SANAE
GO LIVE with us

**SANAE, s. r. o.**
Kopanice 3570/6
821 04 Bratislava

# TEMPEST – Project execution

## Summary

TEMPEST requested testing project execution at the latest stage of a multi-year project of a state procurement portal. Client needed a test analyst with technical background to provide performance, penetration testing, and ethical hacking.

Project length: 4 months

Technology to test: Web base application focused on e-procurement

Used tools: Kali Linux, nmap, meterpeter, dirbuster, Subgraph Vega, Jmeter 4, Fiddler

Keywords: JSON,XSS,SQL,OWASP,performance testing, stress testing, penetration testing, webservices, EH, ethical hacking, exploits

## Solution

Introducing the candidate

SANAE swiftly responded to TEMPEST needs by providing several suitable candidates from its' internal headcount. Client selected one candidate and agreed on short-term contract.

Working on the project

**Ethical hacking and penetration testing**

**Analytical phase:**

This phase consisted of analyzing the SUT from the TEMPEST, studying the data model and software and hardware firewalls , and communication with individual SME (networking, hardware infrastructure) in order to obtain a complete picture of the data flow and possible exploits of the SUT . This was accomplished by creating a plan of the attack.

**Testing phase:**

All the penetration testing and hacking activities were concluded only on designed dates during nights and weekends to prevent non-functional testing environment during office hours. The tests itself consisted examining vulnerabilities like: open ports, cross-scripting, SQL injections, exploits. Many of these included the need to use different tools to query port

**SANAE, s. r. o.**
Kopanice 3570/6
821 04 Bratislava

traffic using the Kali Linux tools or writing small bash or python scripts. The report of achieving OWASP security standards was made partially by Subgraph Vega.

**Performance testing**

**Analytical phase:**

This phase consisted of analyzing the application from the TEMPEST, studying the both public and secured parts of the portal, and communication with individual SME (networking, development) in order to obtain a complete picture of the processes of the SUT. This was accomplished by creating Jmeter projects.

**Testing phase:**

All the performance and stress testing activities were concluded by Jmeter tool. The tests itself consisted measuring backend resources load and reaction times. Also was provided a stress test for the designed parts of the system for extreme (10x of the normal) overload and spikes (20x). One of the test cases caused a blocking issue, which was surplus for the security but problem for the performance test run. This issue required deep and extensive analysis from our test analyst. Based on these results and intensive communication with other teams there was a threat of fail. After confirmatiom from the development that we need to use an alternative method to test this case. Aligned with the dev our conclusion was communicated to the project manager, he decided to accept our arguments and agreed to amend the test case, so the development created a webservice, through this webservice the test case was successfully completed.

## Benefits

TEMPEST benefits from cooperation with SANAE on long-term basis gaining individual and professional approach, access to highly qualified and experienced professionals with warranty. The main benefit for the client was long-term experience in IT, strong technological background and flexibility of resource – work upon monthly requests, making the tester available just for the time of the project need.