A1 Digital

Security-Assessment

Security test of Example - External Infrastructure

Recipient:

Example GmbH
Example Str. 12
1234 Example

Classification: **confidential**
Date: 21.08.2024
Version: **1.0**

Contact at A1 Digital International GmbH:

Alice Codex
ask.security@a1.digital
+431234567890
Department Security

Lassallestraße 9, A-1020 Wien

1 Change record

Date	Version	Author	Description
12.08.2024	0.1	Bob Binary	Initial Creation
16.08.2024	0.8	Alice Codex	First Completion
19.08.2024	0.9	Trent Trustworthy	Review
21.08.2024	1.0	Alice Codex	Published

Table 1: Change record

Contents

2 Management Summary

The results of the security test are summarised briefly below. More detailed descriptions of the individual specific aspects with references to additional resources as well as recommended countermeasures can be found in chapter 5.

2.1 Results

On the dashboard available at `https://dashboard.example.com`, an SQL injection vulnerability was identified that allowed authorized users to read, modify or delete data in the database. Attackers could use this to access user information and passwords. Because the dashboard is connected to the database with a privileged account, the SQL injection can furthermore be leveraged to have command execution on the system.
The application has furthermore been found to have accounts with default credentials. Those allow attackers to easily compromise access controls by testing well known or easily guessable combinations. In combination with the SQL injection this becomes a critical vulnerability, as it allows any attacker to authenticate, and therefore exploit the injection even without their own account.

At the time of the assessment, the `srv02.example.com` system appeared to be using outdated software that had at least the known vulnerability for which there are already publicly available exploits. Attackers could use these exploits to access sensitive data on this system, make the system unavailable, or fully take over the system.

On the target `mail.example.com`, an SMTP server has been identified, on which it was possible to enumerate valid user accounts. Attackers could use the obtained information for follow-up attacks, such as a brute force attack against the discovered users.

In the course of the testing, it was detected that **Remote Desktop Protocol (RDP)** was accessible for the host `srv01.example.com`. RDP has repeatedly been affected by serious security vulnerabilities in the past. Due to the high security risk, RDP should therefore not be directly exposed to the internet.

Some affected systems were configured with weak **SSH settings**. Attackers with access to the network traffic could theoretically break the encryption and thus gain access to sensitive data such as usernames and passwords.

2.2 Recommended next steps

Recommendations for the next 3 months:

- Access to RDP over the internet should be blocked.
- Default accounts should be disabled, or their passwords changed.
- The SQL injection vulnerability should be resolved by using prepared statements in all queries.

Recommendations for the next 6 months:

- It should be ensured that all software in use is up-to-date.
- SMTP commands that allow user enumeration should be disabled.
- SSH and other encrypted protocols should be configured to only support secure and modern cipher, key exchange and MAC algorithms.

Recommendations for the next 12 months:

- An update process should be established for all software in use.
- The newly established security procedures should be tested for effectiveness.

2.3 Overview of weaknesses

The following table provides an overview of the identified weaknesses and an estimate by A1 Digital International GmbH of the effort required to implement countermeasures. Figure 1 shows a schematic representation of the identified weaknesses.

Weakness	Risk (accoring to CVSS3)	Countermeasures
SQL Injection leading to Command Execution	Critical (9.9)	Medium
Default Credential Usage	Critical (9.8)	Easy
Outdated Software with Known Vulnerabilities	High (8.4)	Medium
Open SMTP Server allows User Enumeration	Medium (5.3)	Easy
Remote Desktop Protocol (RDP) Publicly Accessible	Medium (5.3)	Easy
Weak SSH settings	Medium (4.2)	Easy

Table 2: Overview of weaknesses

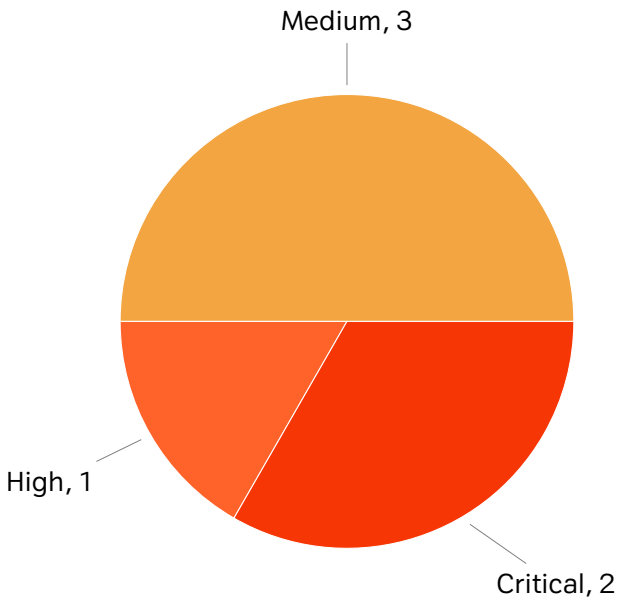


Figure 1: Overview of the identified weaknesses

2.3.1 Weakness categorisation

A coarse categorisation of the identified weaknesses was made to get an overview of the areas in which the most security-relevant findings were identified. The categories of weaknesses are as follows:

- **Configuration Issue**: Errors in the configuration of software or hardware components.
  - If repeated weaknesses have been identified within this category, training for system administrators on how to securely configure the components they support can help.
- **Outdated Software**: Outdated software components with known security-relevant problems.
  - If outdated software is a frequently identified problem, it is recommended to establish a continuous update and patch management process to install security-critical updates in a timely manner.
- **Input Validation/Output Encoding**: Missing validation of user inputs or missing correct encoding of outputs of the software.
  - Frequent errors in this category are likely related to a lack of secure coding training. Regular secure coding training for software developers could increase security and software quality.
- **Other**: Findings that do not fall into one of the three categories above.

The following table identifies the categorisation of weaknesses within the identified findings.

Weakness	Category
SQL Injection leading to Command Execution	Input Validation/Output Encoding
Default Credential Usage	Configuration Issue
Outdated Software with Known Vulnerabilities	Outdated Software
Open SMTP Server allows User Enumeration	Configuration Issue
Remote Desktop Protocol (RDP) Publicly Accessible	Configuration Issue
Weak SSH settings	Configuration Issue

Table 3: Weakness categorisation

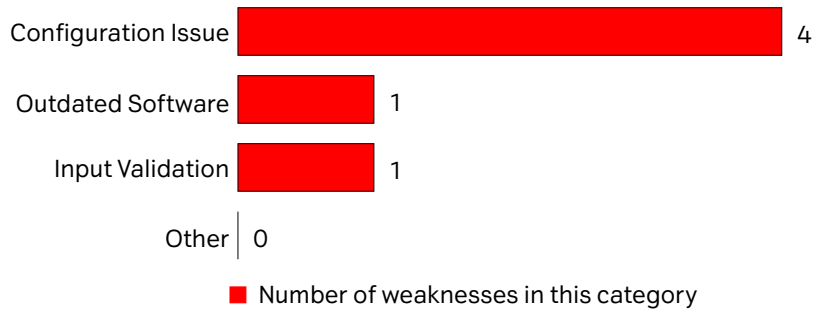


Figure 2: Weakness categorisation

2.4 Disclaimer

The effort for this test was estimated using a time box approach, i.e., only weaknesses within the agreed time window were identified. The aim was to identify and document as many security-relevant weaknesses as possible in the systems being tested. However, we do not assume any liability for completeness of the findings listed in the report.
The test provides a snapshot at the time of the security assessment, so future IT security risks cannot be derived from it.

3 Scope

Example GmbH commissioned A1 Digital International GmbH to perform a security test of the systems listed below.

The security test took place between 12.08.2024 and 16.08.2024.
A more detailed description regarding the procedure can be found in chapter 4.

3.1 Systems tested

The following systems were considered within the assessment.

IP	Hostname
203.0.133.8	nextcloud.example.com
203.0.133.2	srv01.example.com
-	example.com
203.0.133.6	mail.example.com
203.0.133.5	dashboard.example.com
203.0.133.15	relay.example.com

Table 4: Systems tested

3.2 User accounts used

Several test accounts were created on the different exposed services with the e-mail address `pentest@example.com`. It is recommended to block/delete these accounts.

After gaining a remote command execution on the target `dashboard.example.com`, a temporary folder has been created at `/tmp/pentest`. This folder and its content should be deleted permanently.

4 Procedure

To cover the widest possible range of possible weakness categories, the test was conducted following the Open Web Application Security Project (OWASP) Testing Guide Version 4 (see chapter 6.6). The aim was to identify all security-relevant weaknesses that were present in the systems at the time of the test.

A number of criteria were defined in advance to enable classification of penetration tests that have been carried out. The following figure is based on the study "implementation concept for penetration tests"[1] from the BSI and is intended to reflect the procedure within this test.

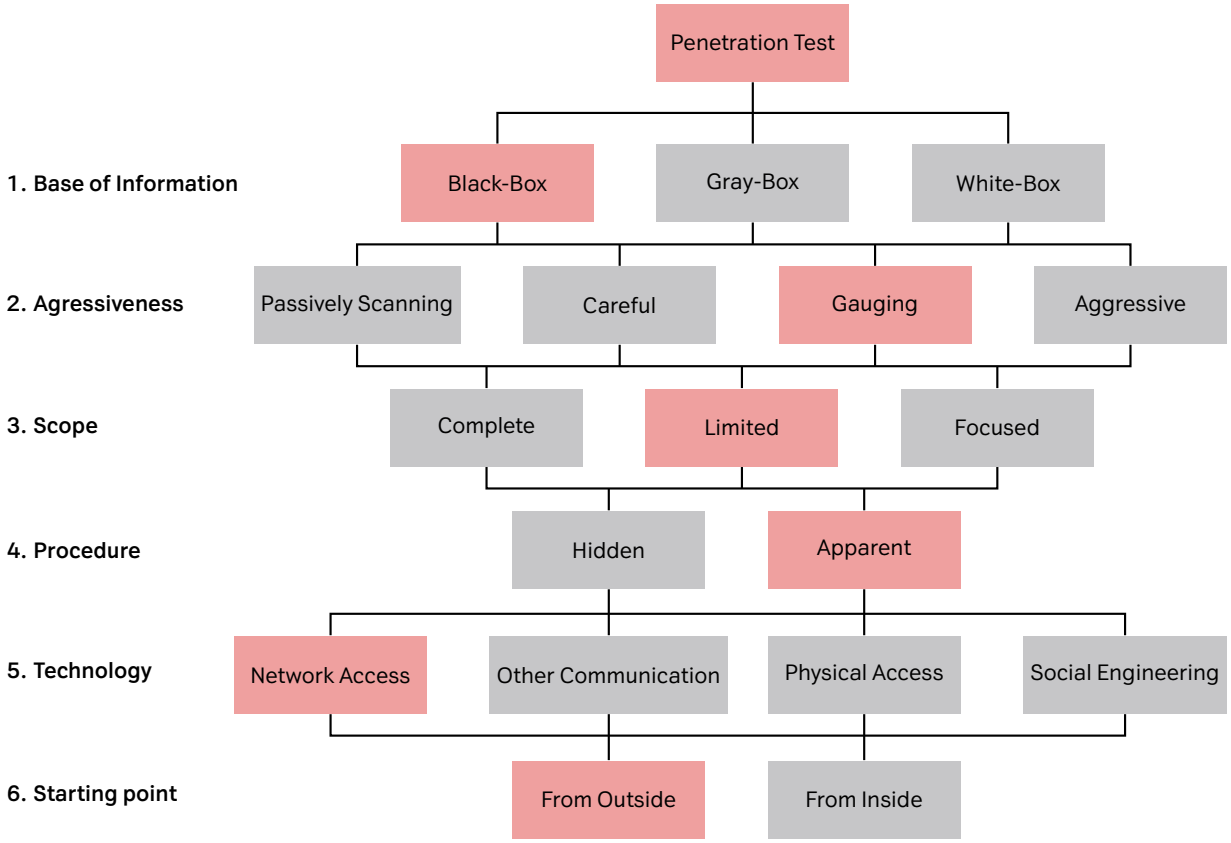


Figure 3: Implementation concept for penetration tests

4.1 Risk assessment according to CVSSv3

The Common Vulnerability Scoring System (CVSS) provides the ability to identify and score the underlying characteristics of a weakness. The result is a numerical value that can range between **0.0 and 10.0**, with **10.0** being the highest and thus most critical value. For a detailed description of the CVSS metrics, see 6.2. To be able to express the risk in words, five different value ranges are defined, which are described in the chapter 6.3. Accordingly, a risk can be classified as **"none", "low", "medium", "high"** and **"critical"**.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf

5 Identified weaknesses

The weaknesses identified during the test are described below and assigned a risk rating. This risk assessment is carried out according to the CVSSv3 standard and was performed by the assessor to the best of his knowledge and belief. The risk assessment may therefore differ from the customer's assessments, as in most cases the assessor does not have sufficient background knowledge to perform a specific business risk assessment.
Each identified weakness described includes recommended countermeasures and references to external resources for further information.

5.1 SQL Injection leading to Command Execution

CVSSv3 Score	**9.9 (Critical)**
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H (show in first.org)

Affected Systems

- dashboard.example.com (203.0.113.5:443 (TCP))

Description

On the dashboard available at `https://dashboard.example.com`, an SQL injection vulnerability was identified that allowed authorized users to read, modify or delete data in the database. Attackers could use this to access user information and passwords. Because the dashboard is connected to the database with a privileged account, the SQL injection can furthermore be leveraged to have command execution on the system.

Recommendations

- Most SQL injection vulnerabilities can be prevented by using **parameterized queries** (also known as **prepared statements**) instead of string concatenation within the query.
- The **principle of least privilege** should be implemented universally.
  - A user different from `postgres` should be created and dedicated to the database of the dashboard.
  - This user should only have access to data that is really necessary.
  - Privileges should also be limited to actions on the database itself and not on the whole Database Management System.
- Source code should be reviewed to check for other potential SQL Injection sources, e.g. user inputs.
- The impact on the network of the compromised server should be evaluated to know how far an attacker would have been able to move.

Technical Description

An **SQL injection** is a web application vulnerability that allows attackers to send queries directly to the database in order to gain unauthorized access to it. The vulnerability occurs when the user's input data is not sufficiently validated on the server side and is passed directly to the database. The following illustration shows an example of how an **SQL injection** can be exploited.

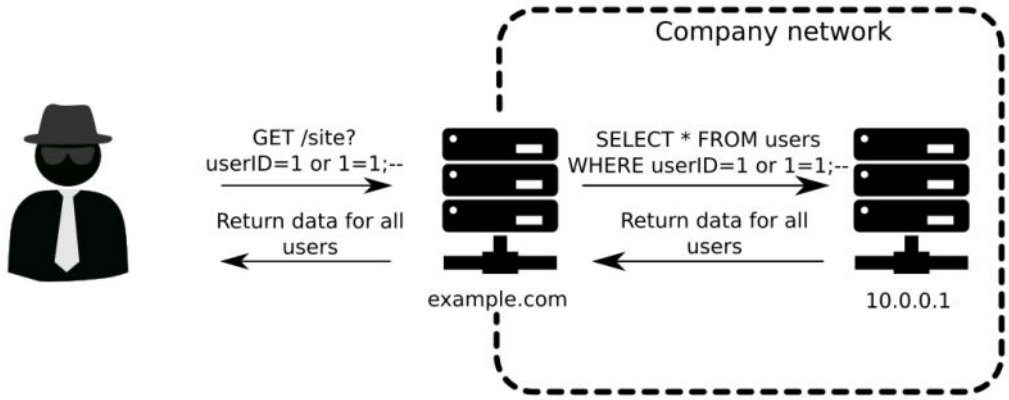


Figure 4: All user data is queried by exploiting an SQL injection vulnerability

In the dashboard application, the URL- and data parameters are not parsed properly. Due to this, attackers can use an SQL injection to directly query the database. In this example, the type of the injection is **blind Boolean-based**. An attacker cannot have the direct output of the query. However, the parameter `success` of the response will be `true` or `false` depending on whether the result is empty or not. Therefore, an attacker can enumerate the whole database, character by character. This requires a large amount of queries, but can be automated with tools like **sqlmap**. At the end, data like the database version or the hash of the admin password can be retrieved, as shown in the screenshots below.

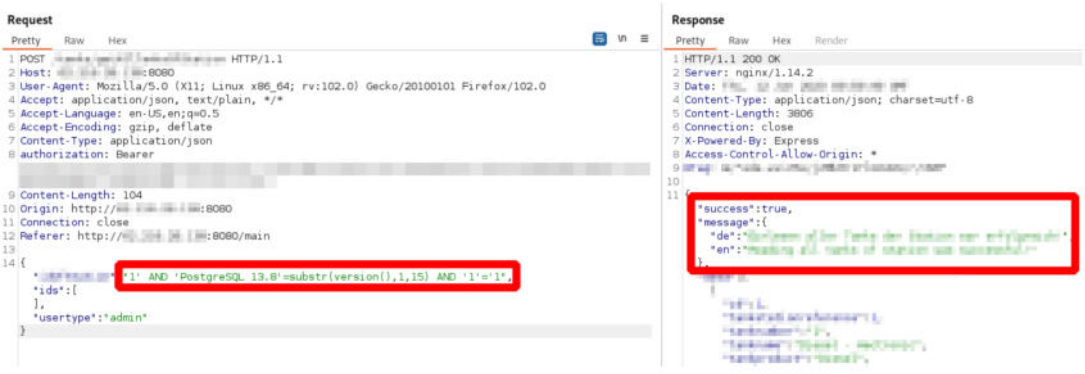


Figure 5: Search for the database version

Figure 6: Search for the admin password

Moreover, the web application is connected to the database with the user `postgres`. As shown below, this user is granted the role of `pg_execute_server_program` which is used to execute commands on the system hosting the database.

```
postgres=#  SELECT oid, rolname FROM pg_roles WHERE pg_has_role('postgres', oid, 'member');
  oid   |          rolname
--------+---------------------------
    10  | postgres
  3373  | pg_monitor
  3374  | pg_read_all_settings
  3375  | pg_read_all_stats
  3377  | pg_stat_scan_tables
  4569  | pg_read_server_files
  4570  | pg_write_server_files
  4571  | pg_execute_server_program
  4200  | pg_signal_backend
```

In the following listing, access gained through this SQL Injection can be seen, confirming the user to be `postgres` and being able to access files.

```
postgres@host: whoami
postgres

postgres@host: id
uid=112(postgres)   gid=118(postgres)   groups=118(postgres),117(ssl-cert)

postgres@host: cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

As a consequence, attackers can execute arbitrary commands on the system. This can lead to a full compromise of the system, if attackers manage to escalate their privileges to the superuser (e.g. root). It can also be used to attack internal vulnerable systems that are not directly accessible from the internet. This way, attackers could steal, delete, or encrypt data, compromising confidentiality, availability, or integrity.

Additional Information / References

- https://www.owasp.org/index.php/SQL_Injection
- https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

5.2 Default Credential Usage

CVSSv3 Score	9.8 (Critical)
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (show in first.org)

Affected Systems

- dashboard.example.com (203.0.113.5:443 (TCP))

Description

The application `https://dashboard.example.com` has been found to have accounts with default credentials. Those allow attackers to easily compromise access controls by testing well known or easily guessable combinations. Due to default accounts often being highly privileged, this can have far-reaching consequences and gives attackers easy access to the application.

Recommendations

- Default accounts should be disabled.
- A strong **password policy** should be enforced, so users need to change passwords on first login/set custom passwords on signing up. The following characteristics for such a policy are recommended:
  - Passwords should be at least 14 characters long.
  - Passwords should consist of upper and lower case letters, numbers and special characters.
  - The password should not be a common password (e.g. sequence of numbers, sequence of letters, dictionary entry, etc).
- It should be evaluated if other accounts are using default credentials too.

Technical Description

Default accounts are artifacts which usually originate from development or quality assurance teams, or from the initial setup of a system. Numerous systems require an already existing account to be able to complete the setup or test phase. For this, a manufacturer often creates an admin account with a trivial password. Such accounts can easily be enumerated for example by trying well-known combinations, analyzing the source code or even the application's binary file.

At the time of the assessment, the following usernames set up with a trivial password, were found on the application `https://dashboard.example.com` by trying known combinations:

- `admin`

Moreover, by gaining this authenticated access, unauthenticated attackers can also leverage the vulnerability described in **SQL injection leading to command execution** to obtain remote code execution.

Additional Information / References

- https://www.owasp.org/index.php/Testing_for_default_credentials_(OTG-AUTHN-002)

5.3 Outdated Software with Known Vulnerabilities

CVSSv3 Score	8.4 (High)
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RC:U (show in first.org)

Affected Systems

- srv02.example.com (203.0.133.8:443 (TCP))

Description

At the time of the assessment, the `srv02.example.com` system appeared to be using outdated software that had at least the known vulnerability **CVE-2019-11043**. For the outdated version of **PHP** identified, there are already publicly available exploits. Attackers could use these exploits to access sensitive data on this system, make the system unavailable, or fully take over the system.

Recommendations

- It is recommended to update the outdated software as soon as possible to the latest stable version which includes the most recent security patches.
- A continuous update process should be established, which guarantees that security-critical updates can be installed quickly.
- If updates are not possible, the affected systems should be isolated and locked down to make access more difficult or impossible.

Technical Description

Using third-party software and services on a system requires keeping them updated. New security issues for publicly available software are discovered every day. These vulnerabilities are quickly known by attackers and exploits can be publicly available shortly after discovery. After the discovery of new vulnerabilities in their software, publishers usually release security patches in a timely manner. Installed versions should be updated on the system right after.

The server `srv02.example.com` is running an outdated version of **PHP** and **nginx**. The following table shows the versions detected by the scan and the latest ones that should be installed:

Software	Installed Version	Current Version
PHP	7.2.10	8.2.6
nginx	1.23.1	1.23.4

Table 5: Software versions detected by the scan

If used with nginx and the FPM module, this version of PHP is known to be vulnerable to **CVE-2019-11043**. There are already published exploits available for vulnerabilities in this version. Attackers can use these exploits to perform remote code execution on the system. This major version of PHP has reached its end of life and is no longer supported. If new critical vulnerabilities are found in the future, no security patch will be available.

For more details on the outdated software products and associated vulnerabilities, see the **Nessus** vulnerability scan attached to this report.

Additional Information / References

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities
- https://nvd.nist.gov/vuln/detail/CVE-2019-11043

5.4 Open SMTP Server allows User Enumeration

CVSSv3 Score	5.3 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (show in first.org)

Affected Systems

- mail.example.com (203.0.133.6:25 (TCP))

Description

On the target `mail.example.com`, an SMTP server has been identified during the security assessment, on which it was possible to enumerate valid user accounts. Attackers could use the obtained information for follow-up attacks, such as a brute force attack.

Recommendations

- It is recommended to disable the `VRFY` command to avoid user enumeration.
- Other mail servers which were not in the scope of the assessment should be checked for user enumeration.
- Others command like `EXPN` and `RCPT TO` also lead to user enumeration and should be disallowed on all mail servers.

Technical Description

User enumeration is a vulnerability that allows attackers to guess valid user accounts. Scanning techniques are used to collect server responses which are then further analyzed to determine if a user account is valid or not. Attackers could then use the information gained in follow-up attacks, such as brute force attacks, to guess the passwords of identified user accounts.

During the security test, it was found that an SMTP server was running on the target `mail.example.com`. This SMTP server allowed the command `VRFY` for anonymous users. Attackers can use this command to check the existence of certain users on the system. The following listing shows which SMTP commands are supported/allowed by the server:

```
$ nmap -p 25 mail.example.com --script=smtp-commands
Nmap scan report for mail.example.com (203.0.133.6)
Host is up (0.045s latency)
PORT        STATE   SERVICE     VERSION
25/tcp      open    smtp        Postfix smtp
|_ stmp-commands: mail.example.com (203.0.133.6), PIPELINING, SIZE 10248080, VRFY, ETRN,
    ↪ ENHANCEDSTATUSCODES, 8BITMIME, DSN, CHUNKING
```

With automated tools, attackers can easily check for common usernames:

```
$ nmap -p 25 mail.example.com --script=smtp-enum-users
Nmap scan report for mail.example.com (203.0.133.6)
Host is up (0.031s latency)
PORT        STATE   SERVICE
25/tcp      open    smtp
| smtp-enum-users:
|_  root
```

The listing above shows, that the user `root` has been detected to be a valid user on the mail server.

Additional Information / References

- https://www.rapid7.com/db/vulnerabilities/smtp-general-vrfy/

5.5 Remote Desktop Protocol (RDP) Publicly Accessible

CVSSv3 Score	5.3 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (show in first.org)

Affected Systems

- srv01.example.com (203.0.133.2:3389 (TCP))

Description

In the course of the testing, the remote maintenance service **Remote Desktop Protocol (RDP)** was detected on the host `srv01.example.com`. RDP has repeatedly been affected by serious security vulnerabilities in the past. Due to the high security risk, RDP should therefore not be directly exposed to the internet.

Recommendations

- It is strongly recommended not to expose sensitive services such as RDP directly to the internet because of the high security risk.
- If access to the RDP server is necessary over the internet, a **Virtual Private Network (VPN)** should be used to limit the network accessibility of the system.

Technical Description

The **Remote Desktop Protocol**, commonly referred to as RDP, is a proprietary protocol developed by Microsoft that allows a graphical connection to be made to a computer via the network. The history of RDP from a security perspective is versatile. Since 2002, there have been at least 20 Microsoft security updates specific to RDP, and at least 24 separate CVEs (see References).

During the course of the assessment, it was determined that the RDP remote service from host `srv01.example.com` is publicly accessible via the internet. The following listing illustrates the current state:

```
$ nmap -p 3389 srv01.example.com
Nmap scan report for srv01.example.com (203.0.133.2)
Host is up (0.0.12s latency).

PORT        STATE   SERVICE
3389/tcp    open    ms-wbt-server

Nmap done 1 IP adresse (1 host up) scanned in 0.84 seconds
```

Additional Information / References

- https://blog.rapid7.com/2017/08/09/remote-desktop-protocol-exposure/

5.6 Weak SSH settings

CVSSv3 Score	4.2 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N (show in first.org)

Affected Systems

- relay.example.com (203.0.133.15:2222 (TCP))

Description

Some affected systems were configured with weak **SSH settings**. Attackers with access to the network traffic could theoretically break the encryption and thus gain access to sensitive data such as usernames and passwords.

Recommendations

- It is recommended to support only secure and modern cipher, key exchange and MAC algorithms.
- If secure configuration (ciphers, key exchange, MAC algorithms) can't be applied, the system should not be directly exposed to the internet. A jump host with proper configuration could be used instead.
- The configuration of other SSH servers, outside the scope of this assessment, should also be examined.

Technical Description

At the time of the assessment, a system using weak **SSH settings** was identified.

The SSH server on `relay.example.com:2222` accepted the following **weak key exchange algorithms**:

- `diffie-hellman-group-exchange-sha1`
- `diffie-hellman-group1-sha1`

The server is also configured to accept several **weak encryption ciphers** that should be disabled in production environments:

- `3des-cbc`
- `aes128-cbc`
- `aes192-cbc`
- `aes256-cbc`
- `blowfish-cbc`
- `cast128-cbc`

Using man-in-the-middle attacks, connections negotiated based on insecure ciphers or using a weak key exchange algorithm could potentially be deciphered, exposing passwords and other sensitive information, which could lead to the compromise of the affected machine.

Additional Information / References

- https://infosec.mozilla.org/guidelines/openssh
- https://linuxhandbook.com/ssh-hardening-tips/
- https://sshcheck.com/
- https://www.sshaudit.com/

6 Appendix

6.1 Contact persons

A1 Digital International GmbH

Name	Role	Telephone	E-Mail
Alice Codex	Execution of Security Assessment	+431234567890	ask.security@a1.digital
Trent Trustworthy	Review	+431234567890	ask.security@a1.digital
Bob Binary	Review	+431234567890	ask.security@a1.digital

Table 6: Contact persons at A1 Digital International GmbH

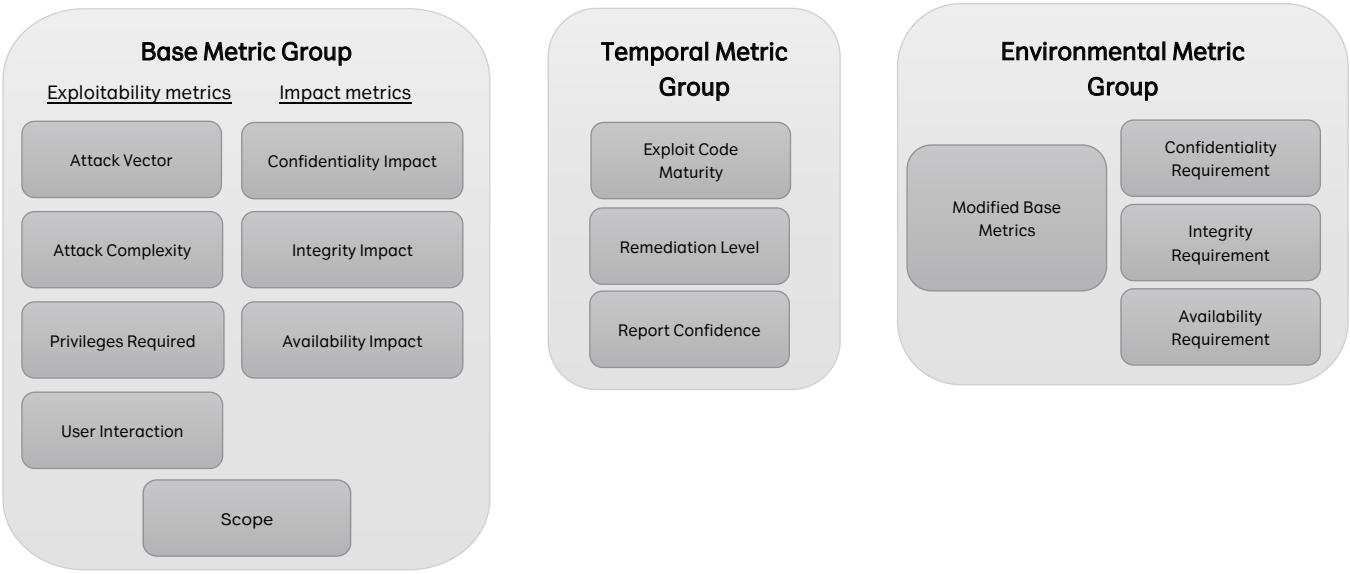
Example GmbH

Name	Role	Telephone	E-Mail
Jane Doe	Lead of Example Department	+4312345678901	jd@example.com
Maximilian Muster	Support	+4312345678902	mm@example.com

Table 7: Contact persons at Example GmbH

6.2 CVSS v3.0 metrics

CVSS comprises three metric groups: **Base, Temporal** and **Environmental** as shown in the figure below:



6.2.1 Base Metric Group

The **Base Metric Group** expresses the fundamental risk of a weakness and assesses the vulnerable component. No valid CVSS value can be formed without a Base Metric. In turn the Base Metric is divided into Exploitability Metrics and Impact Metrics.
The **Exploitability Metric** reflects the ease and required pre-requisites for successful utilisation of the weakness.
The **Impact Metric** on the other hand reflects the direct consequence of the successful utilisation of the weak point - is the confidentiality, integrity or availability of the affected data/ of the affected system endangered?

Metric	Possible values
Attack Vector (V) - attack vector	Network (N), Adjacent (A), Local (L), Physical (P)
Attack Complexity (AC) - attack complexity	Low (L), High (H)
Privileges Required (PR) - privileges required	None (N), Low (L), High (H)
User Interaction (UI) - required user interaction	None (N), Required (R)
Scope (S) - affected area	Changed (C), Unchanged (U)
Confidentiality Impact (C) - loss of confidentiality	None (N), Low (L), High (H)
Integrity Impact (I) - loss of integrity	None (N), Low (L), High (H)
Availability Impact (A) - loss of availability	None (N), Low (L), High (H)

Table 8: Overview of Base Metric Group

6.2.2 Temporal Metric Group

The **Temporal Metric Group** expresses the characteristics of a weak point which may change over time. For example after some time an official patch may be published, which would reduce the Temporal Score.

Metric	Possible values
Exploit Code Maturity (E) - degree of maturity of the exploit code present	Not Defined (X), High (H), Functional (F), Proof of Concept (P), Unproven (U)
Remediation Level (RL) - countermeasures present	Not Defined (X), Unavailable (U), Workaround (W), Temporal Fix (T), Official Fix (O)
Report Confidence (RC) - measures the reliability of the available information regarding the weakness	Not Defined (X), Confirmed (C), Reasonable (R), Unknown (U)

Table 9: Overview of Temporal Metric Group

6.2.3 Environmental Metric Group

The **Environmental Metric Group** is specially set for the user environment. This metric allows the adaptation of the scores with respect to the importance of an affected system for the user/customer. The adjustment is done based on the requirements for confidentiality, integrity and availability.

Metric	Possible values
Confidentiality Requirement (CR) - requirement for confidentiality	Network (N), Adjacent (A), Local (L), Physical (P)
Integrity Requirement (IR) - requirement for integrity	Low (L), High (H)
Availability Requirement (AR) - requirement for availability	None (N), Low (L), High (H)

Table 10: Overview of Environmental Metric Group

6.2.4 Modified Base Metric Group

In addition, the base metrics can be shown as a modified value (modified base metric).
This can be used to describe situations which increase the base score. For example a component could require multiple factors for authentication as standard (PR: High) in order to reach specific resources, whereas in the test environment no authentication was required (PR: None).

Metric	Possible values
Modified Attack Vector (MAV)	The same values as the associated base metrics + not defined (N).
Modified Attack Complexity (MAC)	
Modified Privileges Required (MPR)	
Modified User Interaction (MUI)	
Modified Scope (MS)	
Modified Confidentiality (MC)	
Modified Integrity (MI)	
Modified Availability (MA)	

Table 11: Overview of Modified Base Metric Group

Detailed information regarding the base, temporal and environmental metrics and their values are available on the *first.org* website[2]

6.3 Text representation of CVSS v3.0 scores

In most cases it is helpful to have a text representation of the numerical CVSS scores. Each individual metric (Base, Temporal and Environmental) can be brought into text form using the following table.[3][4]

Severity	CVSS v3 Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table 12: Text representation of CVSS v3.0 scores

[2] https://www.first.org/cvss/specification-document
[3] https://nvd.nist.gov/vuln-metrics/cvss
[4] https://www.first.org/cvss/specification-document#Qualitative-Severity-Rating-Scale

6.4 List of Tables

6.5 List of Figures

6.6 OWASP Testing Guide Version 4.2

Information Gathering
Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)
Fingerprint Web Server (OTG-INFO-002)
Review Webserver Metafiles for Information Leakage (OTG-INFO-003)
Enumerate Applications on Webserver (OTG-INFO-004)
Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)
Identify application entry points (OTG-INFO-006)
Map execution paths through application (OTG-INFO-007)
Fingerprint Web Application Framework (OTG-INFO-008)
Fingerprint Web Application (OTG-INFO-009)
Map Application Architecture (OTG-INFO-010)

Configuration and Deployment Management Testing
Test Network/Infrastructure Configuration (OTG-CONFIG-001)
Test Application Platform Configuration (OTG-CONFIG-002)
Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)
Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)
Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)
Test HTTP Methods (OTG-CONFIG-006)
Test HTTP Strict Transport Security (OTG-CONFIG-007)
Test RIA cross domain policy (OTG-CONFIG-008)
Test File Permission (OTG-CONFIG-009)

Identity Management Testing
Test Role Definitions (OTG-IDENT-001)
Test User Registration Process (OTG-IDENT-002)
Test Account Provisioning Process (OTG-IDENT-003)
Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
Testing for Weak or unenforced username policy (OTG-IDENT-005)

Authentication Testing
Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)
Testing for default credentials (OTG-AUTHN-002)
Testing for Weak lock out mechanism (OTG-AUTHN-003)
Testing for bypassing authentication schema (OTG-AUTHN-004)
Test remember password functionality (OTG-AUTHN-005)
Testing for Browser cache weakness (OTG-AUTHN-006)
Testing for Weak password policy (OTG-AUTHN-007)
Testing for Weak security question/answer (OTG-AUTHN-008)
Testing for weak password change or reset functionalities (OTG-AUTHN-009)
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)

Authorization Testing
Testing Directory traversal/file include (OTG-AUTHZ-001)
Testing for bypassing authorization schema (OTG-AUTHZ-002)
Testing for Privilege Escalation (OTG-AUTHZ-003)
Testing for Insecure Direct Object References (OTG-AUTHZ-004)

Session Management Testing
Testing for Bypassing Session Management Schema (OTG-SESS-001)
Testing for Cookies attributes (OTG-SESS-002)
Testing for Session Fixation (OTG-SESS-003)
Testing for Exposed Session Variables (OTG-SESS-004)
Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
Testing for logout functionality (OTG-SESS-006)
Test Session Timeout (OTG-SESS-007)
Testing for Session puzzling (OTG-SESS-008)

Input Validation Testing
Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
Testing for HTTP Verb Tampering (OTG-INPVAL-003)
Testing for HTTP Parameter pollution (OTG-INPVAL-004)
Testing for SQL Injection (OTG-INPVAL-005)
Oracle Testing
MySQL Testing
SQL Server Testing
Testing PostgreSQL (from OWASP BSP)
MS Access Testing
Testing for NoSQL injection
Testing for LDAP Injection (OTG-INPVAL-006)
Testing for ORM Injection (OTG-INPVAL-007)
Testing for XML Injection (OTG-INPVAL-008)
Testing for SSI Injection (OTG-INPVAL-009)
Testing for XPath Injection (OTG-INPVAL-010)
IMAP/SMTP Injection (OTG-INPVAL-011)
Testing for Code Injection (OTG-INPVAL-012)
Testing for Local File Inclusion
Testing for Remote File Inclusion
Testing for Command Injection (OTG-INPVAL-013)
Testing for Buffer overflow (OTG-INPVAL-014)
Testing for Heap overflow
Testing for Stack overflow
Testing for Format string
Testing for incubated vulnerabilities (OTG-INPVAL-015)
Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)

Testing for Error Handling
Analysis of Error Codes (OTG-ERR-001)
Analysis of Stack Traces (OTG-ERR-002)

Testing for weak Cryptography
Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)
Testing for Padding Oracle (OTG-CRYPST-002)
Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

Business Logic Testing
Test Business Logic Data Validation (OTG-BUSLOGIC-001)
Test Ability to Forge Requests (OTG-BUSLOGIC-002)
Test Integrity Checks (OTG-BUSLOGIC-003)
Test for Process Timing (OTG-BUSLOGIC-004)
Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)
Testing for the Circumvention of Work Flows (OTG-BUSLOGIC-006)
Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)
Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)
Test Upload of Malicious Files (OTG-BUSLOGIC-009)

Client Side Testing
Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
Testing for JavaScript Execution (OTG-CLIENT-002)
Testing for HTML Injection (OTG-CLIENT-003)
Testing for Client Side URL Redirect (OTG-CLIENT-004)
Testing for CSS Injection (OTG-CLIENT-005)
Testing for Client Side Resource Manipulation (OTG-CLIENT-006)
Test Cross Origin Resource Sharing (OTG-CLIENT-007)
Testing for Cross Site Flashing (OTG-CLIENT-008)
Testing for Clickjacking (OTG-CLIENT-009)

Testing WebSockets (OTG-CLIENT-010)
Test Web Messaging (OTG-CLIENT-011)
Test Local Storage (OTG-CLIENT-012)

7 Imprint

A1 Digital International GmbH

Business area: Machine-to-machine communication services, IT solutions, devices and other associated products and services
UID number: ATU 66624566

Representative persons:
Dr. Elisabetta Castiglioni (CEO)
Martin Schiffmann (CFO)

FB number: 366000k
Company legal jurisdiction: HG Vienna
Company headquarters: Vienna
Address: Lassallestraße 9, A-1020 Vienna
Contact details: Telephone: (+43) 5 06640; E-Mail: info@a1.digital
Chamber membership: Wirtschaftskammer Wien
Applicable legal regulations: Telecommunication laws: www.ris.bka.gv.at
Regulatory authority/commercial authorities: Österreichische Regulierungsbehörde für Rundfunk und Telekommunikation (RTR GmbH)