Example Report

Demo Company

Author	Lauritz Holtmann
Date	2025-11-18
Version	0.0.1

Table of Contents

Table of Contents 2

Introduction 3

Version History 4

Scope 5

Technical Details 6

- #PEN20250001: XXE in Test Shop 7
- #PEN20250002: XSS in Test Shop (Fixed) 8
- #PEN-TEST-0003: Open Redirect in Test Shop 10

Conclusion 11

Appendix 12

- Used Tools 12
- Methodology 12

Introduction

A pentest of the *xyz* application of *Z GmbH* was performed from November, 4th to November, 18th 2024. The pentest was performed over the internet against a dedicated pentest instance `pentest.xyz.com`. Additionally, root access to the underlying server of `pentest.xyz.com` as well as full access to the code of the*XYZ* application were granted. During a technical kick-off call, a detailed introduction into the architecture of the application was given.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.

At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur

Version History

The following table lists significant versions and changes of this report.

2025-11-10	0.0.1	Lauritz Holtmann	Report Creation
2025-11-10	0.1.0	Lauritz Holtmann	Addition of Re-Tested Findings from previous Pentest
2025-11-10	0.2.0	Lauritz Holtmann	Addition of Vulnerabilities
2025-11-14	0.7.0	Lauritz Holtmann	Addition of Management Summary (Introduction and Conclusion)
2025-11-14	1.0.0	Lauritz Holtmann	Final Report Creation

Scope

Customer

Test Inc.
Test Street 1
12345 Example City

- **Tim Customer**
- tim@customer.com

Service Provider

Lauritz Holtmann
Südring 25
44787 Bochum

Project Team

- **Lauritz Holtmann**
- pentest@lauritz-holtmann.de

Period: 2025-01-01 - 2025-01-12

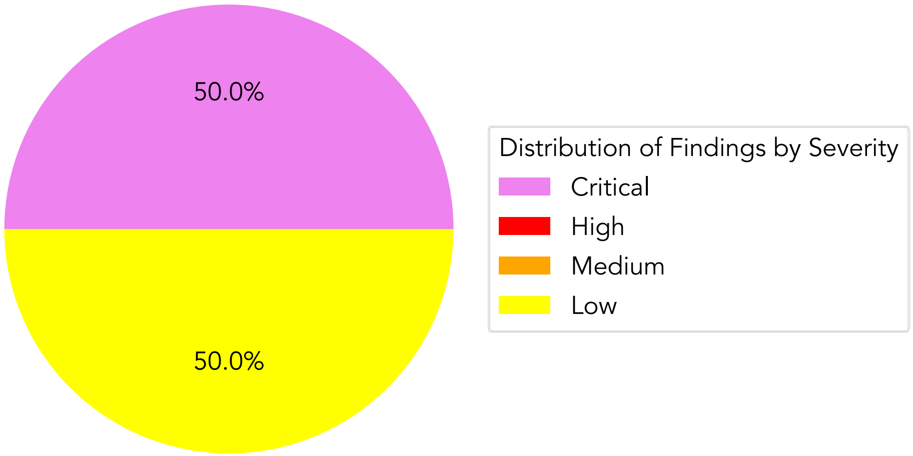
Assets

- Web-Application **Test Shop**
- Database Server **Test DB**

Technical Details

In this section, all identified vulnerabilities are described in detail.

After completion of the pentest, 1 finding(s) with*critical* severity, 0 finding(s) with *high* severity, 0 finding(s) with *medium* severity and 1 finding(s) with *low* severity remain open.



- **Critical** #PEN20250001: XXE in Test Shop (CWE-CWE-611)
- **Low** #PEN-TEST-0003: Open Redirect in Test Shop (CWE-CWE-601)

The following findings were identified and already addressed during the pentest period. They are listed for completeness and are excluded from the statistics and charts above, as they do not require further action but are documented here for transparency.

- **Fixed** #PEN20250002: XSS in Test Shop (CWE-CWE-79)

#PEN20250001: XXE in Test Shop

Asset	CWE	Status	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vector
Test Shop	CWE-611	**Open**	Critical (9.1)	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N*

Description

This type of vulnerability arises, if an application processes XML and is configured to support external entities.

Exemplary Payload:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE abcd [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<example>
   <item>&xxe;</item>
</example>
```

Recommendation

It is recommended to completely disable external entities (DTDs). Further guidance can be found in OWASP's*XML External Entity Prevention Cheat Sheet*.

References

- OWASP: XML External Entity (XXE) Processing

#PEN20250002: XSS in Test Shop (Fixed)

Asset	CWE	Status	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vector
Test Shop	CWE-79	**Fixed**	High (7.1)	*CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N*

Description

A *Cross-Site Scripting* vulnerability has been identified.

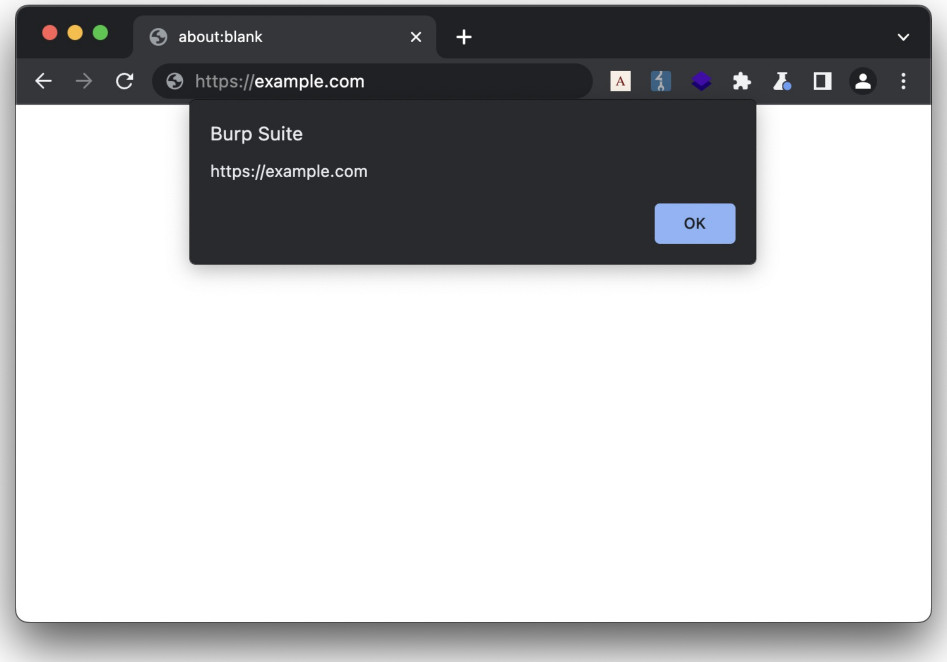
This type of vulnerability arises, if an application uses user-controlled inputs to generate dynamic outputs in an insecure manner.

Exemplary Payload:

```
<s>test</s>
```

JavaScript:

```
[...]
function demo() {
    alert(1);
}
```



Burp Suite

https://example.com

Recommendation

It is recommended to consider all input to the application as potentially dangerous. If user-controlled contents are embedded within the application, they need to be encoded and/or filtered in a *context aware* manner. If the contents are for instance reflected within the JavaScript Context, a different encoding and sanitization needs to be performed than for the HTML context. Further guidance can be found within OWASP's *Cross Site Scripting Prevention Cheat Sheet*.

References

- OWASP: Cross-Site Scripting (XSS)

#PEN-TEST-0003: Open Redirect in Test Shop

Asset	CWE	Status	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vector
Test Shop	CWE-601	**Open**	Low (3.1)	*CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N*

Description

This type if vulnerability arises, if an application redirects to untrusted URLs.

Exemplary Request:

```
GET /redirect?to=https://lhq.at HTTP/1.1
Host: test.shop
```

Response:

```
HTTP/1.1 302 Found
Location: https://lhq.at
```

Recommendation

It is recommended to do not dynamically redirect to untrusted URLs. Further guidance can be found in OWASP's*Open Redirect Prevention Cheat Sheet*.

References

- OWASP: Open Redirect Prevention Cheat Sheet

Conclusion

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.

At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur

Appendix

This chapter includes further supporting materials for this pentest report.

Used Tools

The following tools were used in the course of this pentest:

- Caido: A lightweight web security auditing toolkit
- Burp Suite Professional: Intercepting Proxy
- nmap: Network Mapper
- Nikto: Web server scanner
- SQLmap: SQL injection and database tool
- Nuclei: Vulnerability scanner
- AuRA: Auth. Request Analyser
- sslscan: SSL/TLS service scanner
- testssl: SSL/TLS service scanner
- metasploit: penetration testing framework
- Chromium: Web Browser + Development Tools

Methodology

This penetration test was performed based on industry standards such as the*OWASP Web Security Testing Guide* and the *OWASP Top 10*. The *OWASP Top 10* is regularly updated and covers the most common and relevant threats for web applications. Pentests of mobile applications are additionally performed based on the *OWASP Mobile Security Testing Guide*. Further, pentests of single sign-on (*SSO*) solutions are performed based on best practices such as the*OAuth 2.0 Security Best Current Practice* as well as current research.

Severity Classification

All identified findings are classified according to the Common Vulnerability Scoring System (*CVSS v3.1*). CVSS provides a standardized method to evaluate the technical impact and exploitability of a vulnerability. Scores range from **0.0 to 10.0** and map to the following severity categories:

Severity Level	CVSS Score Range	Description
None	0.0	No direct security impact. However, the condition may still support an attack chain when combined with other weaknesses.
Low	0.1 – 3.9	Limited impact on systems or users. Exploitation typically requires specific circumstances or offers minimal gain to an attacker.
Medium	4.0 – 6.9	Noticeable impact on confidentiality, integrity, or availability. Attackers may exploit the issue with moderate effort or preconditions.
High	7.0 – 8.9	Serious security implications. Exploitation is feasible and may significantly affect data or system operations.
Critical	9.0 – 10.0	Severe risk requiring immediate attention. Vulnerabilities in this range are typically easy to exploit or result in major compromise of systems or data.

Using CVSS ensures consistent prioritization of remediation efforts. Each finding in this report includes its CVSS score, an explanation of the underlying issue, the potential impact, and actionable remediation recommendations.

Timeline of a pentest

A typical timeline of a pentest execution could look as follows:

1. Organizational meeting to discuss the general conditions and the scope
2. Technical meeting to discuss which preparatory actions need to be taken
3. Execution of the pentest
   1. Continuous communications and status updates for all stakeholders, for instance via chat or e-mail
   2. Optional: Immediate access to results in a draft state, for instance via a shared folder or Git repository
4. Creation and submission of the detailed PDF report
5. Final meeting with a presentation of results

After the pentest results are shared, the remediation phase takes place. Optionally, during this phase further consulting can take place. After the identified issues are remediated, typically a retest is performed to verify that the applied measurements effectively address the identified vulnerabilities.