xxsj_web17

> **Note**
>
> `GZCTF-challenges/xxsj_web17`

使用 `dirsearch` 扫描

```
┌──(kali㉿kali)-[~/Desktop/tool/dirsearch][16:28:35]
└─$ python dirsearch.py -u http://IP:PORT/

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 | Wordlist size: 12293

Target: http://IP:PORT/

[16:28:55] Scanning:
[16:29:14] 200 -   593B - /backup.sql
[16:29:24] 301 -   322B - /images  ->  http://IP:PORT/images/
[16:29:24] 200 -    1KB - /images/
[16:29:24] 200 -    1KB - /index.php
[16:29:24] 200 -    1KB - /index.php/login/
[16:29:35] 403 -   280B - /server-status
[16:29:35] 403 -   280B - /server-status/

Task Completed
```

访问 `URL/backup.sql` 自动下载 `backup.sql`

在其中得到 `FLAG`

```
CREATE TABLE IF NOT EXISTS `products` (
  `product_id` INTEGER NOT NULL,
  `name` TEXT(100) NOT NULL,
  `sku` TEXT(14) NOT NULL,
  `price` REAL NOT NULL,
```

```
  `image` TEXT(50) NOT NULL,
  PRIMARY KEY (`product_id`),
  UNIQUE (`sku`)
);

CREATE TABLE IF NOT EXISTS `flag` (
  `secret` TEXT(255)
);

INSERT INTO `flag` (`secret`) VALUES ('flag{GZCTF_dynamic_flag_test}');

INSERT INTO `products` (`product_id`, `name`, `sku`, `price`, `image`)
VALUES
(1, 'Miku', 'VC001', 158.00, 'images/0831.jpg'),
(2, 'Teto', 'VC002', 159.50, 'images/0401.jpg'),
(3, 'Akita', 'VC003', 150.00, 'images/1101.jpg');
```