VULNERABILITY ANALYSIS & PENETRATION TESTING

Secura delivers world-class security testing services. One of our most valued services, and the service with the longest history within Secura, is Vulnerability Analysis and Penetration Testing. Secura started testing for customers in the year 2000 and has been a renowned party in security assessments ever since.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

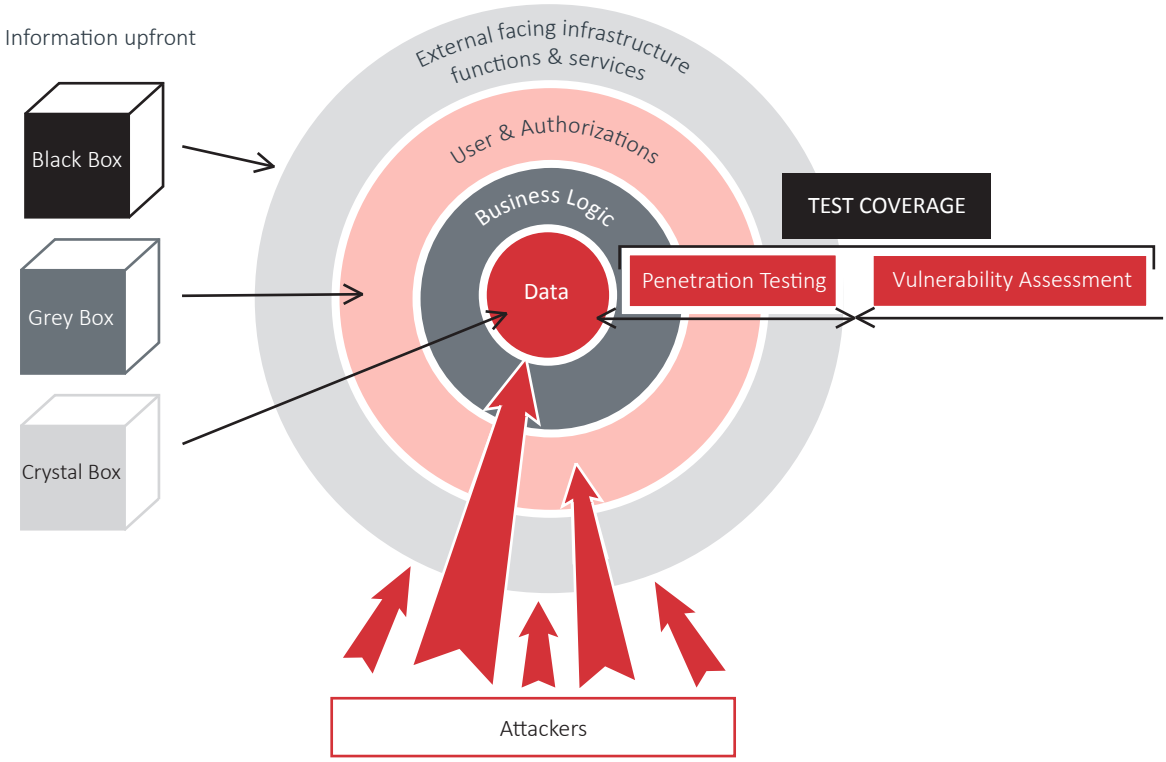
VULNERABILITY ANALYSIS & PENETRATION TESTING

Whether our customers are banks, healthcare providers, utilities, software businesses or government institutions, they all require some form of security testing of their external, online and in-house information systems. Secura offers professional testing services on nearly all types of applications, infrastructures, and devices. With over 18 years of working for our clients, our team is equipped with all the knowledge and hands-on experience you would expect. In this brochure we will explain Secura's view on this particular type of service.

WHY SHOULD YOU TEST?

Companies are more and more dependent on data. Be it for sales, R&D, or their actual product portfolio. Protecting this data is vital, and often also compulsory (for instance when it concerns personal information). Data is accessed by authorised users through applications that contain business logic and security functions. If any weaknesses exist in these access layers, then risks will arise to the business. In order to be in control of these risks, it is necessary to assess the security measures by testing their effectiveness.

SECURITY ASSESSMENT APPROACH



HOW DO WE TEST?

Somewhere after 2010, penetration testing has become to be seen as somewhat of a commodity service in the professional services landscape. Many companies offer fully automated testing and rely on tools for all the work: humans only help translate the results to a readable report and remove false positives. At Secura, we do not believe this approach can ever provide a full view of all the risks. In fact, we frequently find critical issues in previously automatically tested environments.

This is why we test using a combination of automated tools and manual methods. The automated tools are good for catching all easily identified and repetitive cases in the external and internal infrastructure, functions and applications. However tools cannot analyse business logic failures, data leaks, missing security controls or incorrect authorisations within an application. For this, human interaction is necessary. And even for the cases where automated tools are useful, they still always provide some measure of false positives that need to be validated manually and the need identify false negatives always remains.

Our manual tests follow a methodology that was developed in an iterative way, using our own experience, and closely following established security testing frameworks such as the OSSTM and OWASP Testing Framework. Where relevant, we perform Threat Modeling sessions following Microsoft's STRIDE methodology as an initial assessment of where to focus our efforts. We also hugely value knowledge sharing in our team. This is why we regularly update our methodology with the newest insights and have our security specialists work in teams (minimum of two persons) on projects. This is equally true when testing a web application, an IoT device or performing a source code audit.

SCOPING A TEST

Security testing is very different from functional testing. In functional testing, you would try to validate all use-cases. In security testing, we try to identify risky behavior of applications (and infrastructures) for all other cases: expect a username as input? Let's see what happens when we provide a piece of executable code instead… Vulnerability assessment and penetration testing therefore covers many aspects of security, and can have varying levels of depths and scope, depending on the risk profile of the object we are testing.

Important variables that determine what type of tests we can and will execute are for instance:

- Is it an application, middleware, of infrastructure?
- Is the system under a test a Mobile App? SCADA/ ICS? IoT device? WiFi network?
- Do we get to log in as a normal user, so we can see if we can access other users' data?
- Is the source code available to us?
- The available budget.
- Does the customer want a continuous form of security assurance?
- Does the report need to be used for external stakeholders?

TYPES OF TESTS

The information upfront and the depth of testing are related. The information upfront is often described in terms of 'black box' testing, 'grey box' testing or 'white/crystal box testing'. These terms relate to the amount of information available to us beforehand.

A **black box test** is generally associated with a test where we do not know anything beforehand except the target addresses. Black box testing provides you with an answer to the question: "What could an average attacker with limited time and resources do?". Black box testing typically uncovers 'low hanging fruit', but lacks the depth necessary for an answer to questions such as "how well protected is my data really?". In black box testing, a vulnerability assessment is carried out, identifying entry points for an attacker. Further penetration of the deeper layers is then performed by exploiting concrete vulnerabilities. Since no credentials (usernames and passwords) are available to us, most business logic issues and authorization model failures, will not be identified. However, you will have an excellent view of all attack surfaces an attacker could abuse, using black box testing.

In a **grey box test** we have credentials to log in, often for various roles (e.g.: user, supervisor, administrator). This is hugely important if the application or device in question contains any sensitive data, such as medical, financial or other data that should only be available to certain users or roles. "Can a user access the data of another user?", is a question we can only answer adequately with a grey box test. This type of test is the most common for our clients. Black box testing is usually also a part of grey box testing, so that you will be able to differentiate between vulnerabilities that are available to external attackers, and vulnerabilities that can be exploited by authenticated users only.

Finally, in a **crystal box test**, we have the source code (or full configuration information of infrastructure components) while performing grey box testing. While we normally will not perform a full source code review during a vulnerability or penetration test, we do use the source code to identify vulnerabilities in security functions. Especially vulnerabilities in input validation, cryptographic handling and authorization models can be found much more efficiently this way. Having access to the source code or detailed configuration information during a test allows us to answer the question: "How well protected is my data really?".

Keep in mind though, that the distinction between black, grey and crystal box testing is not a strict one, mixing forms is possible. For instance, a common combination when testing web application security is to perform black box testing on the infrastructure, and grey box testing on the application itself. Another common black box penetration test is a penetration test of the internal network (plug in and see how far you can get). In such an internal penetration test we have no information upfront and we try to get access to all the data via exploiting vulnerabilities (usually by gaining domain administrator rights during that process).

TEST TARGET

Another type of test that deserves special mention here is mobile app testing. We offer in-depth testing for mobile applications, both on the iOS platform and Android. More than a tools-based test of only the mobile app, we can assess the mobile app, including the communication to the back-end, and the back-end application. This provides a complete view of the security, as opposed to looking at just the app on the smartphone. Our offering for mobile testing is described in more detail in the Mobile testing brochure.

IoT device testing is also one of our strong subjects. It is also a very fast growing market for Secura. IoT devices are often used in environments that can be hostile (direct internet connections, physical hacking). It is therefore extremely important that security functions such as

cryptographic protections, secure firmware updates and secure authentication are implemented adequately. We have capabilities in this area that many competitors lack, such as 2G, Bluetooth and WiFi communications interception and manipulation, firmware extraction and to a limited extent also hardware security testing. Combined with application-level testing, this means we can provide very solid assurance of the security level of an IoT device (be it a webcam, alarm system, car or MRI-scanner).

Many other questions are relevant, and our sales team will gladly take you through the intake process to determine the appropriate scope and depth. Types of security assessment services Secura often performs are for instance:

- External application penetration test (grey box);
- Black box infrastructure vulnerability assessment;
- Internal network penetration test;
- Mobile Application assessment;
- IoT device penetration test;
- Web Application source code review and penetration test;
- SOAP/REST API penetration test;
- Vulnerability scans on internal network;
- Crystal box infrastructure assessment.

WHAT DO YOU GET?

All our Vulnerability Analysis and Penetration Testing services result in a written report. This report contains an introduction, a management summary describing all the important risks we identified, and a technical section describing the steps we took to identify the risks. This means that in contrast to many other providers, your developers and engineers will be able to repeat our actions using the information in the report, and validate for themselves what we found. As we have dedicated teams running these vulnerability assessment and penetration tests all the time, you also have assurance that all major risks are known to you and can now be mitigated. In our report we tell you what to fix, and with what priority. Our recommendations are actionable and scored: you will know exactly what to do first.

RELATED SERVICES

Secura provides a full spectrum of security services. Typically, our customers have more needs than just Vulnerability Analysis and Penetration Testing services. Related services that Secura offers are for instance:

- **Mobile App testing**: Mobile apps these days are an integral parts of our lives. When testing the security of apps, we do not just look at the app, but at thSSSe full chain, from user, through device, frameworks, resources, network and back-end server.
- **Source code analysis**: When testing an application, we can investigate the important parts of the source code. But it is also possible to take an automated look at the source code. This will provide you with not only security vulnerabilities, but also a view on code quality, maintainability and readability.
- **Continuous Application Scanning**: In modern development environments, a bi-weekly release schedule is common. In those cases, in-depth manual testing is not always feasible, both time-wise and budget-wise. Nevertheless we can offer an extremely valuable automated, periodic scanning service for on-line applications where we use state-of-the-art application vulnerability scanners such as IBM's AppScan, combined with our human experience to provide a periodic report with technical security findings and trend analyses.
- **Red Teaming**: Where vulnerability and penetration testing focus on specific applications and environments, they do not tell you about the general resistance against cyber attacks on your whole organization. In a Red Teaming exercise, we will emulate a full cyber attack, including organisational and process attacks, social engineering and technical vulnerabilities.

INTERESTED?

Would you like to learn more about our services? Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com