SWORDSEC

PENETRATION TESTING SERVICES

2025

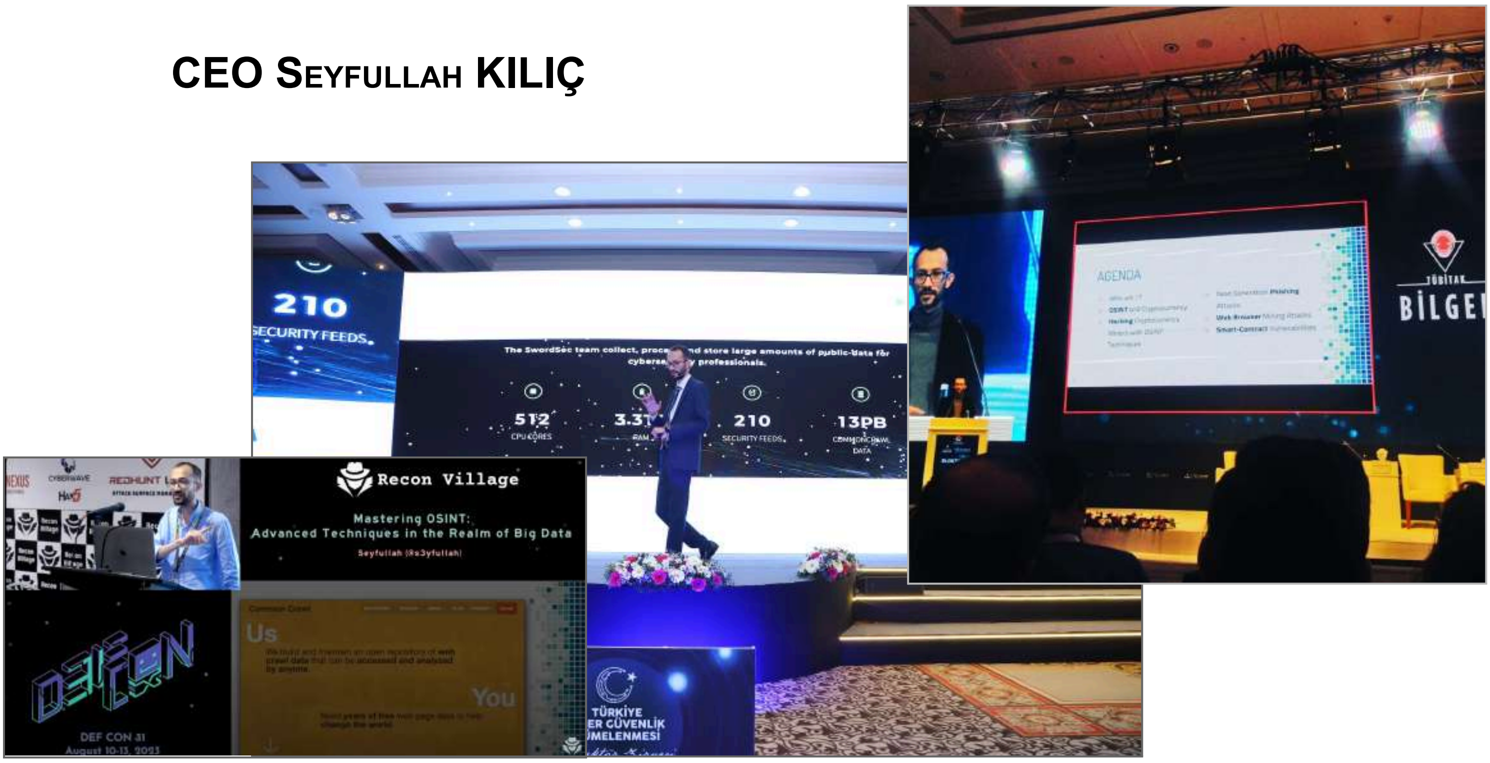
www.swordsec.com

SWORDSEC

PENETRATION TESTING SERVICES

Contects

CEO Seyfullah KILIÇ



Seyfullah KILIÇ, the Founder and CEO of SwordSec, has been working with the mission of making the digital world more secure since **2007** as a white-hat hacker and cybersecurity researcher. He has identified critical security vulnerabilities in globally recognized platforms such as **Facebook**, **Twitter**, **Apple**, and **CERN**, contributing to strengthening their defenses. His contributions have also been recognized on **Google**'s Security Hall of Fame.

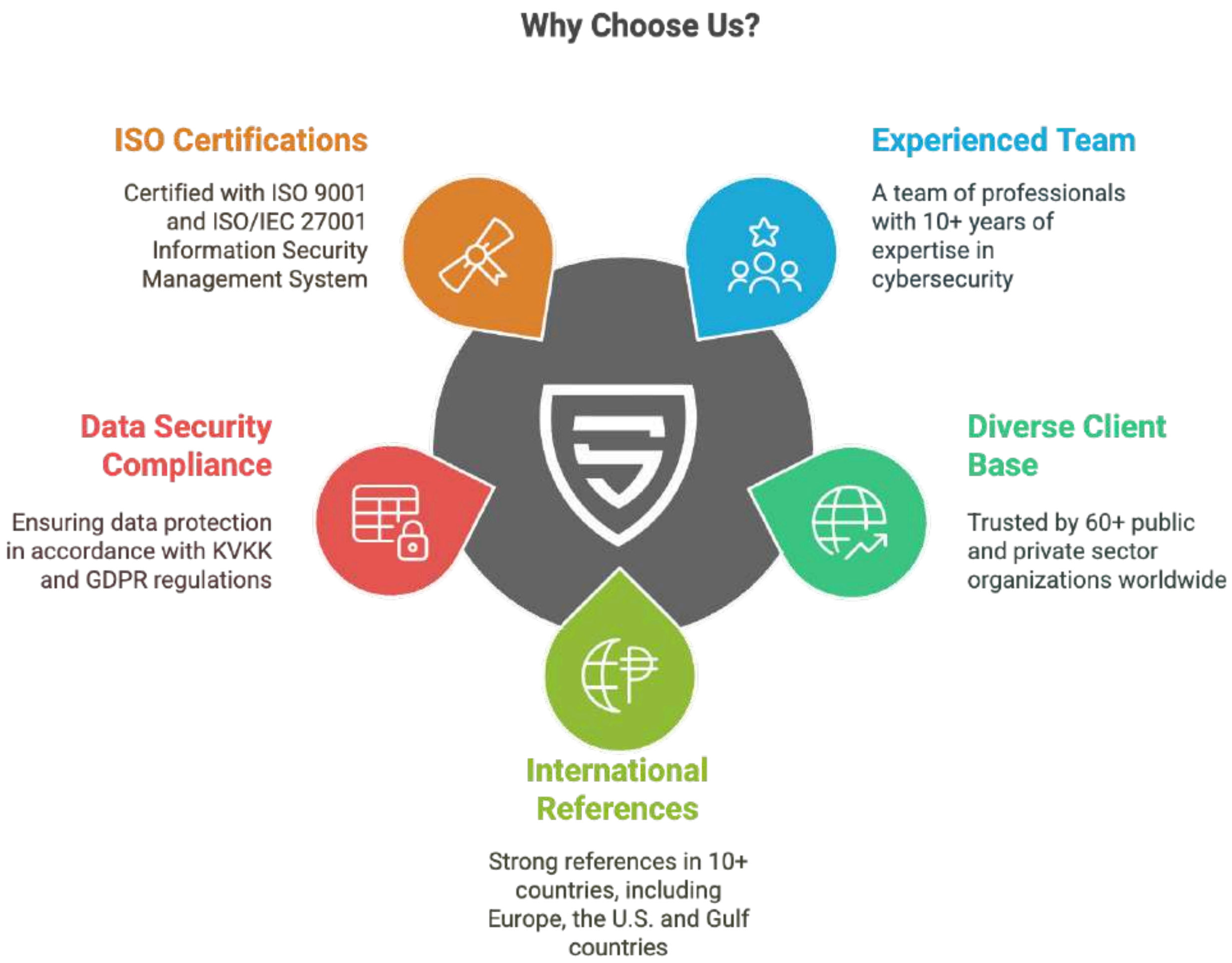
Seyfullah KILIÇ prioritizes knowledge sharing and industry awareness. He has spoken at 20 prestigious cybersecurity events worldwide, including **DEFCON** Las Vegas, **BlackHat** London, and **HackIT** Kiev. Additionally, he has delivered presentations at over 20 universities and leading cybersecurity conferences, continuously sharing his expertise with the community.

At **SwordSec**, we go beyond being just a service provider—we act as a trusted cybersecurity partner, ensuring that our clients' digital assets remain secure. With deep expertise, cutting-edge solutions, and a commitment to innovation, we help businesses stay one step ahead in the digital landscape.

About Us

SwordSec, established in **2018**, is a cybersecurity R&D firm offering “Next Generation Cybersecurity Solutions” to the markets of Turkey, Europe, and the USA. Our team consists of engineers with over **10+ years** of experience, white-hat hackers, and software developers. By closely monitoring and analyzing attackers’ methods, we provide our clients with effective and unique cybersecurity solutions.

Since 2018, we have provided cybersecurity services to leading organizations in nearly 10 countries, including Turkey, Romania, Qatar, Bahrain, and Portugal. Our references include **Turkish Airlines**, **ING Bank Romania**, and the **Qatar Armed Forces**. SwordSec is also a founding member of the Turkey Cyber Security Cluster, operating under the Presidency of Defense Industries of the Republic of Turkey.



Why Choose Us?

ISO Certifications

Certified with ISO 9001 and ISO/IEC 27001 Information Security Management System

Experienced Team

A team of professionals with 10+ years of expertise in cybersecurity

Data Security Compliance

Ensuring data protection in accordance with KVKK and GDPR regulations

Diverse Client Base

Trusted by 60+ public and private sector organizations worldwide

International References

Strong references in 10+ countries, including Europe, the U.S. and Gulf countries

REFERENCES

PRESIDENCY OF THE REPUBLIC OF TÜRKİYE SECRETARIAT OF DEFENCE INDUSTRIES	REPUBLIC OF TÜRKİYE MINISTRY OF NATIONAL DEFENCE	REPUBLIC OF TÜRKİYE MINISTRY OF TREASURY AND FINANCE
TURKISH AIRLINES	ING	dpd
الأهلي ABK		MTi AMERICA
BAI EUROPA	BtcTurk	EUREKO SİGORTA
papara	HAVELSAN	TÜRKSAT
REKABET KURUMU COMPETITION AUTHORITY	ENERJİSA ÜRETİM	KoçSistem
TOFAŞ TÜRK OTOMOBİL FABRİKASI A.Ş.	misli	otelz

* For all our references: swordsec.com/ref

Corporate Identity

Company Name: Swordsec Siber Güvenlik Teknolojileri Anonim Şirketi

Tax Office: İvedik

Tax Number: 7810864284

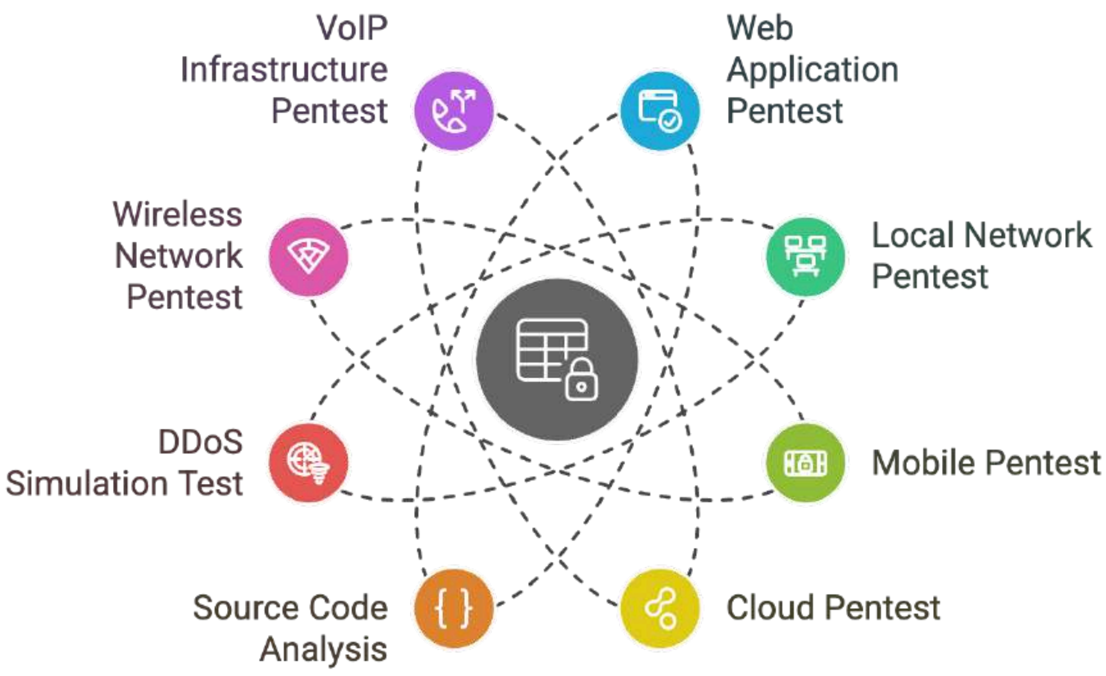
Trade Registry Number: 416430

MERSIS Number: 0781086428400001

DUNS Number: 519843806

Kep Address: swordsec@hs01.kep.tr

Swordsec Penetration Testing Services



Web Application Pentest Service (Web Security)

Security tests are conducted on your organization's publicly accessible services, including Mail, DNS, Web, FTP, and more. Our expert team performs comprehensive penetration testing from an attacker's perspective, identifying vulnerabilities and security flaws. All tests comply with international standards and methodologies. A sample report and methodologies are provided in the appendix.

Local Network (Network) Pentest Service

To identify security risks and potential threats within your local network, internal penetration tests are conducted. Our team examines vulnerabilities arising from connected clients and devices, detecting misconfigurations and weaknesses, which are then compiled into a detailed report.

Mobile Pentest Service

Mobile security assessments are conducted on applications developed for Android and iOS platforms, using both static and dynamic testing techniques. Hybrid mobile applications are also included in the scope. Penetration tests identify security vulnerabilities, which are then analyzed and documented in a detailed report.

Cloud Pentest Service

Your organization's cloud servers and services undergo security testing. Using advanced OSINT techniques, our team identifies misconfigurations, security vulnerabilities, and unauthorized access risks. Network security, system configurations, and security devices are thoroughly examined and reported.

Source Code Analysis Service

The source code of your applications is analyzed in-depth to detect security vulnerabilities. This service ensures that your organization, partners, and customers' software products are protected against cyber threats. Identified weaknesses are documented in a comprehensive report with recommendations for mitigation.

DDoS Simulation Test Service

A detailed analysis of your organization's entire internet infrastructure is performed, followed by real-world DDoS attack simulations. Distributed servers are used for testing, scaling up to 50 Gbps, allowing us to measure your system's resilience under high-traffic conditions. Weak points are identified, and recommendations are provided for strengthening your defenses.

Wireless Network (Wi-Fi) Pentest Service

Your wireless network infrastructure is thoroughly analyzed to detect potential external attacks. Misconfigurations, security gaps, and vulnerabilities are identified and compiled into a detailed security report.

VoIP Infrastructure Pentest Service

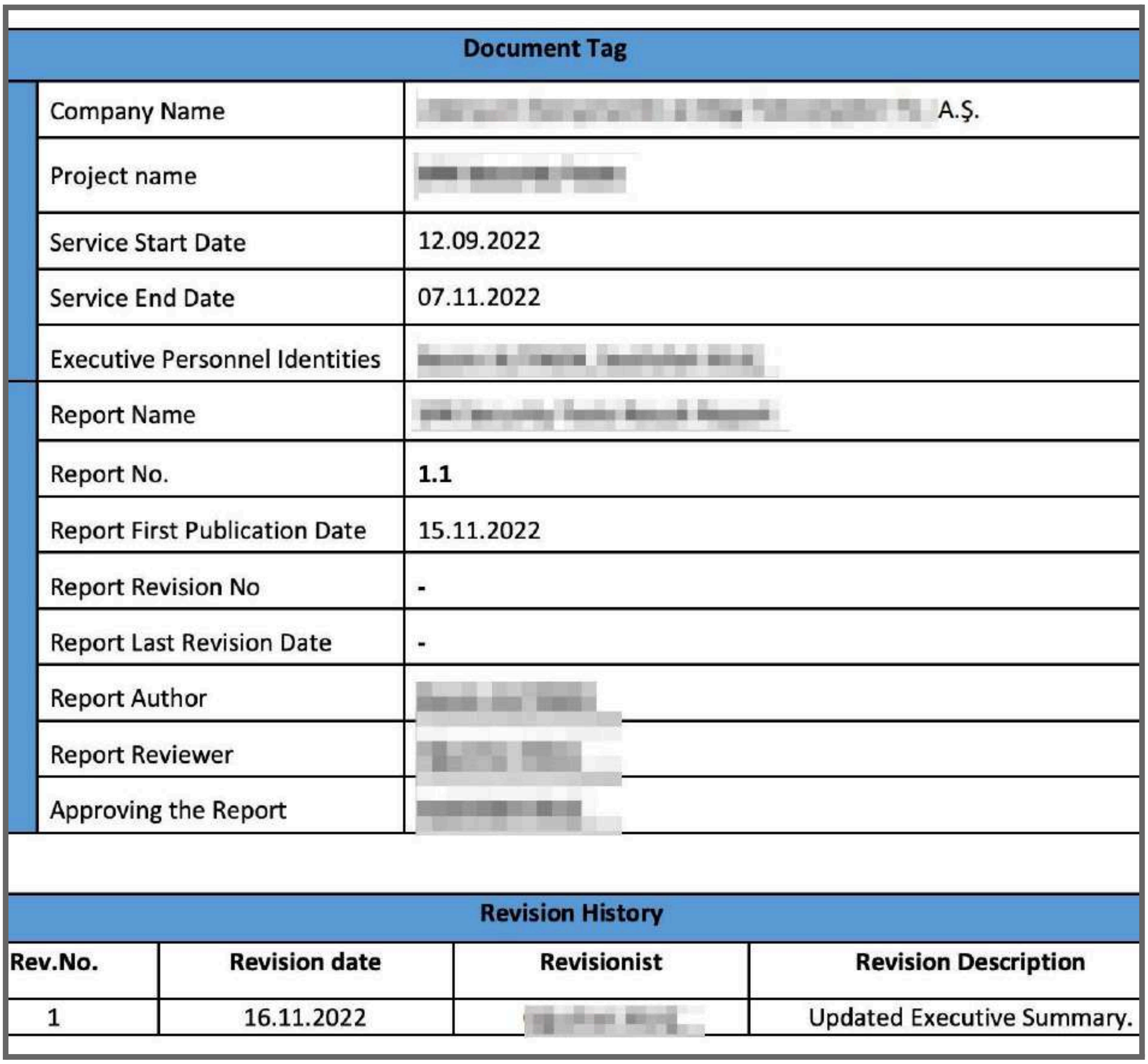
A security assessment of your organization’s IP/VoIP system is conducted, identifying vulnerabilities and potential attack scenarios. All security weaknesses in your VoIP infrastructure are reported along with recommendations for strengthening the system.

Social Engineering / Phishing Test Service

Social engineering attacks are simulated to assess the security awareness of employees. Phishing tests are conducted using real-world attack scenarios, measuring employees’ responses to malicious links and fraudulent emails. Additionally, customized phishing and social engineering scenarios can be designed based on your organization’s needs. The results help enhance employee security awareness, and training programs are provided to improve internal security measures.

Sample Penetration Test Report

The following data includes sample screenshots from a penetration test report. Our penetration testing methodology and techniques are exclusive to our firm, developed based on our expertise and experience, and supplemented with licensed security tools.

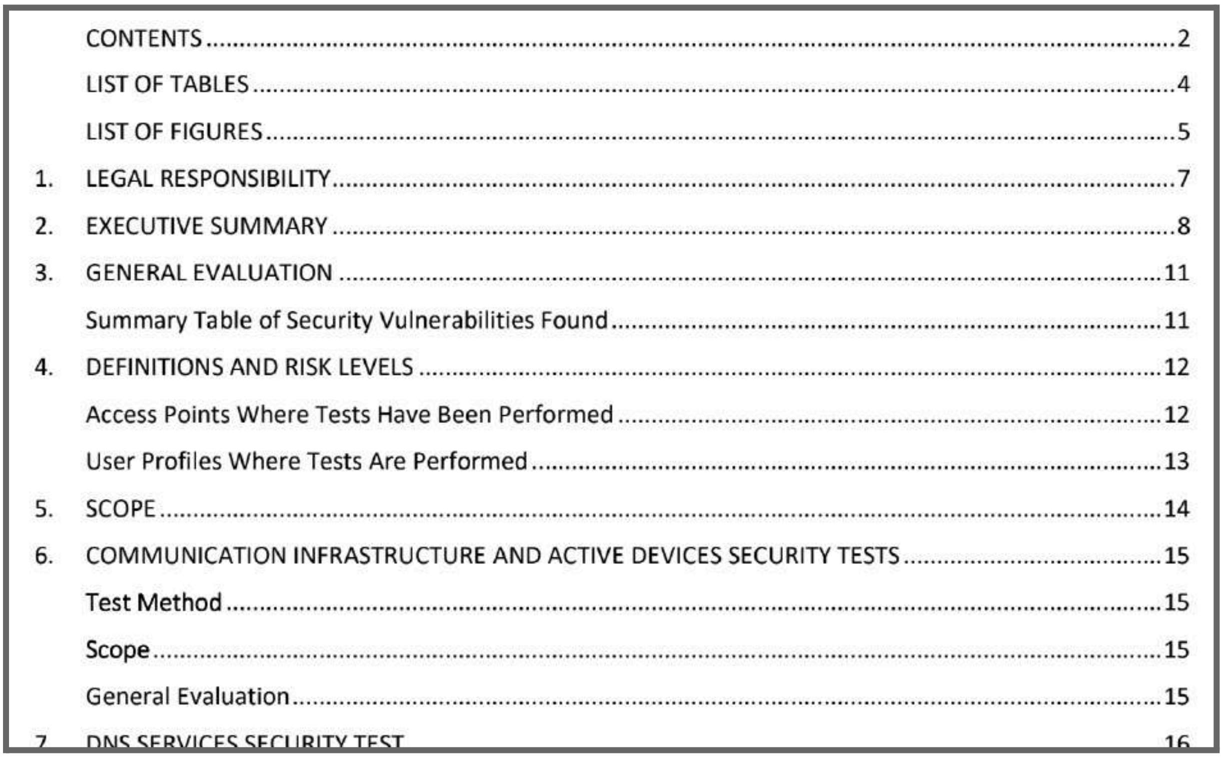


Document Tag	
Company Name	[redacted] A.Ş.
Project name	[redacted]
Service Start Date	12.09.2022
Service End Date	07.11.2022
Executive Personnel Identities	[redacted]
Report Name	[redacted]
Report No.	**1.1**
Report First Publication Date	15.11.2022
Report Revision No	-
Report Last Revision Date	-
Report Author	[redacted]
Report Reviewer	[redacted]
Approving the Report	[redacted]

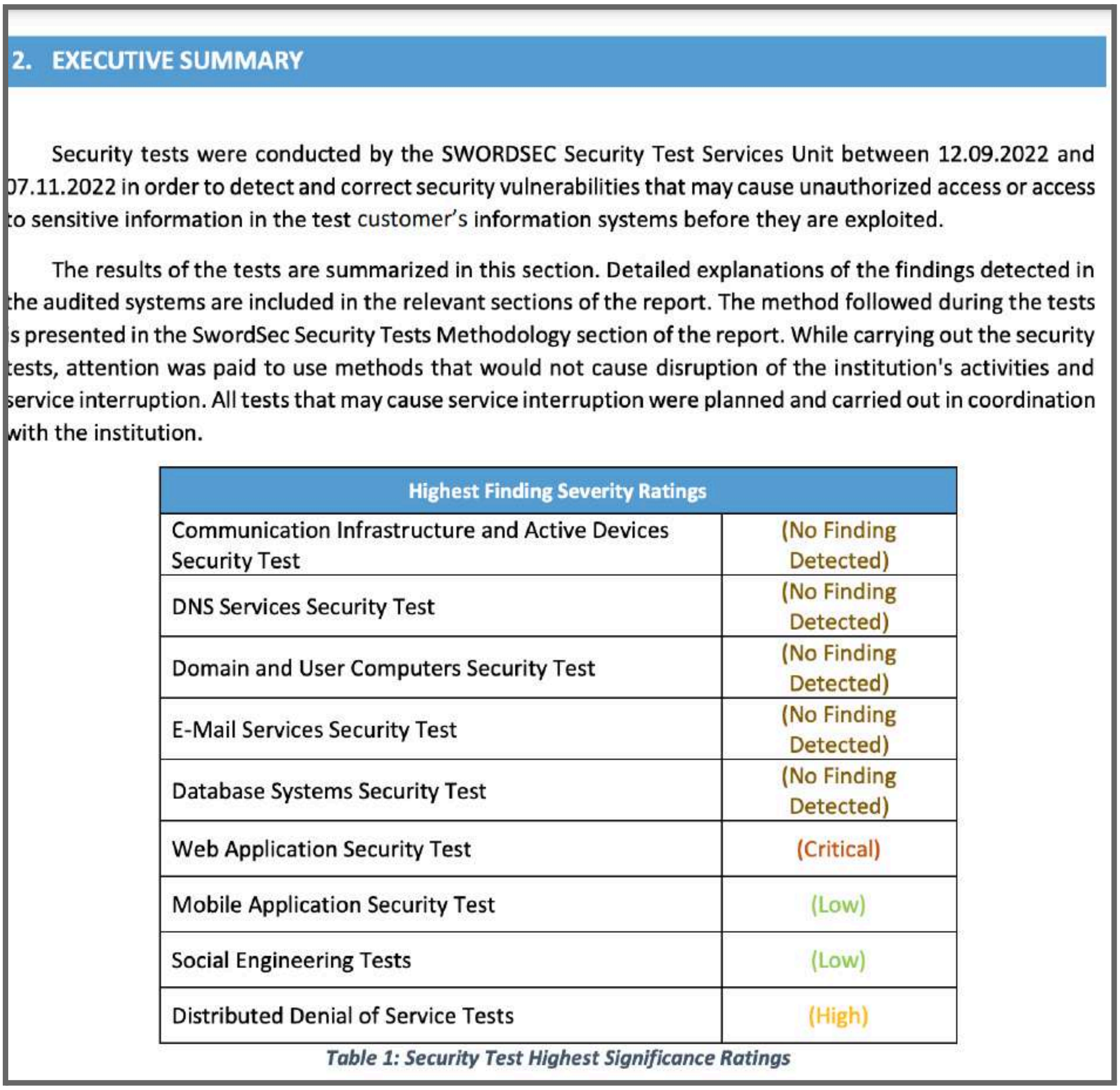
Revision History

Rev.No.	Revision date	Revisionist	Revision Description
1	16.11.2022	[redacted]	Updated Executive Summary.

Penetration Test Report Cover



Penetration Testing Contents



2. EXECUTIVE SUMMARY

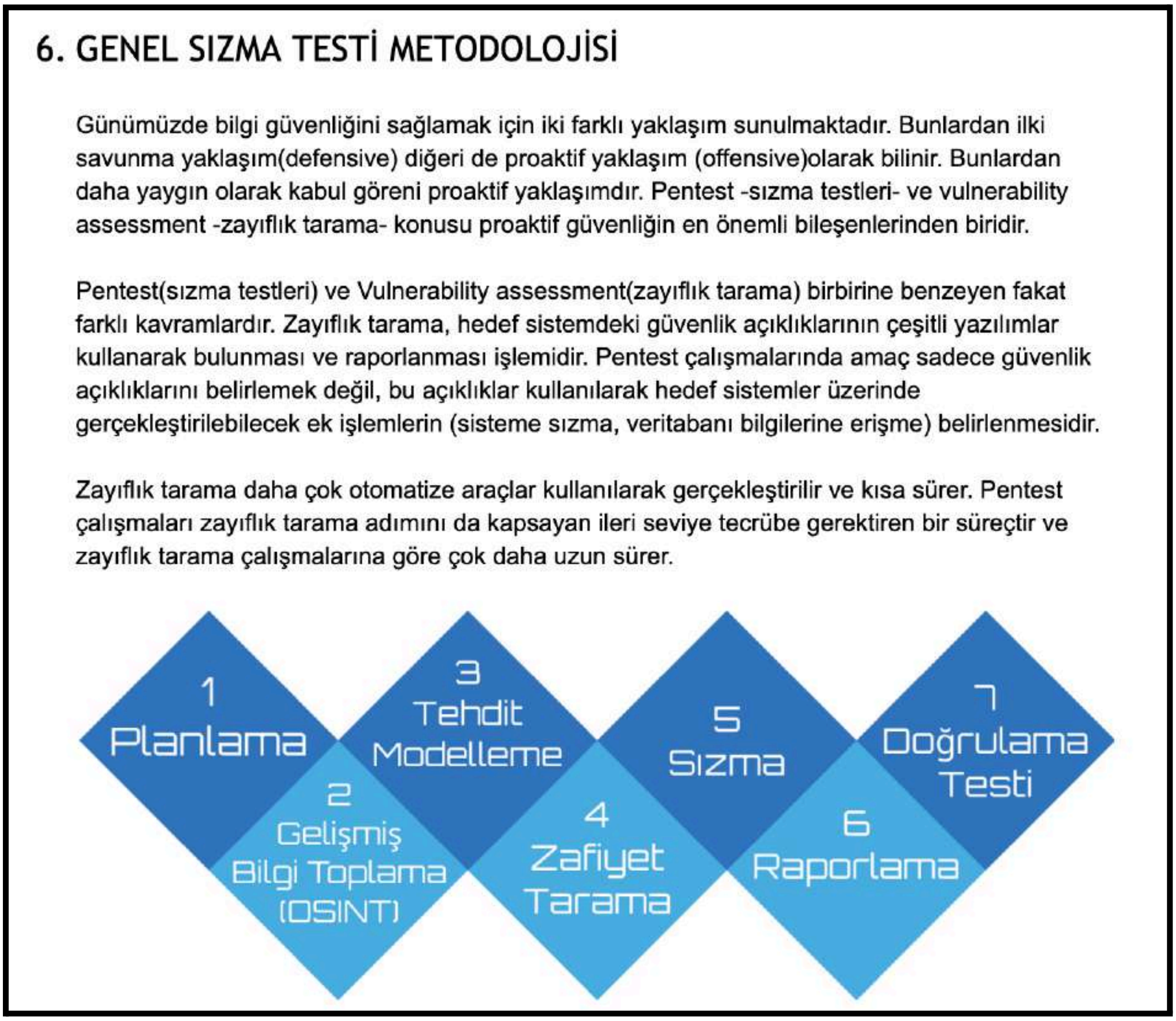
Security tests were conducted by the SWORDSEC Security Test Services Unit between 12.09.2022 and 07.11.2022 in order to detect and correct security vulnerabilities that may cause unauthorized access or access to sensitive information in the test customer's information systems before they are exploited.

The results of the tests are summarized in this section. Detailed explanations of the findings detected in the audited systems are included in the relevant sections of the report. The method followed during the tests is presented in the SwordSec Security Tests Methodology section of the report. While carrying out the security tests, attention was paid to use methods that would not cause disruption of the institution's activities and service interruption. All tests that may cause service interruption were planned and carried out in coordination with the institution.

Highest Finding Severity Ratings	
Communication Infrastructure and Active Devices Security Test	(No Finding Detected)
DNS Services Security Test	(No Finding Detected)
Domain and User Computers Security Test	(No Finding Detected)
E-Mail Services Security Test	(No Finding Detected)
Database Systems Security Test	(No Finding Detected)
Web Application Security Test	(Critical)
Mobile Application Security Test	(Low)
Social Engineering Tests	(Low)
Distributed Denial of Service Tests	(High)

Table 1: Security Test Highest Significance Ratings

Penetration Testing Executive Summary



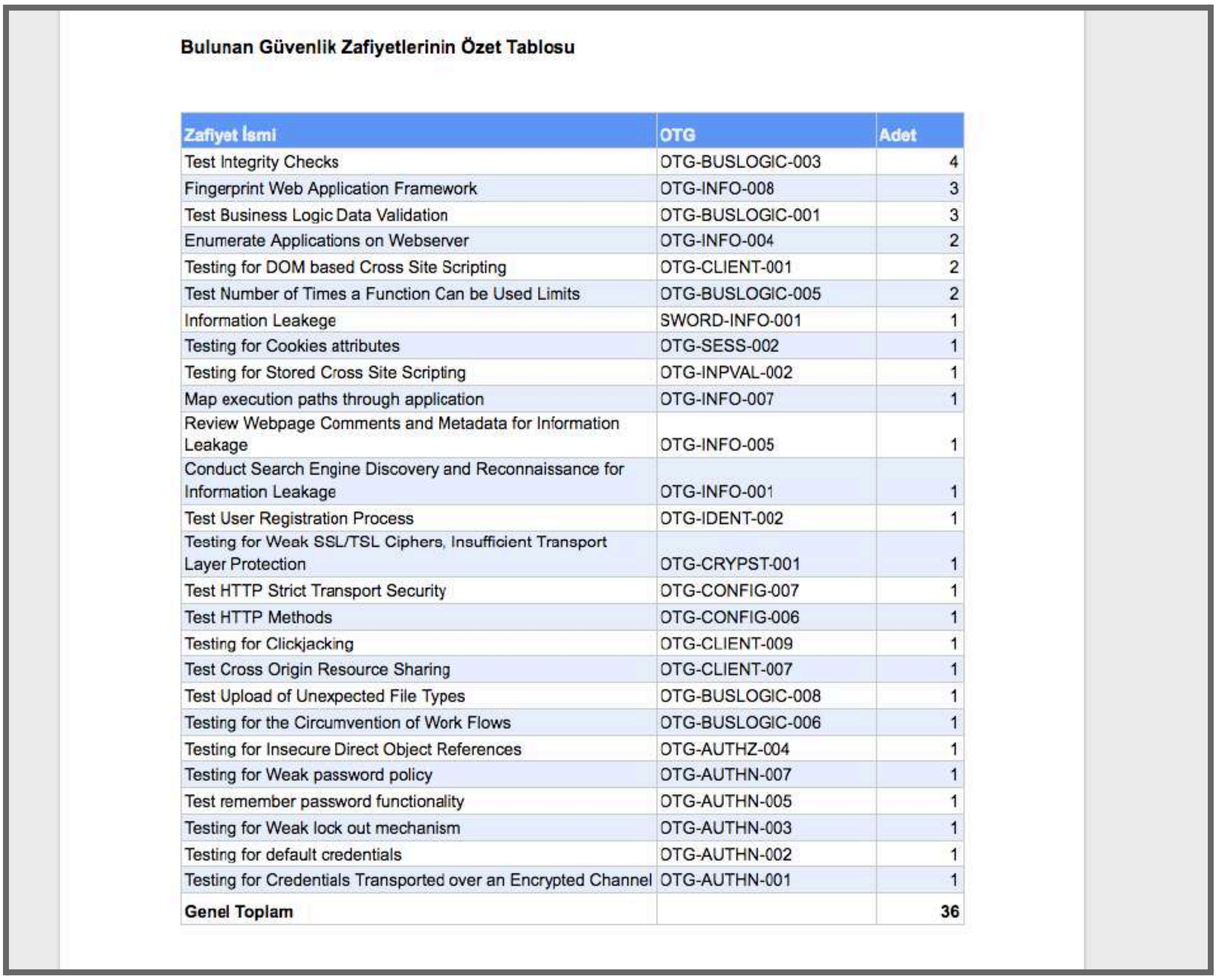
6. GENEL SIZMA TESTİ METODOLOJİSİ

Günümüzde bilgi güvenliğini sağlamak için iki farklı yaklaşım sunulmaktadır. Bunlardan ilki savunma yaklaşım(defensive) diğeri de proaktif yaklaşım (offensive)olarak bilinir. Bunlardan daha yaygın olarak kabul göreni proaktif yaklaşımdır. Pentest -sızma testleri- ve vulnerability assessment -zayıflık tarama- konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Pentest(sızma testleri) ve Vulnerability assessment(zayıflık tarama) birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama, hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Pentest çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir.

Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Pentest çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.

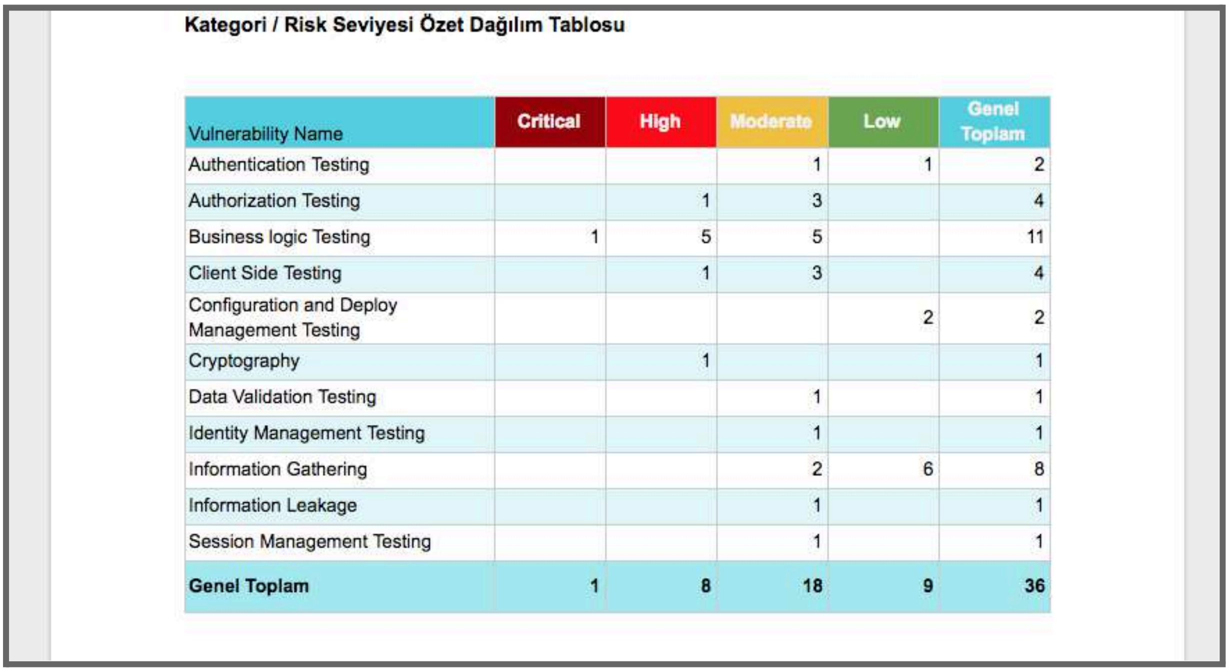
Our methodology



Bulunan Güvenlik Zafiyetlerinin Özet Tablosu

Zafiyet İsmi	OTG	Adet
Test Integrity Checks	OTG-BUSLOGIC-003	4
Fingerprint Web Application Framework	OTG-INFO-008	3
Test Business Logic Data Validation	OTG-BUSLOGIC-001	3
Enumerate Applications on Webserver	OTG-INFO-004	2
Testing for DOM based Cross Site Scripting	OTG-CLIENT-001	2
Test Number of Times a Function Can be Used Limits	OTG-BUSLOGIC-005	2
Information Leakege	SWORD-INFO-001	1
Testing for Cookies attributes	OTG-SESS-002	1
Testing for Stored Cross Site Scripting	OTG-INPVAL-002	1
Map execution paths through application	OTG-INFO-007	1
Review Webpage Comments and Metadata for Information Leakage	OTG-INFO-005	1
Conduct Search Engine Discovery and Reconnaissance for Information Leakage	OTG-INFO-001	1
Test User Registration Process	OTG-IDENT-002	1
Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection	OTG-CRYPST-001	1
Test HTTP Strict Transport Security	OTG-CONFIG-007	1
Test HTTP Methods	OTG-CONFIG-006	1
Testing for Clickjacking	OTG-CLIENT-009	1
Test Cross Origin Resource Sharing	OTG-CLIENT-007	1
Test Upload of Unexpected File Types	OTG-BUSLOGIC-008	1
Testing for the Circumvention of Work Flows	OTG-BUSLOGIC-006	1
Testing for Insecure Direct Object References	OTG-AUTHZ-004	1
Testing for Weak password policy	OTG-AUTHN-007	1
Test remember password functionality	OTG-AUTHN-005	1
Testing for Weak lock out mechanism	OTG-AUTHN-003	1
Testing for default credentials	OTG-AUTHN-002	1
Testing for Credentials Transported over an Encrypted Channel	OTG-AUTHN-001	1
Genel Toplam		**36**

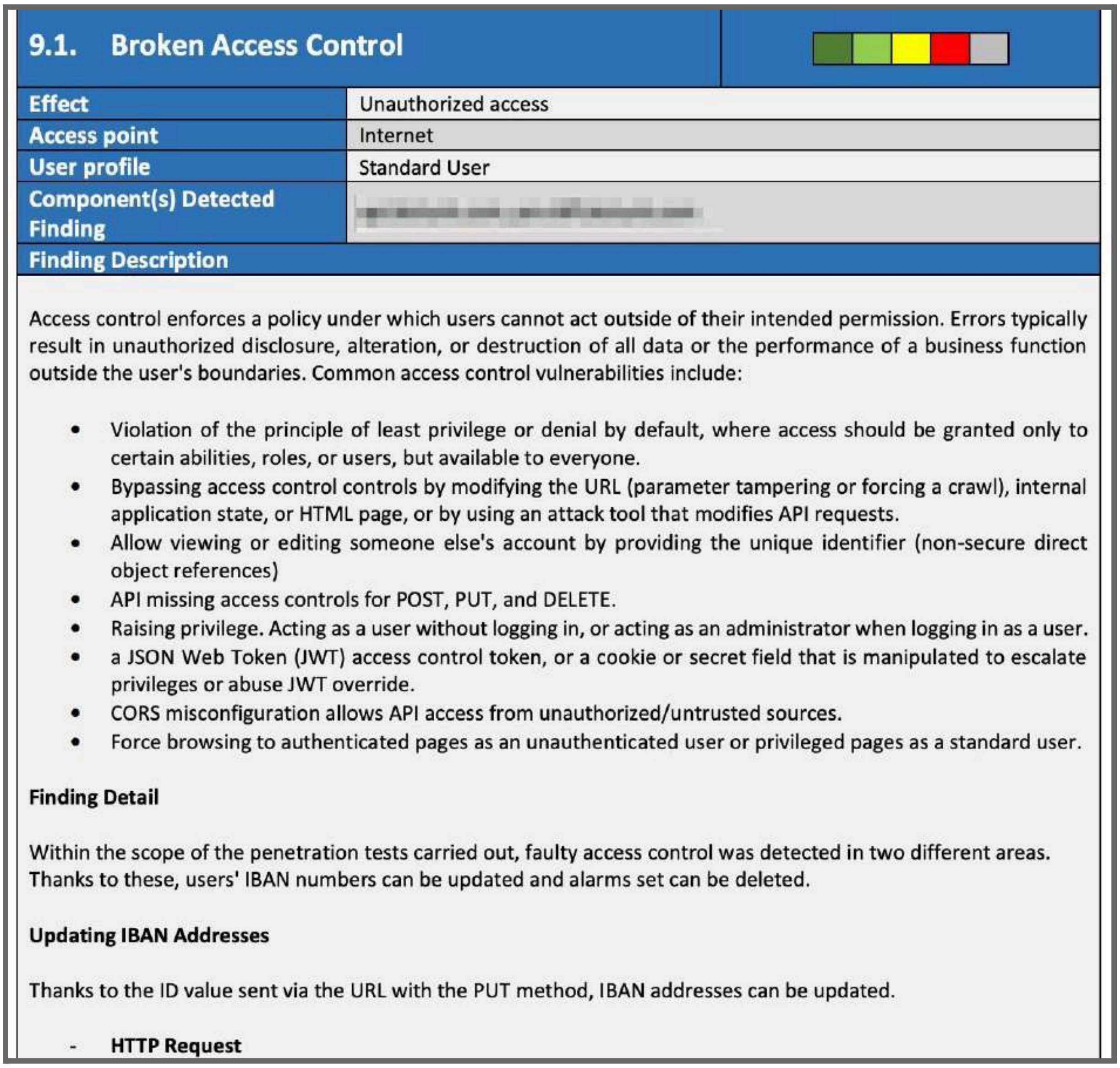
Summary table of vulnerabilities found



Kategori / Risk Seviyesi Özet Dağılım Tablosu

Vulnerability Name	Critical	High	Moderate	Low	Genel Toplam
Authentication Testing			1	1	2
Authorization Testing		1	3		4
Business logic Testing	1	5	5		11
Client Side Testing		1	3		4
Configuration and Deploy Management Testing				2	2
Cryptography		1			1
Data Validation Testing			1		1
Identity Management Testing			1		1
Information Gathering			2	6	8
Information Leakage			1		1
Session Management Testing			1		1
Genel Toplam	**1**	**8**	**18**	**9**	**36**

Risk levels of the vulnerabilities found



9.1. Broken Access Control	🟩🟩🟨🟥⬜
Effect	Unauthorized access
Access point	Internet
User profile	Standard User
Component(s) Detected Finding	[redacted]

Finding Description

Access control enforces a policy under which users cannot act outside of their intended permission. Errors typically result in unauthorized disclosure, alteration, or destruction of all data or the performance of a business function outside the user's boundaries. Common access control vulnerabilities include:

- Violation of the principle of least privilege or denial by default, where access should be granted only to certain abilities, roles, or users, but available to everyone.
- Bypassing access control controls by modifying the URL (parameter tampering or forcing a crawl), internal application state, or HTML page, or by using an attack tool that modifies API requests.
- Allow viewing or editing someone else's account by providing the unique identifier (non-secure direct object references)
- API missing access controls for POST, PUT, and DELETE.
- Raising privilege. Acting as a user without logging in, or acting as an administrator when logging in as a user.
- a JSON Web Token (JWT) access control token, or a cookie or secret field that is manipulated to escalate privileges or abuse JWT override.
- CORS misconfiguration allows API access from unauthorized/untrusted sources.
- Force browsing to authenticated pages as an unauthenticated user or privileged pages as a standard user.

Finding Detail

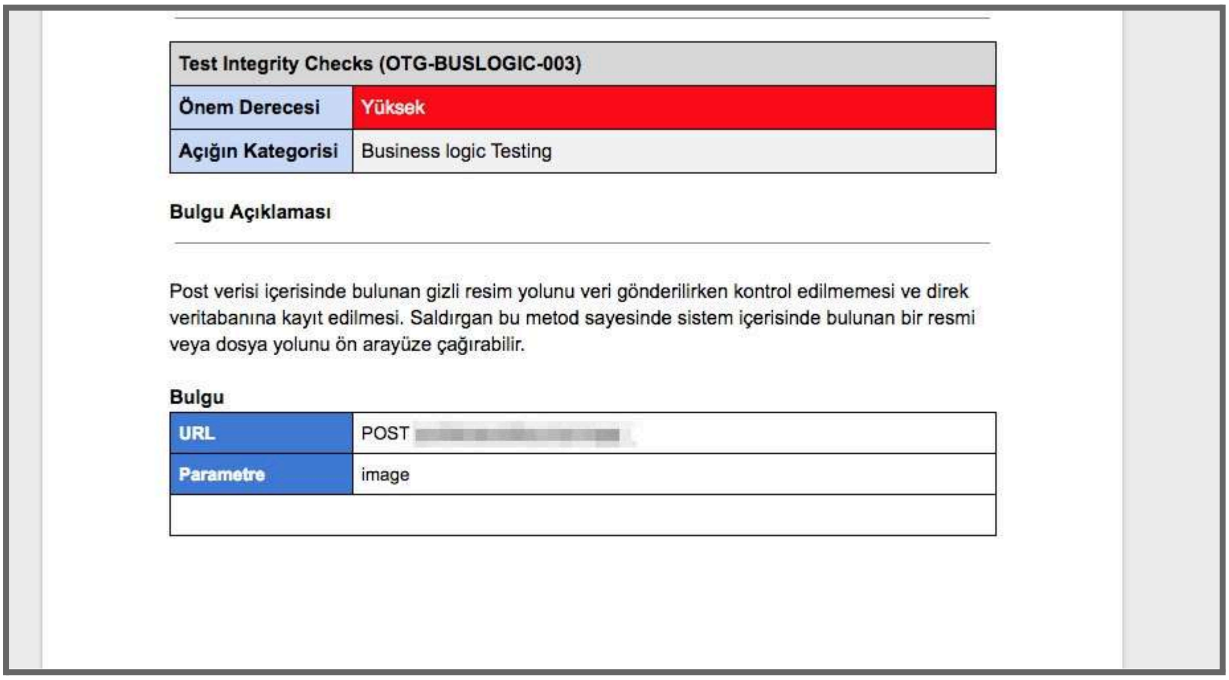
Within the scope of the penetration tests carried out, faulty access control was detected in two different areas. Thanks to these, users' IBAN numbers can be updated and alarms set can be deleted.

Updating IBAN Addresses

Thanks to the ID value sent via the URL with the PUT method, IBAN addresses can be updated.

- **HTTP Request**

Detected vulnerabilities, screenshots and solution suggestions



Test Integrity Checks (OTG-BUSLOGIC-003)	
Önem Derecesi	Yüksek
Açığın Kategorisi	Business logic Testing

Bulgu Açıklaması

Post verisi içerisinde bulunan gizli resim yolunu veri gönderilirken kontrol edilmemesi ve direk veritabanına kayıt edilmesi. Saldırgan bu metod sayesinde sistem içerisinde bulunan bir resmi veya dosya yolunu ön arayüze çağırabilir.

Bulgu

URL	POST [redacted]
Parametre	image

Finding example and explanation

SWORDSEC

ANKARA	TALLINN
Teknopark Ankara E Blok 210 Yenimahalle, Ankara, Turkiye	Veskiposti t. 10138 Tallinn, Estonia
Tel: +90 (850) 532 77 69	**E-mail:** info@swordsec.com
E-mail: info@swordsec.com	**Web:** www.swordeye.io
Web: www.swordsec.com	

www.swordsec.com