

Bsides Munich 2024

Some Thoughts on Penetration Test Reports

Autor

Hans-Martin Münch

Date

11 / 11 / 2024



cat /proc/self

- Hans-Martin Münch
- ~ 20 years in security, mainly doing penetration tests
- Wrote a lot of penetration reports, saw even more

MOGWAI LABS



MOGWAI LABS

is a "no fluff" security outfit specialized on providing penetration tests and technical security reviews.

Agenda

This talk focusses on two aspects of penetration test reporting:

- *Reducing report time*
- *Improving report quality*

1. Finding Templates
2. AI and LLMs
3. Optimizing QA
4. Reporting Tools
5. Severity Ratings
6. Charts and Graphs

Reducing Report Time

- I needed to become more efficient
- At MOGWAI LABS we spend 20 – 30 percent of a penetration test project on reporting
- No one likes doing reporting
- Some things are just ideas, not implemented

01 Finding Templates

Don't repeat yourself

Finding Templates

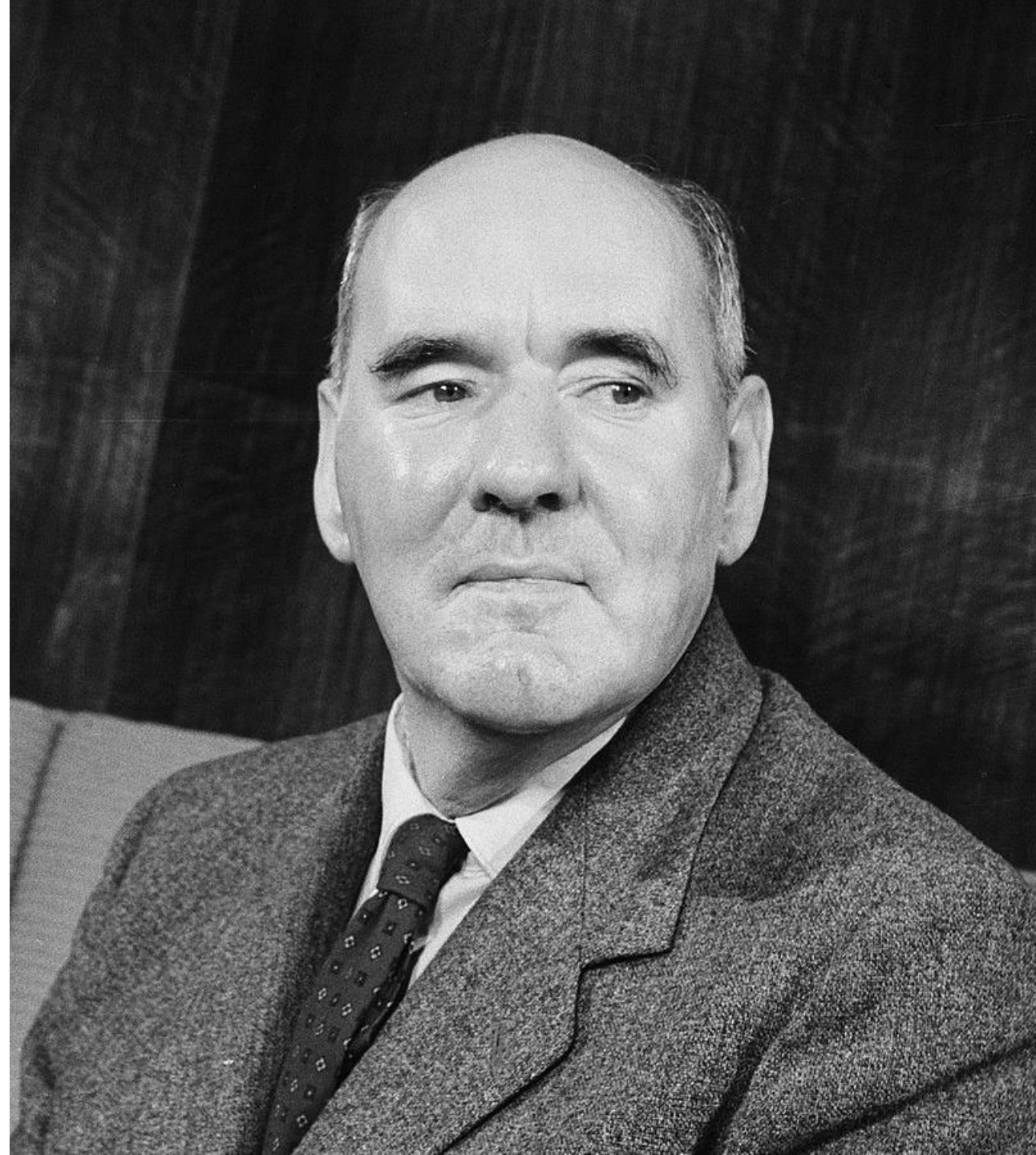
- Best way to reduce time spend on reporting
- Help to "sync" reporting style and quality between team members

Why don't we have a template for that?

Parkinsons Law

“work expands so as to fill the time available for its completion”.

Cyril Northcote Parkinson



You vs. Parkinsons Law

- The penetration test report is the "end product" of the project
- Parkinsons Law: If you have 5 days, the report is done on day 5
- Final report is created while you are already working on the next project (needs to pass QA first)

Fighting Parkinsons Law – Short Deadlines



Solution: Template Driven Reporting

- Similar to "test driven development"
- Don't have a template for finding X? Write it first!
- Use AI to improve the language
- You are doing a first QA by directly using the template

Changing Habits Is Hard

- Not everyone is a good technical writer
- But: Not everyone in your team needs to use that approach
- You don't need to do it on every report
- Two new or improved templates are better than no templates

Splitting Vulnerability Templates

If the root cause or the recommendation differ, we have a different template:

- Reflected / Stored / DOM based Cross Site Scripting (XSS)
- Cross Site Scripting (XSS) through javascript: links
- Cross Site Scripting (XSS) Through WYSIWYG editor
- Cross Site Scripting (XSS) Through HTML / SVG File Upload

03 AI and LLMs

A "fancy autocomplete" is exactly what I want

AI “Problems”

- LLMs need context to generate non generic texts
- I don't want to train an external model with customer data
- Private LLMs to the rescue, but no time to implement this
- Until then: Improving templates

Grammarly on Steroids

I want you to act as an English assistant, spelling corrector and improver. I will speak to you in English and and you answer in the corrected and improved version of my text, in English. I want you to replace my simplified A0-level words and sentences with more beautiful English words and sentences. Keep the meaning same, but use short sentences intended for a technical audience. I want you to only reply the correction, the improvements and nothing else, do not write explanations. Use an active voice. My first sentence is:

Findings Template Writer GPT


ChatGPT allows you to train custom GPTs that serve specific purposes.


When you provide multiple example templates and invest 20 minutes in tweaking, you can already achieve some impressive results.

I use this to scaffold finding templates.


MOGWAI LABS

GPT Updated ×



Penetration Test Findings Template Writer
By MOGWAI LABS GmbH 

Access

 **Invite-only**

[Copy link](#) [View GPT](#)

04 Optimizing QA

Fighting Quality Assurance Fatigue

"Unit Test" Your Reports

- Do placeholders ("ACME", "FOOBAR", "FIXME" and "TODO") exist
- Does content exist twice? (Headlines, Figure descriptions)
- Is the "finding summary" too long?
- Missing image captions / unintended blank pages?
- Do links in the References Section return a HTTP 200 status?

Template / Finding Diffing

- No need to review the same texts again and again
- Diffing usually exists for changes done by the QA, but you want to do this one step earlier.
- Visualize what is part of the template during QA
- Requires a link between the used template (version) and the finding

5.3 Adminer Instance

Severity:

Low

Summary:

The web server **TODC** hosts an instance of the database frontend "Adminer", increasing the overall attack surface of the system.

CVSSv3.1 evaluation:

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N (3.8 – Low)

Vulnerability Description:

"Adminer" is a PHP based web frontend for database systems like MySQL or PostgreSQL, similar to the also very popular tool 'phpMyAdmin'. In contrast phpMyAdmin, Adminer can be deployed in a single file, allowing an easy deployment on web hosts.

While performing a quick analysis of the existing subdomains within the domain foobar.com', we identified an existing Adminer installation, accessible under the following URL:

<https://acme.foobar.com/adminer.php>

Attackers can use the Adminer script to attempt to connect to the internal MySQL database used by the web application. Unlike the web service, the MySQL service can't be directly reached over the internet. By using the Adminer instance, it is possible to bypass this restriction.

The fact that the Adminer login allows the user to configure an arbitrary database host has been previously exploited to perform local file read attacks, using a known design issue in the MySQL protocol (see references). The discovered Adminer instance was on the latest patch level and is not vulnerable to this attack vector.

The Adminer script can also be used to evaluate the firewall rules for outgoing connections by attempting connections to an attacker-controlled system on various ports.

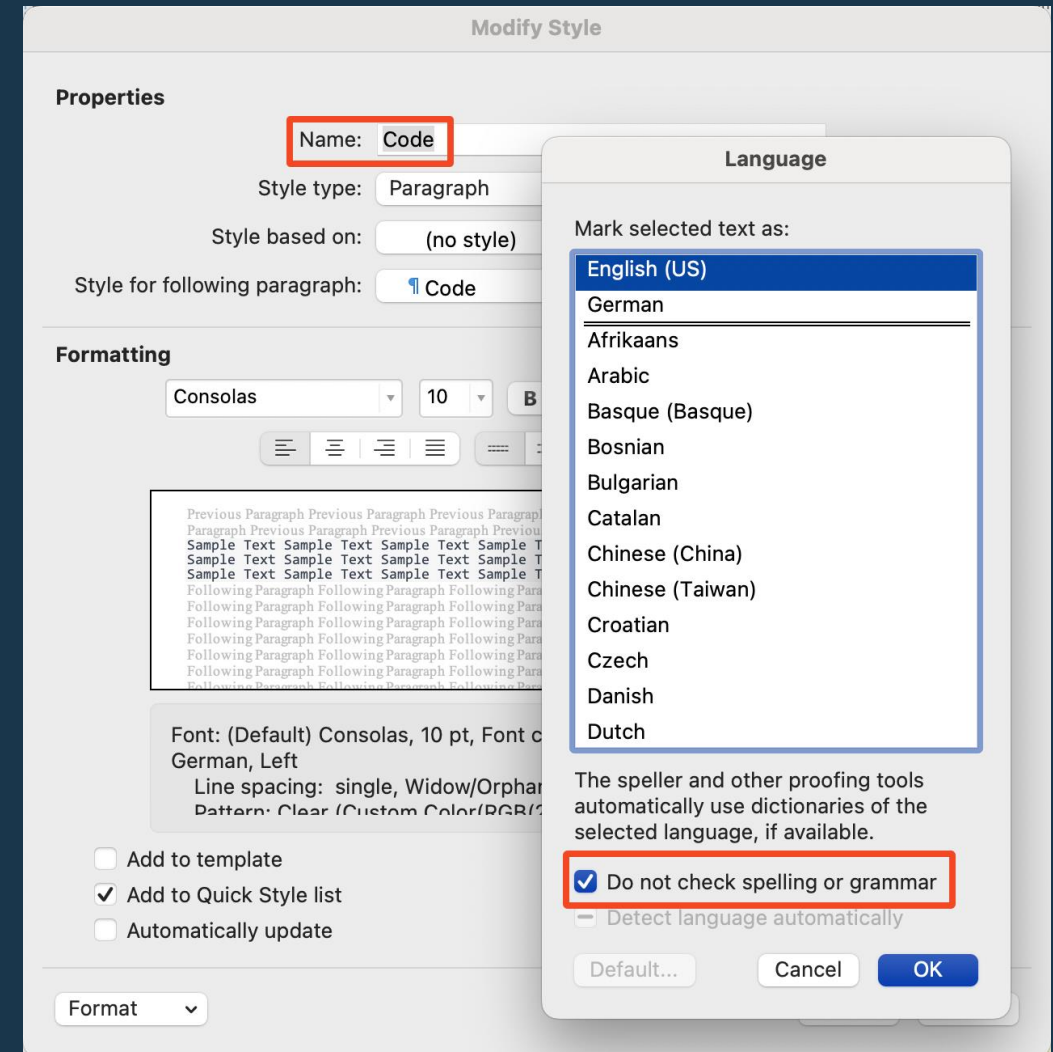
While performing the penetration test, we tried to connect to a MySQL instance under our control, using different ports. This was not successful, we only received incoming DNS requests from Cloudflare.

Reducing Click Fatigue

The general goal is to reduce the total number of clicks during QA

Examples:

- Maintain a custom spell check dictionary for all team members
- Don't check what doesn't make sense



05 Reporting Tools

Your fancy ticketing system...

Penetration Test Reporting Tools

- Countless products and even more inhouse solutions exists
- Key features
 - Template management
 - Keeping report layout in sync
 - Team collaboration
 - Automation (imports etc.)

Failing At A Major Task

Penetration testers are typically not skilled UX designers.

Reporting tools often do not offer a good interface for creating descriptive texts.

MOGWAI LABS

The screenshot displays the Pwndoc web application interface. The main window is titled "Add Vulnerability (Cross Site Scripting (XSS))". It features a form with the following sections:

- Title:** A text input field containing "This is the title".
- Description:** A rich text editor containing the text: "The XXXX WYSIWYG editors are vulnerable to Stored Cross Site Scripting (XSS). By providing malicious HTML code an adversary can inject additional JavaScript code that is executed when the editor tries to render the content. This can be abused to execute commands in the context of the victim's session or modify the displayed HTML content. In the worst-case scenario, a low-privileged user could inject code that grants them administrative access within the application."
- Observation:** A rich text editor containing detailed information about XSS vulnerabilities, including definitions, terms like "stored", and instructions on how to reach the function and what permissions are required.
- Example payload:** A text input field containing the payload: `<h1>test</h1>`.
- CVSS v3.1 Base Score:** A section showing the calculated score of 6.1 (Medium), with sub-scores for Impact (2.8) and Exploitability (2.9).
- Attack Vector:** A section with buttons for Network, Adjacent Network, Local, and Physical.
- Attack Complexity:** A section with buttons for Low and High.
- Privileges Required:** A section with buttons for None, Low, and High.
- User Interaction:** A section with buttons for None and Required.
- Scope:** A section with buttons for Unchanged and Changed.
- Confidentiality Impact:** A section with buttons for None, Low, and High.
- Integrity Impact:** A section with buttons for None, Low, and High.
- Availability Impact:** A section with buttons for None, Low, and High.
- Temporal and Environmental Scores:** A section with a dropdown arrow.
- Remediation:** A rich text editor for providing remediation steps.

Example: Obsidian

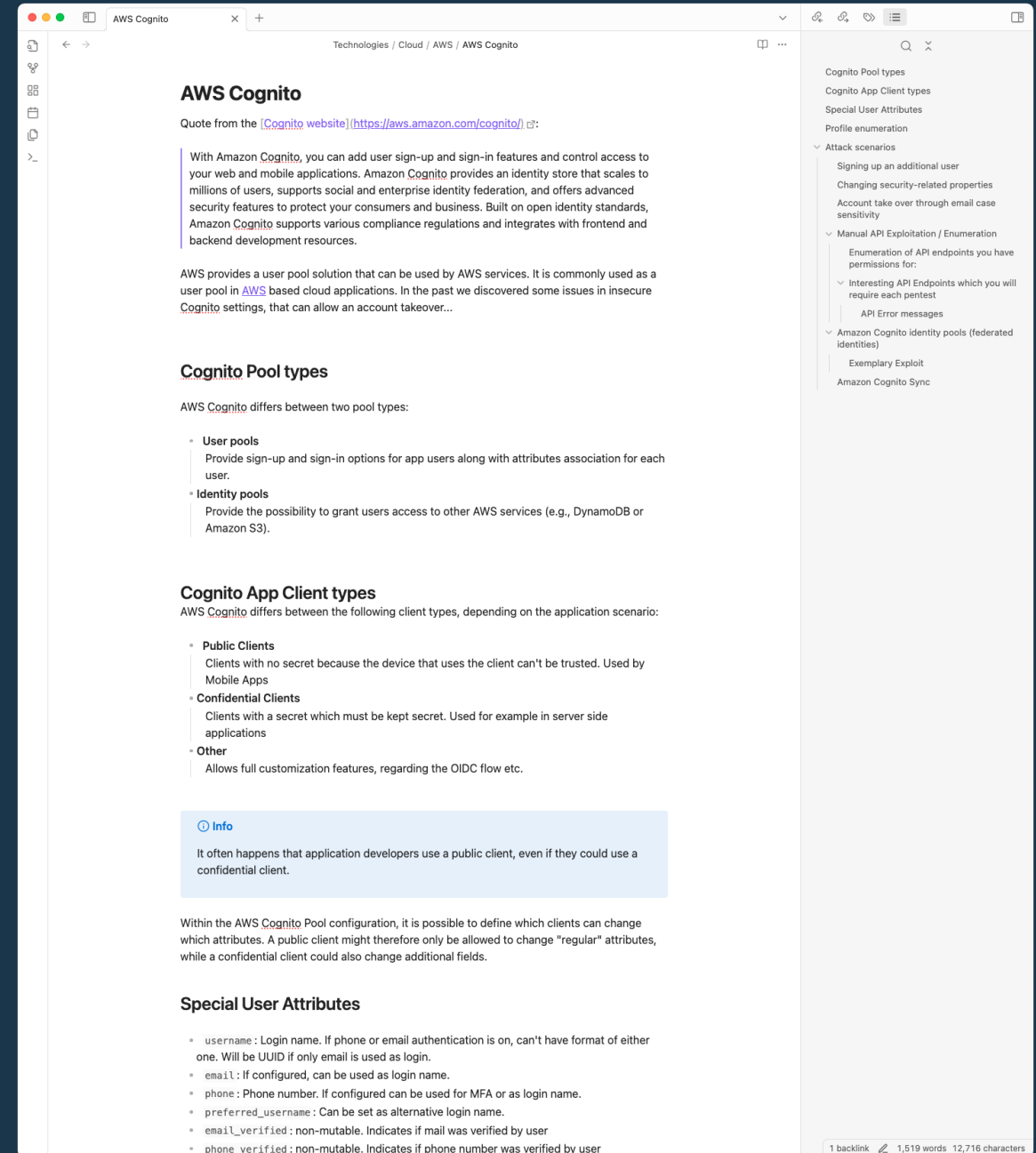
In March 2023, we moved our internal knowledge base from Wiki.js to Obsidian.

The number and quality of entries started to improve.

Other examples:

iA Writer, Ulysses, Bear

MOGWAI LABS



The screenshot shows a web browser window displaying a page titled "AWS Cognito". The page content includes a quote from the AWS Cognito website, a section on "Cognito Pool types" with bullet points for "User pools" and "Identity pools", a section on "Cognito App Client types" with bullet points for "Public Clients", "Confidential Clients", and "Other", an "Info" box stating that application developers often use a public client, and a section on "Special User Attributes" with a list of attributes like "username", "email", "phone", "preferred_username", "email_verified", and "phone_verified". The right sidebar of the browser shows a table of contents for the page, including sections like "Cognito Pool types", "Cognito App Client types", "Special User Attributes", "Profile enumeration", "Attack scenarios", "Manual API Exploitation / Enumeration", and "Amazon Cognito identity pools (federated identities)".

AWS Cognito

Quote from the [Cognito website](https://aws.amazon.com/cognito/) (<https://aws.amazon.com/cognito/>):

With Amazon Cognito, you can add user sign-up and sign-in features and control access to your web and mobile applications. Amazon Cognito provides an identity store that scales to millions of users, supports social and enterprise identity federation, and offers advanced security features to protect your consumers and business. Built on open identity standards, Amazon Cognito supports various compliance regulations and integrates with frontend and backend development resources.

AWS provides a user pool solution that can be used by AWS services. It is commonly used as a user pool in AWS based cloud applications. In the past we discovered some issues in insecure Cognito settings, that can allow an account takeover...

Cognito Pool types

AWS Cognito differs between two pool types:

- **User pools**
Provide sign-up and sign-in options for app users along with attributes association for each user.
- **Identity pools**
Provide the possibility to grant users access to other AWS services (e.g., DynamoDB or Amazon S3).

Cognito App Client types

AWS Cognito differs between the following client types, depending on the application scenario:

- **Public Clients**
Clients with no secret because the device that uses the client can't be trusted. Used by Mobile Apps
- **Confidential Clients**
Clients with a secret which must be kept secret. Used for example in server side applications
- **Other**
Allows full customization features, regarding the OIDC flow etc.

Info

It often happens that application developers use a public client, even if they could use a confidential client.

Within the AWS Cognito Pool configuration, it is possible to define which clients can change which attributes. A public client might therefore only be allowed to change "regular" attributes, while a confidential client could also change additional fields.

Special User Attributes

- **username**: Login name. If phone or email authentication is on, can't have format of either one. Will be UUID if only email is used as login.
- **email**: If configured, can be used as login name.
- **phone**: Phone number. If configured can be used for MFA or as login name.
- **preferred_username**: Can be set as alternative login name.
- **email_verified**: non-mutable. Indicates if mail was verified by user
- **phone_verified**: non-mutable. Indicates if phone number was verified by user

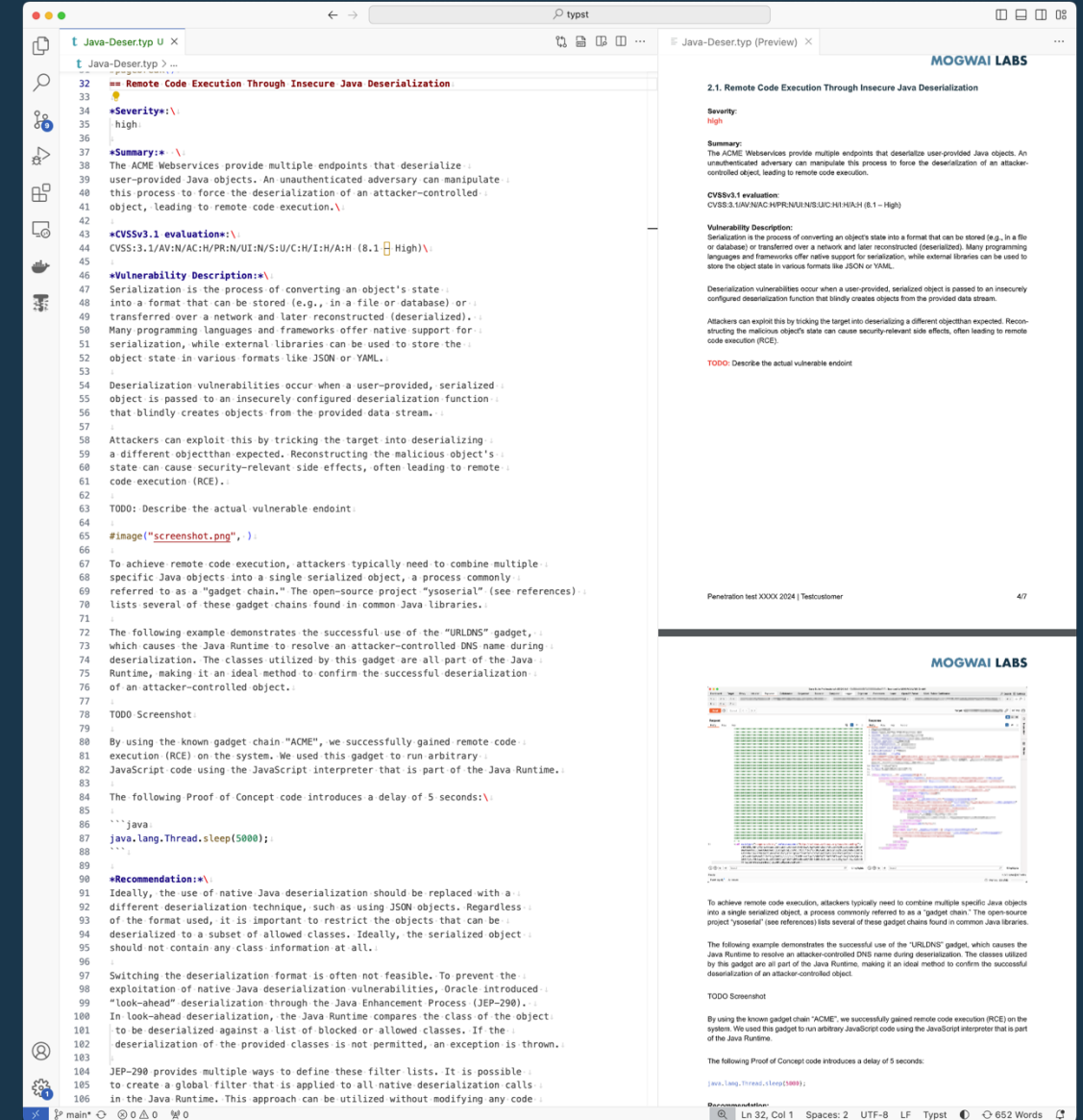
1 backlink 1,519 words 12,716 characters

Typst Is The Better LaTeX

Typst is similar to LaTeX but way less hassle:

- Written in Rust, binary is ~15 MB
- Runs in your web browser through WASM, JavaScript bindings exist
- VSCode extension including live preview (Tinymist Typst)
- Describing error messages
- Decent scripting

MOGWAI LABS



06 Severity Ratings

Are you a 10 out of 10?

Severity Ratings

- CVSS base score is the standard
- We at MOGWAI LABS used CVSS (kind of)
- Still provide the CVSS base score

Custom Scoring System

- Most scorings are variations of the Impact x Likelihood grid
- A finer grid also adds more complexity
- No scoring system is perfect, there are always edge cases

The screenshot shows the OWASP Risk Rating Calculator web application. The browser address bar displays 'owasp-risk-rating.com'. The page title is 'OWASP Risk Rating Calculator'. The interface is divided into two main sections: 'Likelihood Factors' and 'Impact Factors'. The 'Likelihood Factors' section includes 'Threat Agent Factors' (Skill Level, Motive, Opportunity, Size) and 'Vulnerability Factors' (Ease of Discovery, Ease of Exploit, Awareness, Intrusion Detection). The 'Impact Factors' section includes 'Technical Impact Factors' (Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Accountability) and 'Business Impact Factors' (Financial Damage, Reputation Damage, Non-compliance, Privacy Violation). Each factor has a dropdown menu with a value of '0 - N/A'. Below the dropdowns, there are four boxes for 'Threat Agent Factor: Note (TAF: 0)', 'Vulnerability Factor: Note (VF: 0)', 'Technical Impact Factor: Note (TIF: 0)', and 'Business Impact Factor: Note (BIF: 0)'. Below these, there are two boxes for 'Likelihood Factor: Note (LF: 0)' and 'Impact Factor: Note (IF: 0)'. At the bottom, there is a box for 'Overall Risk Severity: Note'. The 'Score Vector' is displayed as '(SL:0/M:0/O:0/S:0/ED:0/EE:0/A:0/ID:0/LC:0/LI:0/LAV:0/LAC:0/FD:0/RD:0/NC:0/PV:0)'. The 'Shortened Score Vector' is displayed as '0000000000000000'. A footer note states 'This Risk Rating Calculator is based on OWASP's Risk Rating Methodology.'

Customer Perspective

- Most customers "think" in severity groups (Critical – Low)
- Vulnerability severity group often defines response deadlines
- They don't care about numbers
- If they do, they need deterministic numbers (CVSS)
- No time to deal with your custom scoring system

Blaze Security Does it Right

- Classification fits on a half page of the report
- Non-technical descriptions
- Avoiding numbers



10.0 Appendix A - Vulnerability Criteria Classification

Below are the risk rating criteria used to classify the vulnerabilities discussed in this report:

SEVERITY	DESCRIPTION
CRITICAL	This leads to the compromise of the system and the data it handles. Can be exploited by an unskilled attacker using publicly available tools and exploits. Must be addressed immediately.
HIGH	Usually leads to the compromise of the system and the data it handles.
MEDIUM	Does not lead to the immediate compromise of the system but when chained with other issues can bring serious security risks. Nevertheless, it is advisable to fix them accordingly.
LOW	Do not pose an immediate risk and even when chained with other vulnerabilities are less likely to cause serious impact.
INFO	Does not pose an immediate risk, but requires continuous surveillance so that it doesn't become a liability through ill-use or future modifications in the system.

07 Charts And Graphs

Let's draw some charts

**Penetration testers love charts
because we assume that management loves charts**



Charts in Management Summaries

Vulnerability Overview

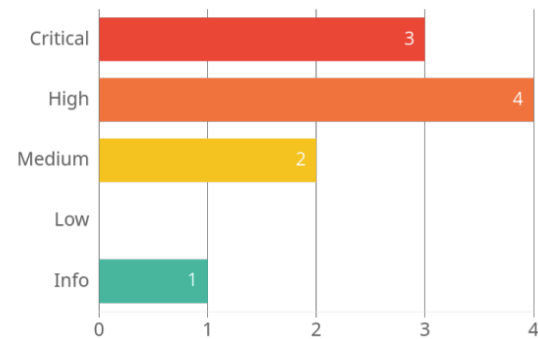


Figure 1 - Distribution of identified vulnerabilities

Finding	Severity
Insecure certificate templates	Critical
Vulnerabilities in outdated software	Critical
Insecure DNS settings enable MitM attacks	Critical
Credentials in Active Directory fields	High
Credentials in Group Policy Preferences	High
Unconstrained delegation for service accounts	High
User accounts vulnerable to Kerberoasting	High
Weak password complexity requirements	Medium
Network access due to missing NAC solution	Medium
Windows Active Directory Audit	Info

2 Management Summary

Es wurde eine Sicherheitsüberprüfung der Webapplikation XYZ der Beispiel XYZ GmbH in Form eines Penetrationstests durchgeführt. Dabei wurde versucht, mit den Mitteln realer Angreifer technische Sicherheitsschwachstellen auszunutzen und mögliche Risiken für die Beispiel XYZ GmbH aufzuzeigen.

Die Erkenntnisse aus dieser Sicherheitsüberprüfung wurden in Form von risikobewerteten Schwachstellen im vorliegenden technischen Detailbericht dokumentiert.

Im Zuge des Penetrationstests wurden **4 Schwachstellen** ermittelt.

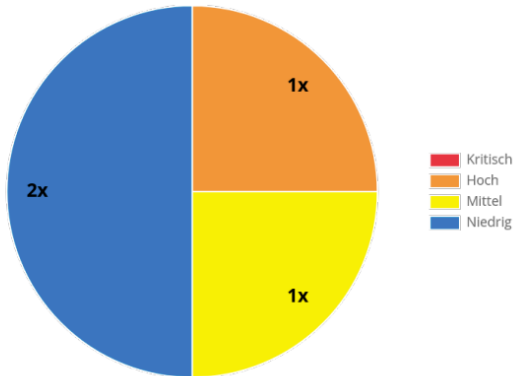


Abbildung 1 - Schwachstellenverteilung

In der Webanwendung konnten Benutzereingaben ungeprüft gespeichert wodurch, welche sogenannte "Stored Cross-Site-Scripting" - Angriffe (XSS) ermöglicht wurden. Die Ausnutzung von gespeicherten XSS-Schwachstellen erfordert keine Benutzerinteraktion, was sie gefährlicher macht als reflektierte XSS-Schwachstellen. Durch solche XSS-Angriffe könnten Session-Cookies gestohlen werden, um Aktionen als der eingeloggte Benutzer durchzuführen, oder die Funktionalität der Seite einzuschränken.

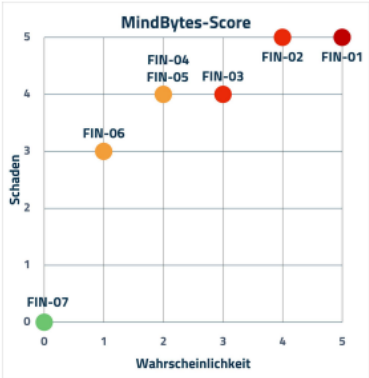


Abbildung 1 - Verteilung nach Schaden und Wahrscheinlichkeit

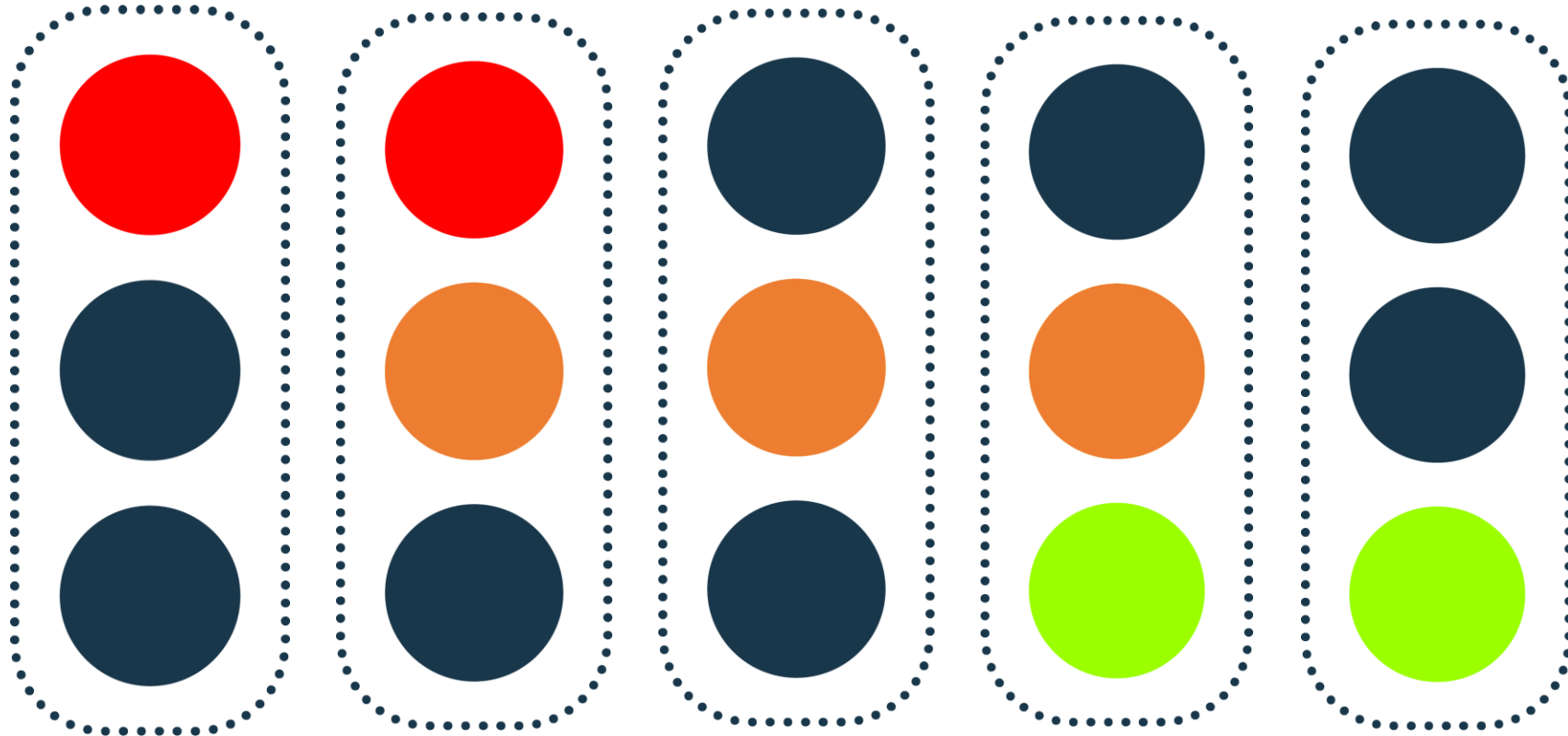


Abbildung 2 - Verteilung nach Risiko

Charts Usage

- Charts allow to compare groups of a data set
- What benefit provides this to the management?
- Management quickly wants to know if they need to take action
- Your visualization must reflect that

HvS Consulting Uses Traffic Lights



08 Summary

Wrapping things up

Summary

- Penetration test reporting provides a lot of optimization potential
- Switching to “Template Driving Reporting” will help you improve
- Don’t bother your customers with things they don’t need
- Talk with your customers about your reports

Thank you!

Do you have any questions?

muench@mogwailabs.de

@h0ng10@infosec.exchange

MOGWAI LABS GmbH

Am Steg 3

89231 Neu Ulm | Germany

info@mogwailabs.de

<https://mogwailabs.de>

MOGWAI LABS