TYPO3 v7.6.15 Unencrypted Login Request Assigned CVE Number: CVE-2017-6370

Proof-of-Concept

Submitted by:
Author: Faiz Ahmed Zaidi
Organization: Provensec LLC
Website: http://provensec.com/

National Vulnerability Database

(https://nvd.nist.gov/cvss/v2-calculator)

Overall CVSS Score: 4

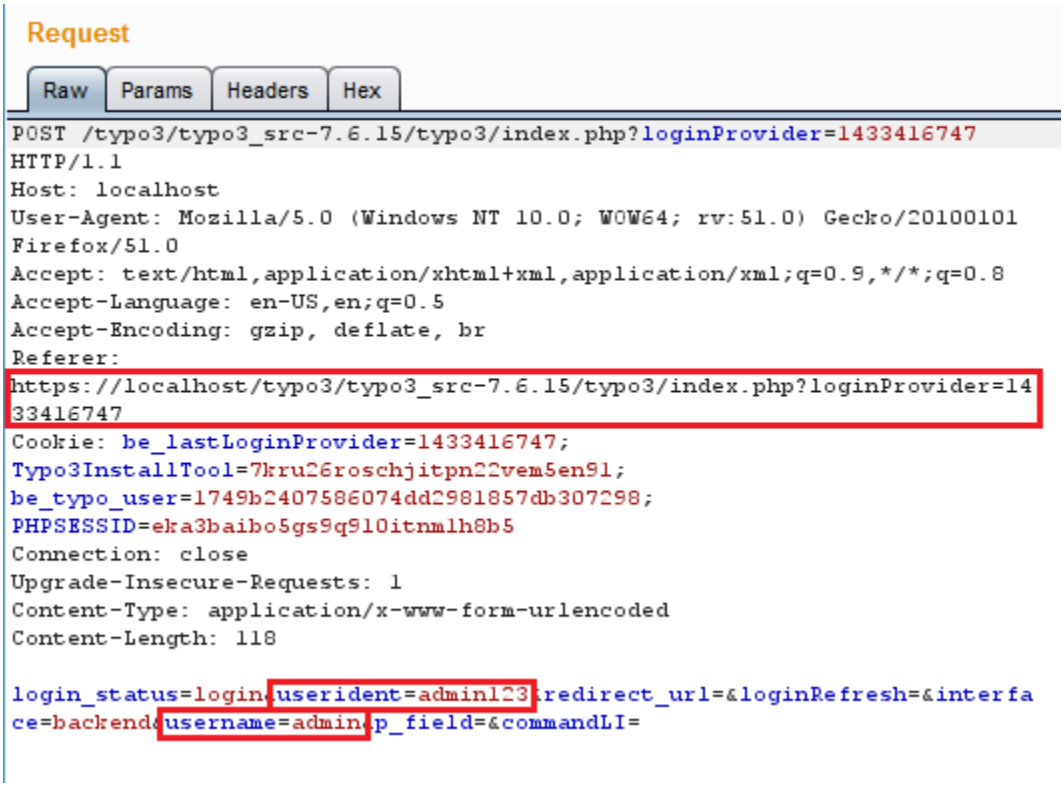
CVSS v2 Vector (AV:L/AC:L/Au:N/C:P/I:P/A:P/E:ND/RL:OF/RC:C)

Proof-of-Concept

I would like to report a vulnerability that I have found today in which the login credentials are sent in Cleartext/ Unencrypted (Tested Using Typo3 Login Module). As the login credentials are sent in clear-text it is easy for an attacker to view the unencrypted credentials and take over the account of the Admin or User.

Hereby I am adding the information related to my finding so that you can have a brief view.

Technical Description: During the application test, it was detected that an unencrypted login request was sent to the server. Since some of the input fields used in a login process (for example: usernames, passwords, e-mail addresses, social security number, etc.) are personal and sensitive. Any information sent to the server as clear text may be stolen and used later for identity theft or user impersonation.



Vulnerability Type:
Unencrypted Login Request

Vendor of Product:
Typo3 Org

Affected Product Code Base:
Typo3 cms - typo3_src-7.6.15

Affected Component:
login_status=login&p_field=&username=admin&useridentt=admin123

Attack Type:
Local

Attack Vectors:
Attacker can use any intercept proxy to capture packets. The attacker is able to view information (admin level user name & password) in clear text from the capture raw packets.

Reference:
https://www.owasp.org/index.php/Testing_for_Sensitive_information_sent_via_unencrypted_channels_(OTG-CRYPST-003)
