Disclosure of Valid Usernames

Ibexa eZ Platform Enterprise 2.5

Classification: **Confidential**
Version: 1.0
Last Change: 12/07/21

it.sec GmbH
Einsteinstr. 55
89077 Ulm
Tel: +49 731/20589-0
Fax: +49 731/20589-29
www.it-sec.de
research@it-sec.de

Table of Contents

1 Summary

Based on the different response times of the web server, valid user names could be identified.

This could be used to generate a list of valid user accounts, which serves as a basis for further attacks on users.

2 Disclosure of Valid Usernames

2.1 Vulnerability Scoring

Vulnerability Class

Exposure of Sensitive Information to an Unauthorized Actor

CVSS 2

Score: 5.0 (Medium)

Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS 3

Score: 5.3 (Medium)

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

2.2 Description

During the penetration test, it was possible to determine whether a correct user name was entered based on the amount of time it took the server to respond to the request.

If a correct username but an incorrect password was entered during login, the server needed approx. 180 milliseconds for a response, as seen in the following figure:

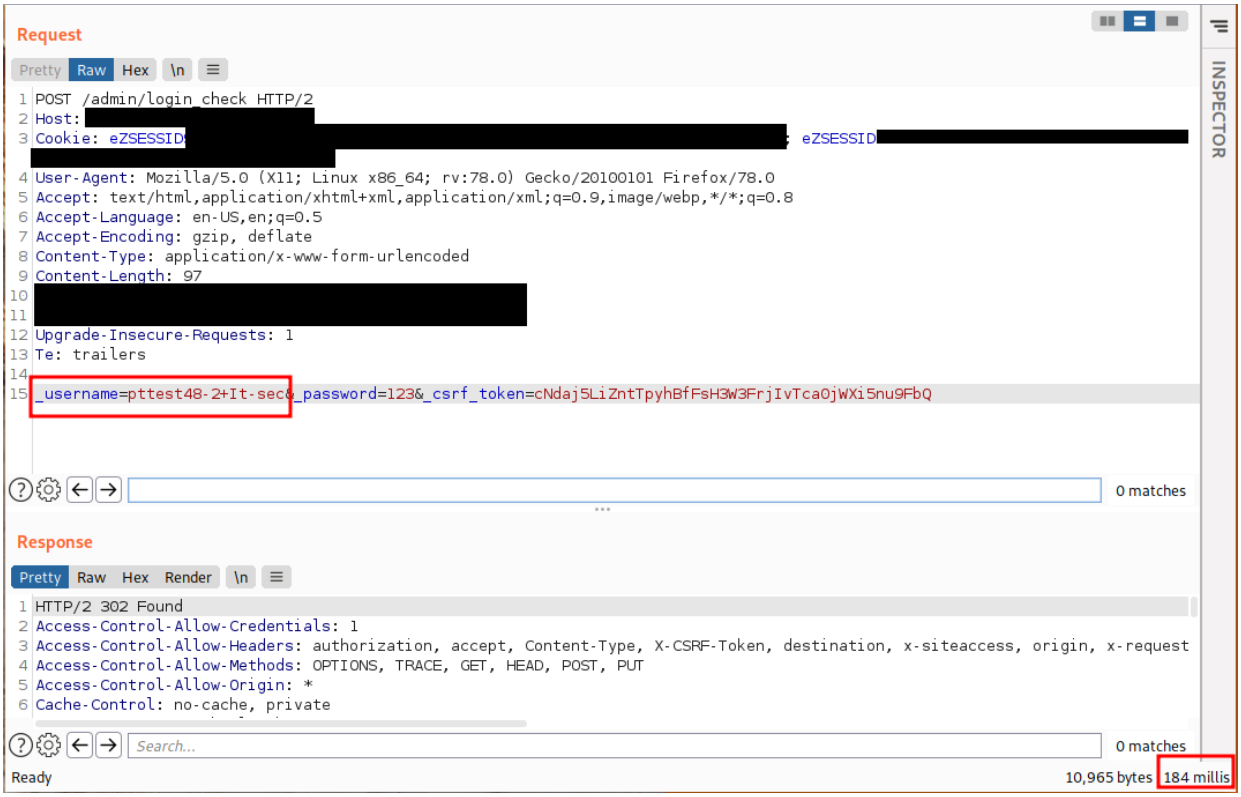


Figure 1: Response time for valid username

If an obviously invalid username was entered, the server response time was much faster.

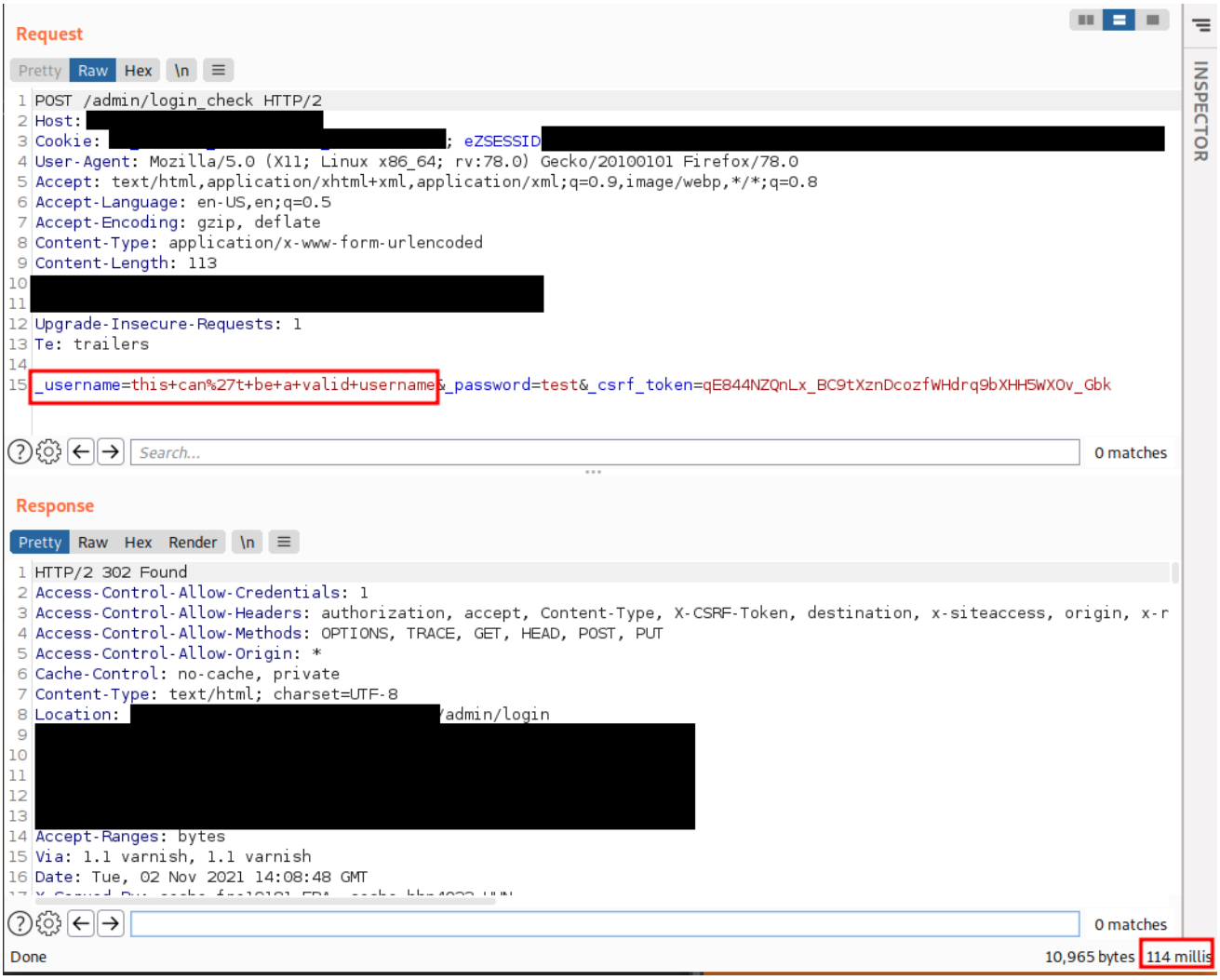


Figure 2: Response time for invalid username

Based on this time difference, valid user names could thus be enumerated.

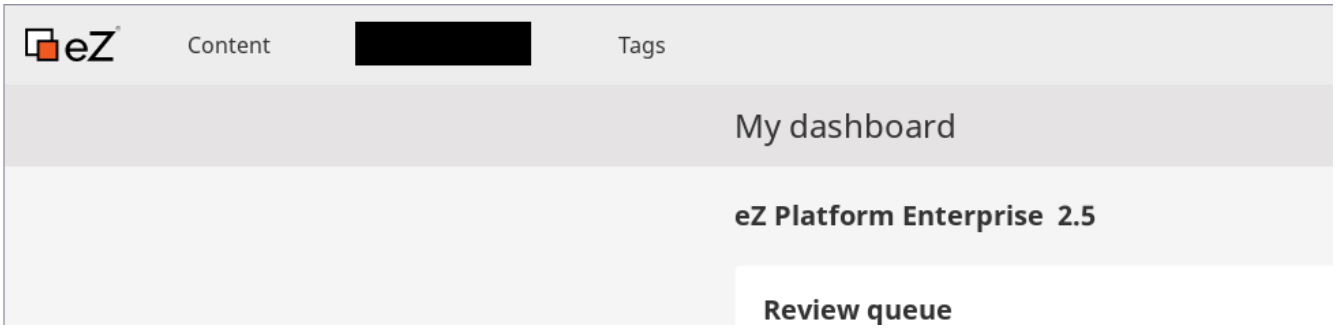
2.3 Recommended Countermeasures

In order to prevent the previously mentioned vulnerability, the following countermeasures are recommended:

- The response time should be independent of the input of a valid or invalid user name.
- The behavior of the application should not allow any conclusions to be drawn about the existence of valid user accounts.

2.4 Affected Systems

This vulnerability was identified in the login page of the eZ Platform Enterprise 2.5.



3 Contact it.sec GmbH

Christoph Rottermanner

IT-Security Consultant

OSCP, OSWE

Information Security / Penetration Tests / Data Protection / IT Forensics

it.sec GmbH

Zweigniederlassung Österreich

Gußhausstr. 22/4

1040 Wien

T: +43 1 37 50 247-23

F: +43 1 37 50 247-29

M: +43 660 135 333 4

crottermanner@it-sec.de

www.it-sec.de