

PENETRATION TEST REPORT

Example, Inc.

Example Pentest

yyyy-mm-dd (1.0)

This report is for the sole information and use of Example, Inc.

Secure By Default, Inc.

+0 123 456 789

contact@sbd.local

<https://sbd.local/>

Executive Summary

Example, Inc. (i.e. the customer) engaged Secure By Default, Inc. to conduct a penetration test on their systems. In accordance with the customer the following types of penetration tests have been conducted:

- pentest against web applications
- pentest against IP hosts

The following vulnerability classes have been found:

Class	Issues
Class A	
Class B	
Total	3

Vulnerabilities with severity scores between 6.0 and 9.8 (both out of 10) have been found. A detailed list thereof, including descriptions on how they were found, and recommendations for mitigations, can be found in Section 2.

Quisque ut finibus mauris. Etiam mattis nisl nulla, eu iaculis urna tincidunt vitae. Etiam pel-lentesque metus vel luctus malesuada. Phasellus auctor scelerisque nisi sed semper. Aliquam vel molestie nulla, nec lacinia mi. In a feugiat erat, at laoreet lorem.

Nunc sit amet tristique sem. Fusce arcu erat, mollis sit amet velit ac, tincidunt porta lorem. Suspendisse at augue aliquet, sodales tellus et, molestie lorem. Phasellus id pharetra tellus. Phasellus vel condimentum justo. Maecenas sem ligula, tincidunt quis scelerisque quis, ultrices ut quam.

Contents

Executive Summary **2**

1 Introduction **4**

1.1 Personnel 4

1.2 Scope 4

1.3 Methodology 4

1.4 Required Information 4

1.5 Limitations 4

1.6 Tools 5

2 Results **6**

2.1 Lorem Ipsum Dolor sit Amet 7

2.1.1 Evidence 7

2.1.2 Affected Assets 7

2.1.3 Severity 7

2.1.4 Recommendations 8

2.1.5 References 8

2.2 Aenean Gravida Pulvinar Lacus 10

2.2.1 Evidence 10

2.2.2 Affected Assets 10

2.2.3 Severity 10

2.2.4 Recommendations 10

2.2.5 References 10

2.3 [EXAMPLE] Lorem Ipsum Dolor sit Amet 11

2.3.1 Evidence 11

2.3.2 Affected Assets 11

2.3.3 Severity 11

2.3.4 Recommendations 12

2.3.5 References 12

1 Introduction

Example, Inc. (i.e. the customer) engaged Secure By Default, Inc. to conduct a penetration test on their systems. In accordance with the customer the following types of penetration tests have been conducted:

- pentest against web applications
- pentest against IP hosts

1.1 Personnel

The following people were part of this penetration test:

- Customer (customer@example.com)
- Software Engineer (se@example.com)
- Project Lead (lead@sbd.local)
- Pentester (hacker@sbd.local)

1.2 Scope

Between yyyy-mm-dd and yyyy-mm-dd the following components have been analyzed:

- `example.com` (application server)
- `https://example.com/` (web application)

All test-related IP traffic originates from the following addresses:

- 11.22.33.44/24

1.3 Methodology

Ex cumque unde ipsum molestias. Perferendis aut veritatis quas cum fugiat ea. Eligendi consequatur cupiditate excepturi. Aliquam blanditiis non nihil hic exercitationem unde.

Optio magni quasi nulla nobis adipisci. Consequuntur placeat omnis impedit dolorum id. Eum assumenda nam in earum ea. Ipsa aliquam facilis cupiditate eos. Nam est neque ipsam quis voluptatum.

Adipisci quo architecto ex fugit dolorem. Inventore soluta perspiciatis minus dolores dolore ipsam iste tempora. Vel et sunt suscipit praesentium vitae voluptatem sequi inventore.

1.4 Required Information

Secure By Default has asked for the following information to be provided:

- access to the web application: fulfilled
- credentials for the web application: fulfilled

1.5 Limitations

During the engagement the following limitations were detected. Secure By Default recommends to re-test the affected components once all limitations have been resolved.

Dapibus

In dapibus est nec elit fermentum, et lacinia ipsum auctor. Praesent rhoncus, metus a tempor ultricies, ex ligula consequat elit, non sollicitudin massa libero vel odio. Duis blandit cursus metus. Quisque ac tincidunt lorem. Cras laoreet urna sed mi sagittis, et sagittis enim mattis. Praesent

porttitor, dolor sagittis egestas hendrerit, ex neque sagittis sapien, vel tincidunt dui libero et sem. Fusce a odio faucibus, finibus augue non, aliquam augue.

Convallis

Nulla vitae nunc at magna molestie sodales convallis non libero. Pellentesque nec lectus lacinia, ultricies nulla in, laoreet lectus. Mauris eget urna efficitur, hendrerit diam eu, gravida mi. Phasellus porta lacinia ligula, ut dictum mi viverra at. Nullam dictum eros vitae massa ultrices, ac iaculis ante rhoncus. Donec pellentesque nec est sed porta.

1.6 Tools

The following tools have been used during the engagement:

- Nmap: network scanner
- cURL: command-line tool for transferring data using various network protocols
- SSLyze: TLS scanning tool
- Nessus: vulnerability scanner
- Burp Suite: web application security scanner
- Git: collaboration tool
- \LaTeX : document preparation

2 Results

Vulnerability	Severity
Lorem Ipsum Dolor sit Amet	<div><div></div></div> 9.8 (critical)
Aenean Gravida Pulvinar Lacus	<div><div></div></div> 6.0 (medium)

Table 1: Issues of component “EXAMPLE”.

Vulnerability	Severity
[EXAMPLE] Lorem Ipsum Dolor sit Amet	<div><div></div></div> 6.5 (medium)

2.1 Lorem Ipsum Dolor sit Amet

Repellat corporis aut odio veniam non autem vel. Repudiandae rerum et unde. Accusamus quae et repellat. Quod deserunt facilis voluptate dignissimos quidem ut iste. Accusantium sed et maiores deleniti. Officia eaque ad est amet.

Blanditiis

Blanditiis reprehenderit aspernatur aliquam qui. Ut quisquam et a cupiditate. Eum quaerat adipisci in cum esse reiciendis laborum.

Possimus facilis aliquid consequatur consequuntur quos perferendis quia. Magni eveniet quas omnis culpa assumenda doloribus voluptas. Vero repellat sed vero facere error ducimus et.

Laudantium

Qui quia et aut officiis laudantium possimus possimus. Alias velit cumque sit. Et hic ipsum dolores et porro voluptatem. Non sunt quaerat sit cum error dolorem sapiente.

Omnis

Dolorem omnis unde itaque sit architecto autem sequi. Ut nemo ratione fugiat. Veniam incidunt voluptatum cumque aut. Rerum est odio cupiditate id esse sed rerum.

2.1.1 Evidence

2.1.1.1 vulnerable.example.com

Repellat corporis aut odio veniam non autem vel. Repudiandae rerum et unde. Accusamus quae et repellat. Quod deserunt facilis voluptate dignissimos quidem ut iste.

```
$ curl -iks https://vulnerable.example.com/ | grep -i 'server:'  
Server: Apache 2.14
```

Ut quisquam et a cupiditate (see Figure 1).

Severity: critical

2.1.1.2 POST api.example.com/v2/resource

Possimus facilis aliquid consequatur consequuntur quos perferendis quia. Magni eveniet quas omnis culpa assumenda doloribus voluptas. Vero repellat sed vero facere error ducimus et.

Severity: low

2.1.2 Affected Assets

- vulnerable.example.com
- api.example.com

2.1.3 Severity



Attack Vector

<input type="checkbox"/> Network	<input type="checkbox"/> Adjacent	<input type="checkbox"/> Local	<input type="checkbox"/> Physical
----------------------------------	-----------------------------------	--------------------------------	-----------------------------------

Scope

<input type="checkbox"/> Unchanged	<input type="checkbox"/> Changed
------------------------------------	----------------------------------

Attack Complexity

<input type="checkbox"/> Low	<input type="checkbox"/> High
------------------------------	-------------------------------

Confidentiality

<input type="checkbox"/> None	<input type="checkbox"/> Low	<input type="checkbox"/> High
-------------------------------	------------------------------	-------------------------------

Privileges Required

<input type="checkbox"/> None	<input type="checkbox"/> Low	<input type="checkbox"/> High
-------------------------------	------------------------------	-------------------------------

Integrity

<input type="checkbox"/> None	<input type="checkbox"/> Low	<input type="checkbox"/> High
-------------------------------	------------------------------	-------------------------------

User Interaction

<input type="checkbox"/> None	<input type="checkbox"/> Required
-------------------------------	-----------------------------------

Availability

<input type="checkbox"/> None	<input type="checkbox"/> Low	<input type="checkbox"/> High
-------------------------------	------------------------------	-------------------------------

2.1.4 Recommendations

- Alias velit cumque sit.
- Ut quisquam et a cupiditate.
- Ut nemo ratione fugiat.

2.1.5 References

- Reference A
- Reference B
- Reference C



Figure 1: Vero repellat sed vero facere error ducimus et.

2.2 Aenean Gravida Pulvinar Lacus

Nullam gravida urna eget massa sagittis sodales. Aenean venenatis convallis diam. Nulla eu nulla eget ligula bibendum placerat in vel nisi. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

Curibatur

Curabitur quis lectus nisi. Duis eu auctor nulla. Etiam non velit quam. Nunc et lectus sagittis, mattis ligula ut, sodales lectus. Fusce dignissim nisi non dolor suscipit mattis. Quisque hendrerit egestas quam.

Rhoncus

Aenean rhoncus rhoncus elit. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer ac massa non sapien congue hendrerit vel ac augue. Pellentesque eros mi, sagittis in metus vestibulum, pretium iaculis est. Ut euismod tortor in quam iaculis tempus. Vestibulum sed consequat sem.

2.2.1 Evidence

2.2.1.1 GET api.example.com/v2/resource

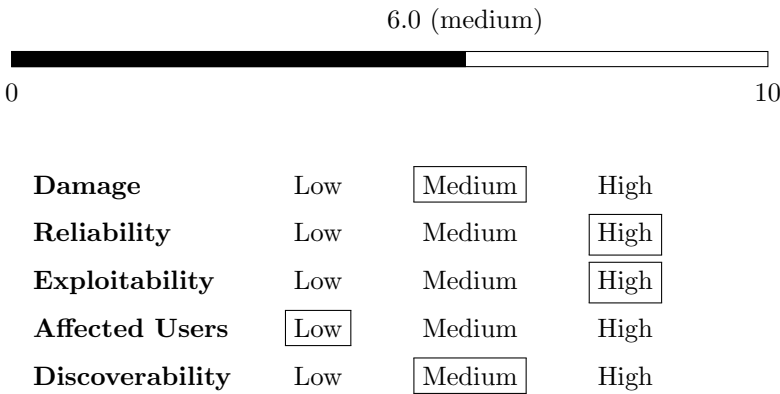
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer ac massa non sapien congue hendrerit vel ac augue. Pellentesque eros mi, sagittis in metus vestibulum, pretium iaculis est.

Severity: medium

2.2.2 Affected Assets

- api.example.com

2.2.3 Severity



2.2.4 Recommendations

- Mauris at nisi finibus velit.
- Sed ut ligula hendrerit orci elementum luctus.
- Fusce dignissim nisi non dolor suscipit mattis.

2.2.5 References

- Example Reference
- Another Reference

2.3 [EXAMPLE] Lorem Ipsum Dolor sit Amet

Repellat corporis aut odio veniam non autem vel. Repudiandae rerum et unde. Accusamus quae et repellat. Quod deserunt facilis voluptate dignissimos quidem ut iste. Accusantium sed et maiores deleniti. Officia eaque ad est amet.

Blanditiis

Blanditiis reprehenderit aspernatur aliquam qui. Ut quisquam et a cupiditate. Eum quaerat adipisci in cum esse reiciendis laborum.

Possimus facilis aliquid consequatur consequuntur quos perferendis quia. Magni eveniet quas omnis culpa assumenda doloribus voluptas. Vero repellat sed vero facere error ducimus et.

Laudantium

Qui quia et aut officiis laudantium possimus possimus. Alias velit cumque sit. Et hic ipsum dolores et porro voluptatem. Non sunt quaerat sit cum error dolorem sapiente.

Omnis

Dolorem omnis unde itaque sit architecto autem sequi. Ut nemo ratione fugiat. Veniam incidunt voluptatum cumque aut. Rerum est odio cupiditate id esse sed rerum.

2.3.1 Evidence

2.3.1.1 vulnerable.example.com

Repellat corporis aut odio veniam non autem vel. Repudiandae rerum et unde. Accusamus quae et repellat. Quod deserunt facilis voluptate dignissimos quidem ut iste.

```
$ curl -iks https://vulnerable.example.com/ | grep -i 'server:'
Server: Apache 2.14
```

Ut quisquam et a cupiditate (see Figure 2).

Severity: critical

2.3.1.2 POST api.example.com/v2/resource

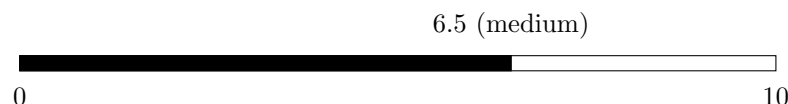
Possimus facilis aliquid consequatur consequuntur quos perferendis quia. Magni eveniet quas omnis culpa assumenda doloribus voluptas. Vero repellat sed vero facere error ducimus et.

Severity: low

2.3.2 Affected Assets

- vulnerable.example.com
- api.example.com

2.3.3 Severity



Attack Vector

 Adjacent Local Physical

Attack Complexity

 High

Privileges Required

 Low High

User Interaction

 Required

Scope

 Changed

Confidentiality

None High

Integrity

None High

Availability

 Low High

2.3.4 Recommendations

- Alias velit cumque sit.
- Ut quisquam et a cupiditate.
- Ut nemo ratione fugiat.

2.3.5 References

- Reference A
- Reference B
- Reference C



Figure 2: Vero repellat sed vero facere error ducimus et.