session, and authorization tests – We perform 'account enumeration', misconfigurations, ways to bypass security (bypass) and ways to get extra privileges in a system and get deeper into the system (horizontal/vertical privilege escalation). In addition, it is checked whether files, folders or other components can be accessed unintentionally.

6. Cryptographic test - Various tests against SSL/TLS ciphers, protocols, and cryptographic errors.

7. Logging and monitoring test - During this test, it is checked whether there is an indication that logging and monitoring are present. This includes looking at the presence of a WAF or specific headers (such as CSP).

Rapportage

The investigation results in a report; the content and structure will be further coordinated with the persons involved from Customer. By default, we report in English, and our report consists of the following parts:

A management summary, including:

- The period (date/time) in which the test took place.
- A summary and description of the main risks, including per risk:
    - A description according to which crucial digital access paths have been tested, how this has been determined, paying attention to the attack surface (internal, external, both);
    - Technical and organizational advice to mitigate the risks.

Technical overview, including:

- Detailed overview of the findings identified, including:
  - Location and IP addresses from which the test was performed;
  - Finding, substantiation, and possible risks;
  - Categorization of finding based on applied security guidelines;
  - Recommendation/advice to mitigate the risks of findings;
  - For which systems/applications and to which places within the application, the finding applies;
  - A unique serial number for each finding;
  - Score structure according to the Common Vulnerability Scoring System (CVSS 3.1), with a description of whether a test finding is low, average, high, or critical.
- Methodology, technique, and parameters used to reproduce findings;
- If relevant, a description of the applications/tools used, including version number;
- If deviating from this plan of approach, a description of the chosen approach/methodology applied during the execution of the security test and, if deviating, a total overview of all tested vulnerabilities.

The test results will be presented to relevant stakeholders on location or via Teams. One of the testers will be present during the presentation to elaborate on the findings. The presentation date will be agreed upon after the test has been carried out.