Example Report

Demo Company

Author Lauritz Holtmann
Date 2022-08-19

Table of Contents

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, *12* findings with *high* severity, *3* findings with *medium* severity and one finding with informational severity were identified.

- **High**: Example
- **Informational**: Lorem
- **Informational**: Ipsum

#PEN20220001: XXE in Test Shop

Asset	CWE	Severity (CVSS v3.0 Base Score)	CVSS v3.0 Vektor
Test Shop	CWE-611	Critical (9.1)	*CVSS:3.0/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

#PEN20220002: XSS in Test Shop

Asset	CWE	Severity (CVSS v3.0 Base Score)	CVSS v3.0 Vektor
Test Shop	CWE-79	High (7.1)	*CVSS:3.0/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.

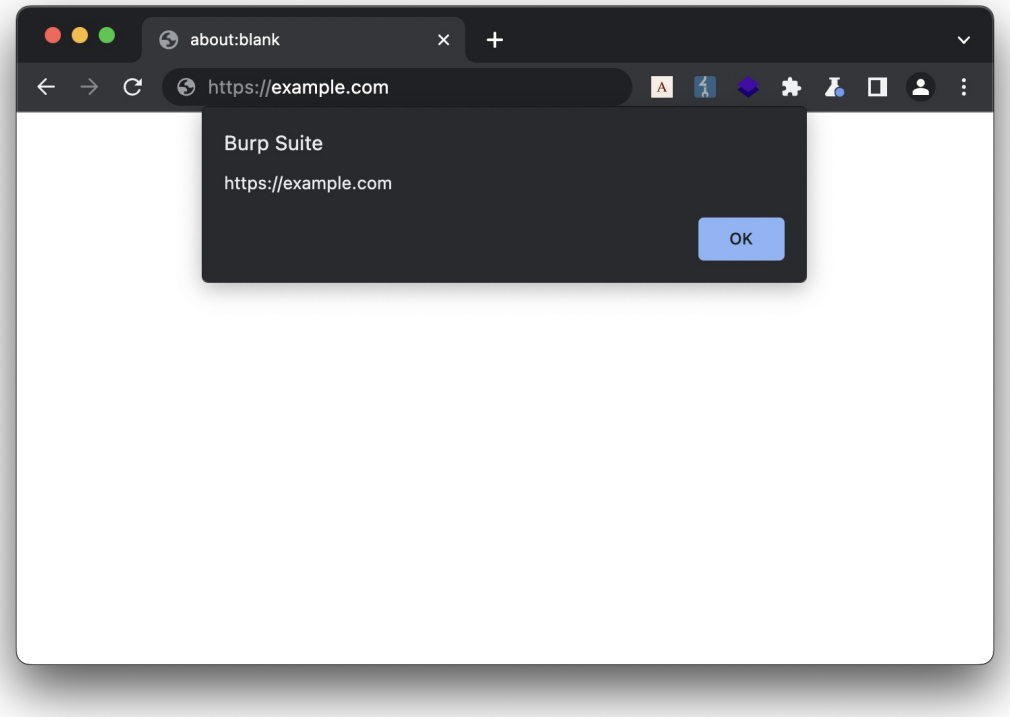
This type of vulnerability arises, if an application uses user-controlled inputs to generate dynamic outputs in an insecure manner.

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)

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