Flags and Passwords to the QCTF

|  |  |  |
| --- | --- | --- |
| Nr | Vlag | Punten |
| 1 | $**manireallyhackedmysqlanditfeltgood$** | 10 |
| 2 | $**whatevenisrobots.txt$** | 5 |
| 3 | $**jerrywhyisthisfilehere$** | 5 |
| 4 | **$hahaimhidinginthesourcecode$** | 3 |
| 5 | **$thatssomeadvancedexploitation$** | 10 |
| 6 | **$edgecasehell$** | 2 |
| 7 | **$updatemybadpassword$** | 20 |
| 8 | **$tryandgetmewithxss$** | 10 |
| 9 | **$iknowmyfundamentals$** | 5 |
| 10 | **$networkingiseasy$** | 5 |
| 11 | **$networkdiagnosisismine$** | 5 |
| 12 | **$mysecurityisimpeccable$** | 5 |
| 13 | **$ihaveofficiallycompletedallquizzes$** | 5 |
| 14 | **$networksbetterwatchout$** | 10 |
| 15 | **$imhidingintheconsole$** | 3 |
| 16 | **$imhidinginthejavascriptvariables** | 3 |

[Passwords](#_30lqqm4560vz)

[Unix users](#_5wxy493pimxx)

[MySQL](#_g1mn2fgmh4wc)

[Flags](#_yb8witt7abji)

[SQL](#_w2qxgm6wkt8v)

[Smart Searching](#_sxd2kvwzr3lk)

[Robots.txt](#_8du8vpqoaiye)

[/flag](#_7otit0hdod1u)

[Source to /](#_455tqx17nbx7)

[/config (without .php ← Source code)](#_5wh78khw50ce)

[fs:/home/jerry/flag.txt](#_udj99395rkhu)

[Specials](#_sfw6tl120bel)

[PHP files](#_524zhpton092)

[Cats.php](#_j7qn8c4xrylp)

[Dogs.php](#_q8s1p05bj4ah)

# Passwords

## Unix users

User: jerry

Pass: password123

User: john

Pass: ilikeducks

## MySQL

User: john

Pass: ilovemysql

User: admin

Pass: Dz$QR4A7#He42aK&3Nw7

# Flags

## SQL (10 pts)

Visit webpage on index.html. Enter %'; SELECT \* FROM flags; should yield the flag: 1. $**manireallyhackedmysqlanditfeltgood$**

## Smart Searching

### Robots.txt (5 pts)

2. Argument *Flag:* yields the flag: $**whatevenisrobots.txt$**

### /flag (5 pts)

3. Yields flag: $**jerrywhyisthisfilehere$**

### Source to /search/index.php (3 pts)

4. Yields flag: **$hahaimhidinginthesourcecode$**

### /config (without .php ← Source code) (10 pts)

5. Yields flag: **$thatssomeadvancedexploitation$**

### / (source code) (2 pts)

6. Yields flag: **$edgecasehell$**

### fs:/home/jerry/flag.txt (20 pts)

7. Yields flag: **$updatemybadpassword$**

## XSS (10 pts)

### /blog

Wanneer een user <script></script> in de message heeft, of onload=, krijgt de user een alert 8. met een flag: **$tryandgetmewithxss$**

# Quiz (5 pts each)

## Fundamentals

9. Completing quiz: **$iknowmyfundamentals$**

## Networking

10. Completing quiz: **$networkingiseasy$**

## OSI Model

11. Completing quiz: **$networkdiagnosisismine$**

## Security Goals

12. Completing quiz: **$mysecurityisimpeccable$**

## Bonus for completing all quizzes:

13. Flag: **$ihaveofficiallycompletedallquizzes$**

# Sniffing (10 pts)

14. Finding flag in pcap yields: **$networksbetterwatchout$**

# Specials

## PHP files

### Cats.php

This is a PHP shell executor. It does not show stderr, nor does it allow the use of cat.

### Dogs.php

This is a PHP Local File Inclusion tool. It replaces the cat function in the cats.php listed above. NOTE: THIS INCLUDES FILES INSTEAD OF DISPLAYING THEM. PHP CODE EXECUTION CAN HAPPEN HERE, NEVER UNDER ANY CIRCUMSTANCE INCLUDE Dogs.php!