This project is co-financed by the European Union
and the Republic of Turkiye

Technical Assistance for "A Smart Network for Technology Transfer and Commercialisation with Funnel Model (SMARTNET)"

Contract No: TR14C2.2.05-04/001

EUROPEAID/140284/IH/SER/TR

PENETRATION TEST PLAN (PENTEST-P) AND PENETRATION TEST RESULTS (PENTEST-R)

22.05.2023

Technical Assistance for “A Smart Network for Technology Transfer and Commercialisation with Funnel Model (SMARTNET)”

Contract No: TR14C2.2.05-04/001

EUROPEAID/140284/IH/SER/TR

PENETRATION TEST PLAN (PENTEST-P)

AND PENETRATION TEST RESULTS (PENTEST-R)

22.05.2023

Document Control and Approval Sheet

Project Name	Technical Assistance for “A Smart Network for Technology Transfer and Commercialisation with Funnel Model (SMARTNET)”
Contract Number	TR14C2.2.05-04/001
Reference Number	EUROPEAID/140284/IH/SER/TR
End Recipient of Assistance	Yıldız Technical University
Contract Signed	08.03.2022
Commencement Date	25.05.2022
Duration	36 Months
Prepared By	Technical Assistance Team
Date of Document	22.05.2023
Contractor	SwanLeuco Danışmanlık AŞ Kiliçdede Mah. Kastamonu Sok. No:6 11/54 55060 İlkadım Samsun 0362 503 55 64 okan.gumus@swanleuco.com

Revision Information

Date	Revision	Notes and Changes
22.05.2023	1.0	Initial Revision

DISCLAIMER

This document has been produced with the technical assistance of the European Union under Technical Assistance for “A Smart Network for Technology Transfer and Commercialisation with Funnel Model (SMARTNET)” Project, Türkiye. Service Contract Number: “EUROPEAID/140284/IH/SER/TR”.

The contents of this publication are the sole responsibility of SwanLeuco in consortium with Evoluxer, Asturex, RRDA, StartUp Division, Inycon and can in no way taken as the view of the European Union and the Ministry of Industry and Technology of the Republic of Türkiye.

TABLE OF CONTENTS

LIST of ABBREVIATIONS

API	Application Programming Interface
CA	Contracting Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CISOP	Competitiveness and Innovation Sector Operational Programme
CORS	Cross-Origin Resource Sharing
ERA	End Recipient of Assistance (Beneficiary)
EUD	Delegation of the European Union to Türkiye
GTU	Gebze Technical University
HKU	Hasan Kalyoncu University
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
ICT	Information and Communication Technologies
ISECOM	Institute for Security and Open Methodologies
IT	Information Technologies
ITU	Istanbul Technical University
KE	Key Expert
MIS	Management Information System
MoIT/DoEUFP	Ministry of Industry and Technology Directorate of EU Financial Programmes
OCU	Operation Coordination Unit
OS	Operating Structure
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PENTEST	Penetration Testing
PCI DSS	Payment Card Industry Data Security Standard
RCOP	Regional Competitiveness Operational Programme
SQL	Server Query Language
SSL	Secure Sockets Layer
TAT	Technical Assistance Team
TLS	Transport Layer Security
ToR	Terms of Reference
TTI	Technology Transfer Intermediary
TTO	Technology Transfer Office
URL	Uniform Resource Locator
YTU	Yıldız Technical University

1. INTRODUCTION

Under Component I of the **A Smart Network for Technology Transfer and Commercialisation with Funnel Model (SMARTNET)** project, one of the primary activities is **Activity 1. Establishment of TTI Network and Development of Institutional Infrastructure** which aims to establish and operationalize **SMARTNET** by delivering training, mentoring/consulting and fundraising services to the target groups for supporting them to commercialize their technology-oriented business ideas.

Activity A.1.1. Development of TTI Network Software Platform focuses on the design, development, and operationalisation of the **SMARTNET Artificial Intelligence Based TTI Network Software Platform (SMARTNET Platform)**.

The **Smartnet MIS Platform**; is a web-based Management Information System (MIS) which will act as commercialisation automation software and a management decision support system that would coordinate the transfer of technology and commercialisation activities and provide mutual information flow in the network constituted by stakeholder TTIs, with the following identified list of developed modules:

- Module 1 - Entrepreneurs management
- Module 2 - Mentors management
- Module 3 - Investors management
- Module 4 - Intellectual Property (IP) management
- Module 5 - Integration web services
- Module 6 - Artificial intelligence and decision support
- Module 7 - Standard and custom reporting
- Module 8 - System management and administration

as well as two auxillary modules:

- Module 9 - Web Portal (Content Management System)
- Module 10 - e-Learning Platform (ME-Learning)

The purpose of this **Penetration Test Plan (PENTEST-P)** and it’s Results Report **(PENTEST-R)** is to present the planning and the findings and recommendations resulting from the penetration testing performed on the Smartnet MIS Platform, developed by the Technical Assistance Team (TAT). The penetration testing is aimed to simulate real-world attack scenarios and assess the platform's resilience against unauthorized access, data breaches, and other security threats.

The penetration testing was conducted by the independent security contractor, **Çetinkale Informatics**, during the week of 8th to 12th of May 2023. The purpose of this assessment was to evaluate the security posture of the Smartnet MIS Platform and identify potential vulnerabilities that could be exploited by malicious actors.

The results of the tests conducted was presented on 15th of May and recommended remedies was immediately introduced by the Software Development team on the 15th and 16th of May. A retest on identified issues was performed on 17th of May and final report was received on the 18th of May 2023.

2. TEST PLAN FOR PENETRATION TESTING

Test Plan for Penetration Testing on Smartnet MIS Platform:

Objective:

The objective of the penetration testing is to assess the security resilience of the Smartnet MIS Platform and identify potential vulnerabilities and weaknesses that could be exploited by unauthorized individuals. The testing will simulate real-world attack scenarios to evaluate the platform's ability to protect against unauthorized access, data breaches, and other security threats.

Scope:

The penetration testing will focus on the Smartnet MIS Platform hosted on servers provided by YTU. The assessment will cover both external and internal components of the platform, including the web application, server infrastructure, network architecture, and associated databases. The testing will primarily target areas such as authentication mechanisms, authorization controls, input validation, session management, data protection, and secure communication.

Methodology:

The penetration testing will follow a systematic and comprehensive approach, employing a combination of automated tools and manual techniques.

The testing will include but not be limited to the following activities:

a) Information gathering and reconnaissance to identify potential attack vectors.
b) Vulnerability scanning to discover known security weaknesses.
c) Manual testing to identify complex vulnerabilities that cannot be detected by automated tools.
d) Exploitation attempts to validate identified vulnerabilities and assess their potential impact.
e) Privilege escalation to evaluate the platform's access control mechanisms.
f) Data validation and integrity testing to ensure the protection of sensitive information.
g) Reporting of identified vulnerabilities along with their severity and recommended remediation steps.

Test Schedule:

The penetration testing will be indicatively conducted during the week of 8th to 12th of May 2023, with specific activities and timelines as follows:

- **Information gathering and reconnaissance**: 8th to 9th of May 2023.
- **Vulnerability scanning and automated testing**: 9th to 10th of May 2023.
- **Manual testing and exploitation**: 10th to 11th of May 2023.
- **Privilege escalation and data validation**: 11th to 12th of May 2023.
- **Indicative re-testing of identified issues and vulnerabilities (if any)**: 17th of May 2023.

Reporting and Remediation:

A preliminary report of identified vulnerabilities and their severity will be presented on 15th of May. The software development team will work on remediation steps immediately on the 15th and 16th of May. A re-test will be performed on any identified issues on 17th of May. The final penetration testing report will be presented in at most two working days following the re-testing, which will include a detailed summary of findings, recommended remediation measures, and an overall assessment of the platform's security posture.

Communication and Confidentiality:

All communication related to the penetration testing of the Smartnet MIS Platform, including findings, remediation steps, and the final report, will be handled with utmost confidentiality and shared only with authorized personnel from the contracting party involved in the security assessment and remediation process. Appropriate measures will be taken to ensure the secure transmission and storage of sensitive information.

3. PENETRATION TEST RESULTS

The following penetration test results report is presented **as-is** without providing any changes to the content, some sections of the report containing tables or screenshots with sensitive internal information were redacted for this report at the recommendation of the security firm conducting the tests. These sections are marked as [**REDACTED**].

Style formatting was applied to the report to match the Smartnet Project Reporting Template as well as heading styles were adjusted to comply with the table of contents.

SMARTNET Penetration Testing Report

(v1.5 - FINAL VERSION)

Prepared by: **CETINKALE INFORMATICS**

Reviewed by: **Koray Burak ÇETİNKALE**

Date: **18.5.2023**

Limitations on Disclosure and Use of this Document

This report was prepared by CETINKALE INFORMATICS for the exclusive benefit of SWANLEUCO DANIŞMANLIK A.Ş. and is proprietary information. Unauthorized use or reproduction of this document is prohibited. The Non-Disclosure Agreement (NDA) in effect between CETINKALE INFORMATICS and SWANLEUCO DANIŞMANLIK A.Ş. governs the disclosure of this report to all other parties, including product vendors or suppliers.

This report contains information about potential vulnerabilities of the SMARTNET WEB APPLICATION and methods for exploiting them. CETINKALE INFORMATICS recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein. CETINKALE INFORMATICS has retained and secured a copy of the report for customer reference. All copies of the report have been delivered electronically to:

Mr Okan GÜMÜŞ
okan.gumus@swanleuco.com
+90 (362) 503 55 64

SwanLeuco Danışmanlık A.Ş.
Kılıçdede Mah. Kastamonu Sok. No:6 11/54
İlkadım, 55060, Samsun
TÜRKİYE

By providing this report to SWANLEUCO DANIŞMANLIK A.Ş., CETINKALE INFORMATICS does not constitute any form of representation, warranty, or guarantee that the systems are 100% secure from every form of attack. While CETINKALE INFORMATICS methodology includes both automated and manual testing to identify and attempt exploitation of the most common security issues, testing was limited to an agreed upon time frame.

Document Details

Project Name	Smartnet Web Application (Grey box) Penetration Testing Report
Project Resources	Koray Burak ÇETİNKALE (KBC)
Project Duration	8-18.5.2023

Document History

Version	Date	Author	Comments
1.0	12.5.2023	KBC	Initial Version
1.1	13.5.2023	NC	Internal Peer Review
1.2	13.5.2023	KBC	Review and Corrections
1.3	15.5.2023	KBC	Preliminary Version
1.4	17.5.2023	KBC	Re-test findings to validate issue remediations by the Development Team
1.5	18.5.2023	KBC	Final Version

3.1 Executive Summary

SWANLEUCO DANIŞMANLIK A.Ş. engaged CETINKALE INFORMATICS to perform a penetration testing of the SMARTNET web application. The primary goal of this web application (Grey box) penetration testing project was to identify any potential areas of concern associated with the application in its current state and determine the extent to which the system may be breached by an attacker possessing a particular skill and motivation. The assessment was performed in accordance with the "best-in-class" practices as defined by ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP) and Penetration Test Guidance for PCI DSS Standard.

CETINKALE INFORMATICS conducted the penetration testing during the period of 9.5.2023 and 12.5.2023. All testing activities were performed on the SMARTNET Web Application production environment provided by the customer having made a complete backup of the system. While performing the testing activities, CETINKALE INFORMATICS emulated an external attacker without prior knowledge of the environment. To test the user-authenticated area and privilege escalation vulnerabilities, the customer supplied CETINKALE INFORMATICS credentials for several registered user and admin accounts.

The scope of the assessment included the following sites:

https://smartnet.global

Notes:

- It should be noted, that the Dashboard - Panel "System Parameters" functionality offered by the Consumer Facing Web App was not available during the penetration test and was excluded from the scope of the current assessment.
- The SMARNET web application environment provided by for the application penetration testing utilized partner stub & sandbox integrated environments only.

During the course of this assessment, CETINKALE INFORMATICS did not identify any critical vulnerabilities that could lead to full compromise of the system. However, CETINKALE INFORMATICS did find several medium and low severity issues, which should be addressed.

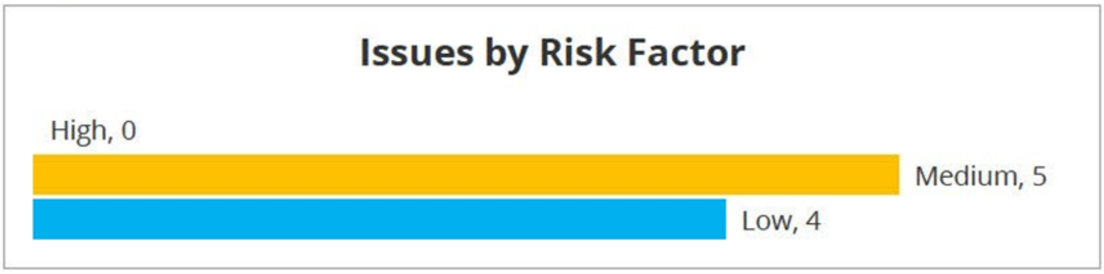
Further detailed information can be found in the "Issues Remediation" section of this report.

CETINKALE INFORMATICS strongly recommends to remediate all medium severity issues detected to mitigate against the possible risk of a sensitive data compromise. The remediation of the low severity findings is not so urgent due to the low probability of their successful exploitation. Nonetheless, it should be noted that the existence of these known issues could decrease the overall security posture of the system.

As of 18.5.2023, the SMARTNET development team has fixed all of the discovered medium vulnerabilities.

This report summarizes what CETINKALE Informatics believes are the most important issues to address in the application.

The chart below outlines a number of issues identified that are grouped by risk factors. Note the risk ratings were given to help assist in prioritizing remediation efforts. True risk can only be calculated by an in-depth understanding of business processes and data, as well as the likelihood of exploitation.



The table below summarizes the findings for OWASP Top 10 list for web application vulnerabilities. OWASP Top 10 represents the list of the most critical web application security flaws, which are accompanied by OWASP security experts from around the world. The list provides a powerful awareness document for web application security and is utilized within many security standards:

Category	**Discovered**
Injection	NO
Broken Authentication	**YES**
Sensitive Data Exposure	NO
XML External Entities (XEE)	NO
Broken Access Control	NO
Security Misconfiguration	**YES**
Cross Site Scripting (XSS)	NO
Insecure Deserialization	NO
Using Components with Known Vulnerabilities	NO
Insufficient Logging & Monitoring	NO

CETINKALE INFORMATICS can re-verify the remediated issues found during this penetration test within 5 working days of this report delivery (until 22.5.2023). CETINKALE INFORMATICS can also arrange to include into this re-scan missing functionality (“System Parameters”) that was not available at the time of this current assessment.

3.2 Issues Remediation

CETINKALE INFORMATICS re-verified all previously found issues on 15.5.2023. The tested application was accessible by the same URLs used during the initial testing.

As of 17.5.2023, the following issues were successfully remediated:

- M1. Enumeration of registered emails
- M3. Sensitive cookies without the “Secure” flag
- M4. The password reset link is reusable
- M5. The application is vulnerable to brute-force attacks
- L2. Cross-domain policy misconfiguration

A subsequent re-test was performed on 18.5.2023. As of 18.5.2023 the following issue was successfully remediated:

- M2. Persistent cookie with sensitive information

The other issues (L1, L3, L4) are still actual.

3.3 Assessment Methodology

CETINKALE INFORMATICS based the findings and recommendations, outlined in this report, on application vulnerability scans and manual penetration testing performed against the application.

3.4 Automated Application Scan

CETINKALE INFORMATICS used several commercial tools to survey the targeted environment and identify potential vulnerabilities. The automated scanning software identifies application-level vulnerabilities. The scope of testing includes but not limited by the following:

- Parameter Injection
- SQL Injection
- Cross-Site Scripting
- Directory Traversal
- Parameter Overflow
- Buffer Overflow
- Parameter Addition
- Path Manipulation
- Character Encoding
- Site Search
- SSL Strength
- Sensitive Developer Comments
- Web Server/Web Package Identification
- Permissions Assessment
- Brute Force Authentication attacks

3.5 Manual Application Testing

Using the information produced by the automated testing software, CETINKALE INFORMATICS also employed manual testing techniques to identify and attempt exploiting additional vulnerabilities in the targeted application, and to eliminate false positives produced by the automated scanning process. The assessment was conducted in accordance with the best-in-class practices as defined by such methodologies as ISECOM's Open Source Security Testing Methodology Manual (OSSTMM) and the Open Web Application Security Project (OWASP).

CETINKALE Informatics performed the following actions as part of this testing:

- Gathered information about the application
- Mapped application content and analyzed it

- Observed types and placement of security controls
- Reviewed web page HTML source code for possible vulnerabilities
- Tested application authentication, session management and access controls
- Tested application for client data validation issues
- Tested application for input-based vulnerabilities
- Tested application for business logic flaws
- Checked for application server vulnerabilities

The test focused on possible vulnerabilities in the application logic, looking for issues including but not limited to:

- SQL and command injection
- Authentication and authorization implementation defects
- Access control issues and privilege elevation
- Session management/hijacking
- File input/output implementation defects
- Parameter overflow and handling
- HTTP/URL manipulation
- Application logic defect
- Improper web server configuration Concurrency issues
- Information leakage
- SSL and transport layer weaknesses
- Application-level denial-of-service

4. Criteria for Risk Ratings

The table below outlines the general rules for assigning risk ratings to identified vulnerabilities:

RISK RATING	DESCRIPTION
HIGH	These issues identify conditions that could directly result in the compromise or unauthorized access of a network, system, application or sensitive information. Examples of High-Risk issues include remote execution of commands, known buffer overflows; unauthorized access and disclosure of sensitive information.
MEDIUM	These issues identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application of information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, application or information. Examples of Medium Risk issues include directory browsing, partial access to files on the system; disclosure of security mechanisms and unauthorized use of services.
LOW	These issues identify conditions that do not immediately or directly result in compromise of a network, system, application or information, but do provide information that could be used in combination with other information to gain

	insight into how to compromise or gain unauthorized access to a network, system, application or information.
REMEDIATED	The issue has been fixed since the previous round of penetration testing.

5. Assessment Findings

Summary

The table below outlines summary of findings identified during the penetration testing:

Finding Description	**Status**
Medium Risk Findings	**REMEDIATED**
M1. Enumeration of registered emails	REMEDIATED
M2. Persistent cookie with sensitive information	REMEDIATED
M3. Sensitive cookies without the "Secure" flag	REMEDIATED
M4. The password reset link is reusable	REMEDIATED
M5. The application is vulnerable to brute-force attacks	REMEDIATED
Low Risk Findings	
L1. Strict-Transport-Security header is not used	LOW
L2. Cross-domain policy misconfiguration	REMEDIATED
L3. Auto-complete feature is not disabled for password fields	LOW
L4. The application server supports TLS cipher suites without forward security	LOW

6. High Risk Findings

No **high**-severity issues were found in the application.

7. Medium Risk Findings

Five **medium**-severity issues were found in the application, as described below.

7.1 M1. Enumeration of registered emails

Risk Rating: **REMEDIATED**

Remediation Efforts: **MEDIUM**

Summary

CETINKALE INFORMATICS identified that the application notified the user about the existence of the entered email address. Such behavior provides the ability to a potential malefactor to enumerate all emails registered within the system. The collected information could be used for further attacks (for instance for spreading phishing emails or other social engineering attacks).

Affected Functionality

The following request required a user email as an input:

[REDACTED]

Proof of Concept

The image below shows the server response for the signup functionality in the case where the entered email exists in the system:

[REDACTED]

Recommendations

In order to avoid automated enumeration of valid e-mails, CETINKALE Informatics suggests using one of the following techniques:

1) Do not show an error message providing information about the existence or non-existence of the entered email. In both cases, the application should return a generic message that the required information has been sent to the entered email address.
2) Add a CAPTCHA challenge after the series of failed attempts to prevent automated email enumeration.

Remediation

As of 17.5.2023, the issue was successfully **remediated**. Currently, a unique random invite code delivered by the application administrator is required for the account creation process:

[REDACTED]

7.2 M2. Persistent cookie with sensitive information

Risk Rating: **REMEDIATED**

Remediation Efforts: **LOW**

Summary

CETINKALE Informatics identified that the SMARTNET application used persistent cookies for session tracking in the Administration Portal. The cookies were stored to the hard disk and survived a browser restart. As the cookie contained authentication information, this can allow a local attacker to access the application without knowledge of the password.

Moreover, it was noticed that the user's session cookies lifetime was two weeks, this is quite a big time range to allow for potential malicious activities.

Affected Functionality

The following session token of web site Administration portal was persistent:

[REDACTED]

Proof of Concept

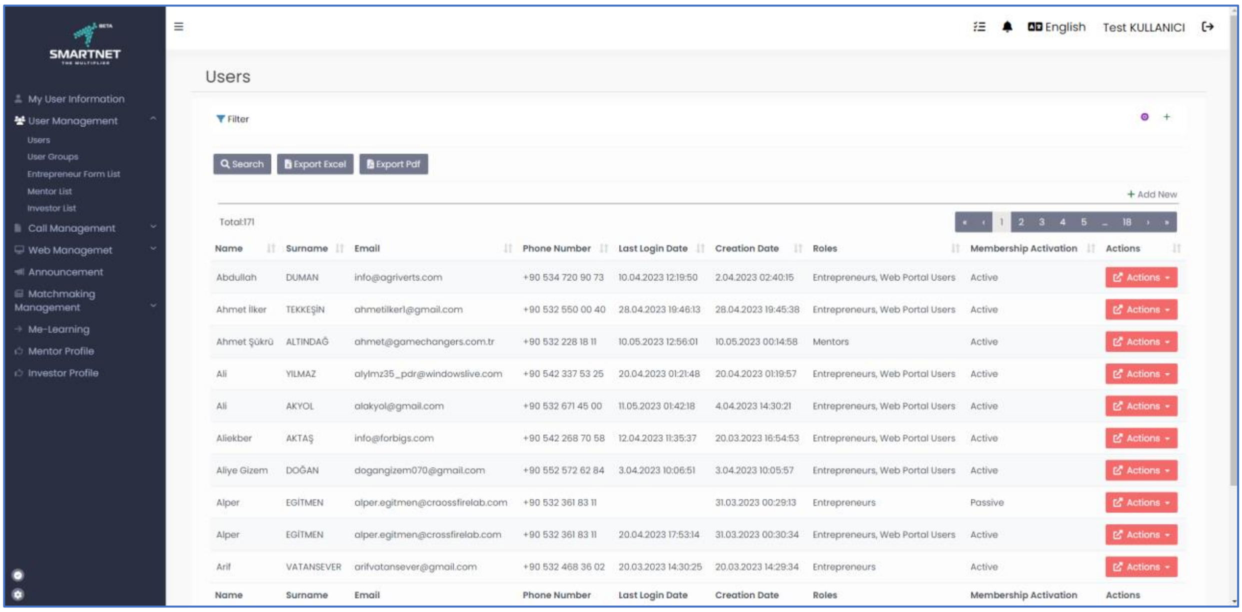
Log in to the application as an administrator user and inspect server responses in a web proxy. The method "GET /Manage/User/UsersList /" sets a cookie named "sessionid" that is used by the SMARTNET Web application:

[REDACTED]

Please note that the cookie contains an expiration date that makes it persistent.

Close the browser, restart and open URL **https://smartnet.global/Manage/User/ListUsers**.

Notice that the user is still authorized in the application:



Total:171

Name	Surname	Email	Phone Number	Last Login Date	Creation Date	Roles	Membership Activation	Actions
Abdullah	DUMAN	info@agriverts.com	+90 534 720 90 73	10.04.2023 12:19:50	2.04.2023 02:40:15	Entrepreneurs, Web Portal Users	Active	Actions
Ahmet İlker	TEKKEŞİN	ahmetilkerl@gmail.com	+90 532 550 00 40	28.04.2023 19:46:13	28.04.2023 19:45:38	Entrepreneurs, Web Portal Users	Active	Actions
Ahmet Şükrü	ALTINDAĞ	ahmet@gamechangers.com.tr	+90 532 228 18 11	10.05.2023 12:56:01	10.05.2023 00:14:58	Mentors	Active	Actions
Ali	YILMAZ	alylmz35_pdr@windowslive.com	+90 542 337 53 25	20.04.2023 01:21:48	20.04.2023 01:19:57	Entrepreneurs, Web Portal Users	Active	Actions
Ali	AKYOL	alakyol@gmail.com	+90 532 671 45 00	11.05.2023 01:42:18	4.04.2023 14:30:21	Entrepreneurs, Web Portal Users	Active	Actions
Aliekber	AKTAŞ	info@forbigs.com	+90 542 268 70 58	12.04.2023 11:35:37	20.03.2023 16:54:53	Entrepreneurs, Web Portal Users	Active	Actions
Aliye Gizem	DOĞAN	dogangizem070@gmail.com	+90 552 572 62 84	3.04.2023 10:06:51	3.04.2023 10:05:57	Entrepreneurs, Web Portal Users	Active	Actions
Alper	EGİTMEN	alper.egitmen@craossfirelab.com	+90 532 361 83 11		31.03.2023 00:29:13	Entrepreneurs	Passive	Actions
Alper	EGİTMEN	alper.egitmen@crossfirelab.com	+90 532 361 83 11	20.04.2023 17:53:14	31.03.2023 00:30:34	Entrepreneurs, Web Portal Users	Active	Actions
Arif	VATANSEVER	arifvatansever@gmail.com	+90 532 468 36 02	20.03.2023 14:30:25	20.03.2023 14:29:34	Entrepreneurs	Active	Actions
Name	Surname	Email	Phone Number	Last Login Date	Creation Date	Roles	Membership Activation	Actions

Recommendations

CETINKALE Informatics recommends to avoid using persistent cookies for storing authorization tokens or other sensitive information. Session cookies should be used instead, which are never saved to disk and are automatically cleared when a user closes the browser.

Remediation

As of 18.5.2023, the issue was successfully **remediated**. The web site admin application uses session cookies with sensitive information:

[REDACTED]

7.3 M3. Sensitive cookies without the "Secure" flag

Risk Rating: **REMEDIATED**

Remediation Efforts: **LOW**

Summary

CETINKALE Informatics has determined that the SMARTNET Web Application issued an authentication cookie without the "Secure" flag. The purpose of the "Secure" flag is to prevent cookies from being observed by unauthorized parties due to the transmission of the cookie in cleartext. To accomplish this goal, browsers that support the secure flag will only send cookies with the Secure flag when the request is going to an HTTPS page.

Affected Functionality

The following cookie was not marked by the “Secure” flag:

[REDACTED]

Proof of Concept

The following screenshot demonstrates the authentication cookie without the “Secure” flag:

[REDACTED]

Launch the Wireshark Network Analyzer and start capturing the traffic to and from TCP port 80 and 443. In the browser open the following URL **https://smartnet.global/Manage/Notification** with the insecure and secure schema and inspect the captured traffic in Wireshark we find unencrypted cookies. That demonstrates that the cookie can be intercepted sniffing the network.

[REDACTED]

Recommendations

It’s recommended to set on the “Secure” flag for any authentication and session cookies. Using such an approach, the browser will not send a cookie with the secure flag set over an unencrypted HTTP request.

Remediation

As of 17.5.2023, the issue was successfully **remediated**. CETINKALE Informatics confirms that the “Secure” flag was set for the session cookie:

[REDACTED]

7.4 M4. The password reset link is reusable

Risk Rating: **REMEDIATED**

Remediation Efforts: **MEDIUM**

Summary

CETINKALE Informatics found that a password reset link could be used multiple times. If a user’s email account is compromised, the token used to reset the password would be valid even if the user already reset their password.

Affected Functionality

The issue affected the forgot password functionality.

Proof of Concept

The screenshots below demonstrate that a reset password link can be used several times:

[REDACTED]

Recommendations

The reset password link should be single-used. Once a user's password has been reset, the randomly-generated token should no longer be valid.

Remediation

As of 17.5.2023 , the issue was successfully **remediated**. It is not possible to use a reset password link several times:

[REDACTED]

7.5 M5. The application is vulnerable to brute-force attacks

Risk Rating: **REMEDIATED**

Remediation Efforts: **MEDIUM**

Summary

While testing authentication functionality, CETINKALE Informatics observed that the SMARTNET Web Application did not utilize any account lockout policy upon failed login attempts. CETINKALE Informatics performed more than 20 failed login attempts for one of the test accounts without receiving any lock messages. As far as CETINKALE Informatics could determine, no account lockout mechanism was in place.

The absence of an account lockout ability could give an attacker an infinite number of attempts to enter guesses of the current password to achieve a valid variant (known as "brute-force" attack). There are many scripts and tools that automate this type of attack available on the Internet that can be used against a web- based application.

Affected Functionality

The issue affected the login functionality of the web site Administration portal:

[REDACTED]

Proof of Concept

1. A user successfully logins to the application:

[REDACTED]

2. Logout the user and then try to login with the same login but wrong password multiple times:

[REDACTED]

3. After that, the user can still successfully log in to the application:

[REDACTED]

Recommendations

CETINKALE INFORMATICS recommends employing a password lockout mechanism that temporarily locks an account if more than a preset number of unsuccessful login attempts are made. This approach significantly slows down attackers, while allowing the accounts to be open for legitimate users.

The most secure approach for the implementation of an account locking function assumes notifying the blocked user about the blocking only via a third-party channel (for instance via email or mobile phone). In this way, the malicious user trying to guess the valid password will not be able to know that the account is locked and all his further attempts will be unsuccessful.

Another approach is utilizing CAPTCHA services, which should force the user to input additional information provided in a human only understandable format.

Remediation

As of 17.5.2023, the issue was successfully remediated. A user account was blocked after 5 incorrect login attempts to the application:

[REDACTED]

Also, in the administrative panels as well:

[REDACTED]

8. Low Risk Findings

Four **low**-severity issues were found in the application, as described below.

8.1 L1. Strict-Transport-Security header is not used

Risk Rating: **LOW**

Remediation Efforts: **LOW**

Summary

CETINKALE INFORMATICS noticed that all applications did not utilize the "Strict-Transport-Security" header for encrypted communication. The aforementioned header forces browsers to use only an encrypted channel for communication with the server even in case the potential malefactor tries to downgrade the communication to an unsafe HTTP connection.

Without a Strict Transport Security policy, the application may be vulnerable against several attacks:

If the web application mixes the usage of HTTP and HTTPS, an attacker can manipulate pages in the unsecured area of the application or change redirection targets in a manner that the switch to the secured page is not performed or done in a manner, that the attacker remains between client and server.

If there is no HTTP server, an attacker in the same network could simulate a HTTP server and trick the user to click on a prepared URL by using a social engineering attack.

Affected Functionality

The issue affected all responses from the following applications:

https://smartnet.global

Proof of Concept

The example of the server response is shown below:

[REDACTED]

Recommendations

The application should instruct web browsers to only access the application using encrypted HTTPS channel. For that, HTTP Strict Transport Security (HSTS) should be enabled by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS.

To apply the policy to all subdomains, the 'includeSubDomains' flag could be also utilized. As an additional security measure the domain should be submitted to an HSTS preload service.

The detailed information can be found via the following links below:

- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/HTTP Strict Transport Security_Cheat_Sheet.md
- https://hstspreload.org/?domain=smartnet.global

Due to the fact that the affected applications utilize Front as the CDN system for delivering static content, there is no direct way to set the required server header. However, as a workaround solution, it is possible to introduce an intermediate Edge Lambda function which puts the appropriate headers onto CloudFront HTTP responses before they're sent to the clients, see reference links below. (Note: however, such a configuration introduces an extra point of failure and could affect performance and availability of the site):

- https://medium.com/@netscylla/adding-security-headers-to-s3-websites-2002f243aa8f
- https://johnlouros.com/blog/setup-security-headers-s3-host-website
- https://adamj.eu/tech/2019/04/15/scoring-a+-for-security-headers-on-my-cloudfront-hosted-staticwebsite/

As a possible way of remediation for the web site CMS used by one of the applications (https:// smartnet.global /admin), it is recommended to set appropriate security parameters within web site middleware as it is described in the article below:

- https://docs.djangoproject.com/en/3.0/ref/middleware/#http-strict-transport-security

Remediation

As of 17.5.2023, the issue was **not remediated**. Applications still do not utilize the “Strict-TransportSecurity” header for encrypted communication:

[REDACTED]

8.2 L2. Cross-domain policy misconfiguration

Risk Rating: **REMEDIATED**

Remediation Efforts: **LOW**

Summary

CETINKALE INFORMATICS found that the application servers provided the ability to execute cross-domain requests from any domain to all the server's resources using HTML5 cross- resource sharing (CORS). Trusting arbitrary policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk. If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged-in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access.

Affected Functionality

The issue affected all responses from the following application endpoints:

https://smartnet.global

Proof of Concept

The images below show the examples of the server's responses allowing cross-domain requests from any domain ("Access-Control-Allow-*"):

[REDACTED]

Recommendations

CETINKALE INFORMATICS strongly recommends setting the scope of allowed domains and permissions to be as restrictive as possible. In the case CORS functionality is not used at all, the server must prohibit it. It is recommended to implement appropriate settings at the proxy server level located in front the Windows Server or directly in Microsoft IIS as outlined in the official documentation referenced below:

- https://www.iis.net/downloads/microsoft/iis-cors-module
- https://learn.microsoft.com/en-us/iis/extensions/cors-module/cors-module-configuration-reference

Remediation

As of 17.5.2023, the issue was successfully **remediated**. CETINKALE INFORMATICS confirms, that now the application prohibits cross-domain interaction at all:

[REDACTED]

8.3 L3. Auto-complete feature is not disabled for password fields

Risk Rating: **LOW**

Remediation Efforts: **LOW**

Summary

Modern browsers offer users the ability to manage their multitude of credentials by storing them insecurely on their computers. This client-side feature could potentially compromise a user's account on the application in the event of the compromise of a client's workstation.

It was possible to remediate this issue previously by appending this additional parameter "autocomplete="off" to the opening form tag or an individual form element of the password field to indicate to the browser that it should not offer to store that information. However, nowadays, almost all modern browsers ignore this attribute. The best approach for blocking passwords saving on the browser side is using the "autocomplete='new-password" attribute, however, the attribute is not handled by old versions of some browsers (Firefox below version 38, Google Chrome below 34, and Internet Explorer below version 11). As an alternative way of preventing password autofilling, could be the utilization of a 3rd party client-side library like the "jquery.disableAutoFill" plugin.

Affected Functionality

The issue affected the following functionality:

https://smartnet.global/Login/Login (autocomplete="off')

Proof of Concept

The image below shows an example of enabled autocomplete for the application login forms:

[REDACTED]

Recommendations

The password autocomplete should always be disabled, especially in sensitive applications, since an attacker, if able to access the browser cache, could easily obtain the password in clear-text.

The detailed information about autocomplete implementation in all modern browsers can be found in these articles below:

- https://developer.mozilla.org/en-US/docs/Web/Security/Securing your site/Turning off form autocompletion
- https://developer.mozilla.org/en-US/docs/Web/Security/Securing your site/Turning off form autocompletion#Tools for disabling autocompletion
- https://developer.mozilla.org/en-US/docs/Web/HTML/Attributes/autocomplete#Browsercompatibility

Remediation

As of 18.5.2023, the issue was **not remediated**. The password autocomplete is still enabled for the password fields.

8.4 L3. Auto-complete feature is not disabled for password fields

Risk Rating: **LOW**

Remediation Efforts: **LOW**

Summary

CETINKALE INFORMATICS noticed that the application servers supported TLS cipher modes that used RSA encryption for key exchange. Though the encryption algorithm was considered secure, it did not provide Forward Secrecy (FS). It also could potentially lead to a private key compromise in the presence of such vulnerabilities as Bleichenbacher's Oracle or ROBOT or other yet unknown vulnerabilities.

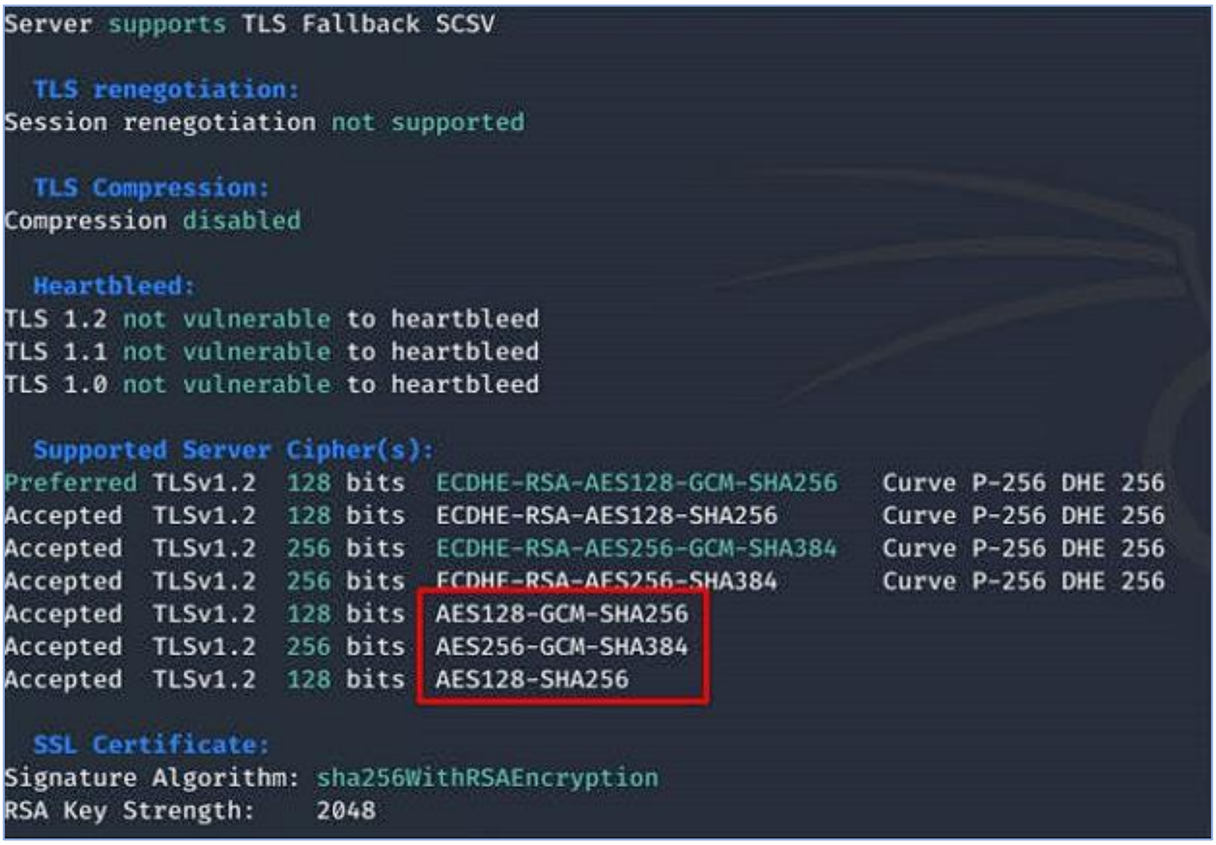
Affected Functionality

The issue affected all cipher suites except the ECDHE ones allowed by the application servers: at smartnet.global (443/TCP);

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256

Proof of Concept

The images below show all cipher suites allowed by the application servers. The weak ones are marked red:



```
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA256

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048
```

Recommendations

It strongly recommended to utilize only cipher suites allowing perfect forward secrecy features. Such an approach should minimize possible security risks connected with decryption of previously sniffed encrypted traffic in case the private key has been compromised.

Detailed information about perfect forward secrecy could be found in the article below:

- https://www.keycdn.com/blog/perfect-forward-secrecy

Since the affected application utilizes Windows Server, the issue could be fixed by applying up-to-date TLS security policies for the corresponding coding resources:

- https://www.hass.de/content/setup-microsoft-windows-or-iis-ssl-perfect-forward-secrecy-and-tls-12

Note that it's necessary to verify that Secure Transfer is enforced for all buckets (including those which serve as storage for CloudFront distributions).

Remediation

As of 18.5.2023, the issue was **not remediated**. The application servers still accept the mentioned cipher suites.

The contents of this publication are the sole responsibility of SwanLeuco in consortium with Evoluxer, Asturex, RRDA, StartUp Division, Inycon and can in no way taken as the view of the European Union and the Ministry of Industry and Technology of the Republic of Türkiye.