Example Report

Demo Company

Author Lauritz Holtmann
Date 2023-03-24

Table of Contents

Table of Contents 2
Introduction 3
Scope 4
Technical Details 5
#PEN20230001: XXE in Test Shop 6
#PEN20230002: XSS in Test Shop 7
#PEN20230003: Open Redirect in Test Shop 8
Conclusion 9
Appendix 10
Used Tools 10
Methodology 10

Introduction

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

Scope

Lorem Ipsum dolor sit amet

Customer

Test Inc.
Test Street 1
12345 Test

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

Service Provider

Lauritz Holtmann
Test Street 5
12345 Test

Project Team

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

Period: 2022-01-01 - 2022-01-12

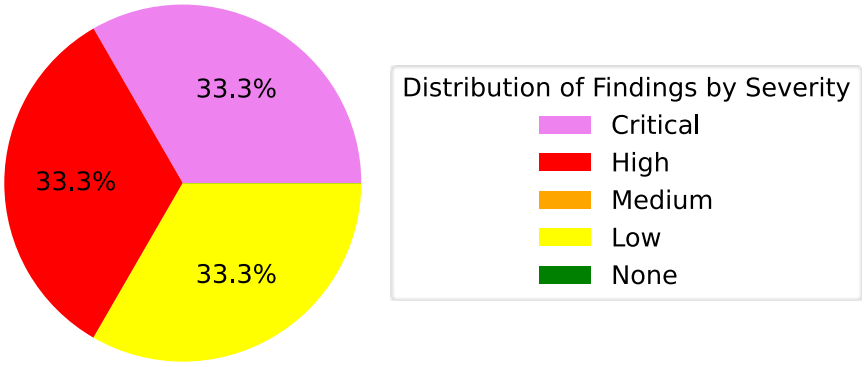
Assets

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

Technical Details

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

During the pentest, 1 finding(s) with *critical* severity, 1 finding(s) with *high* severity, 0 finding(s) with *medium* severity and 1 finding(s) with *low* severity were identified.



- **Critical** #PEN20230001: XXE in Test Shop (CWE-CWE-611)
- **High** #PEN20230002: XSS in Test Shop (CWE-CWE-79)
- **Low** #PEN20230003: Open Redirect in Test Shop (CWE-CWE-601)

#PEN20230001: XXE in Test Shop

Asset	CWE	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vektor
Test Shop	CWE-611	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

#PEN20230002: XSS in Test Shop

Asset	CWE	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vektor
Test Shop	CWE-79	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.

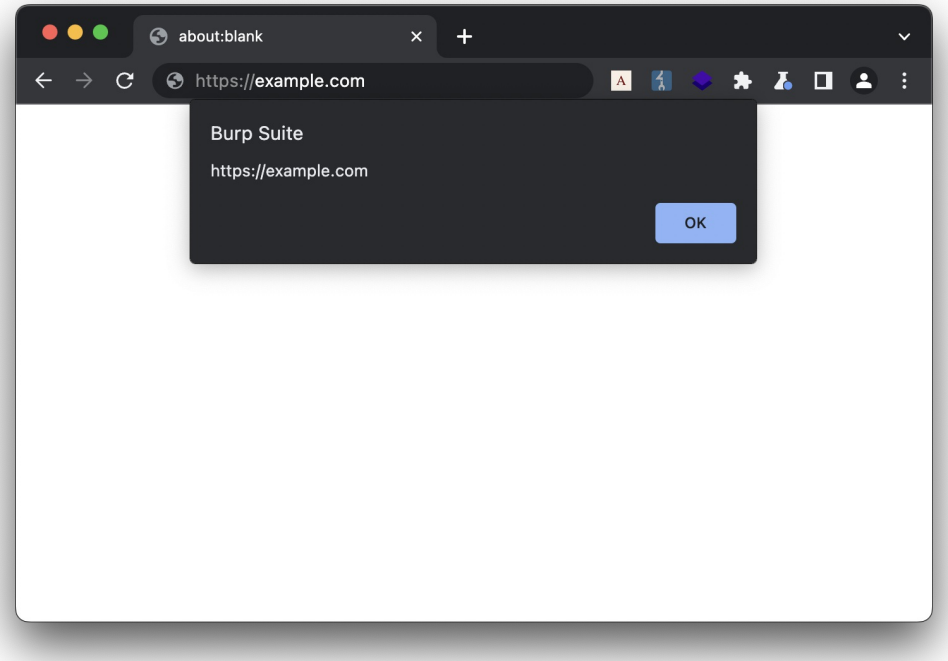
This type of vulnerability arises, if an application uses user-controlled inputs to generate dynamic outputs in an insecure manner.

Exemplary Payload:

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

JavaScript:

```
3   [...]
4   function demo() {
5       alert(1);
6   }
```



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)

#PEN20230003: Open Redirect in Test Shop

Asset	CWE	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vektor
Test Shop	CWE-601	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:

- 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.

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.