# Vulnerability Assessment Report

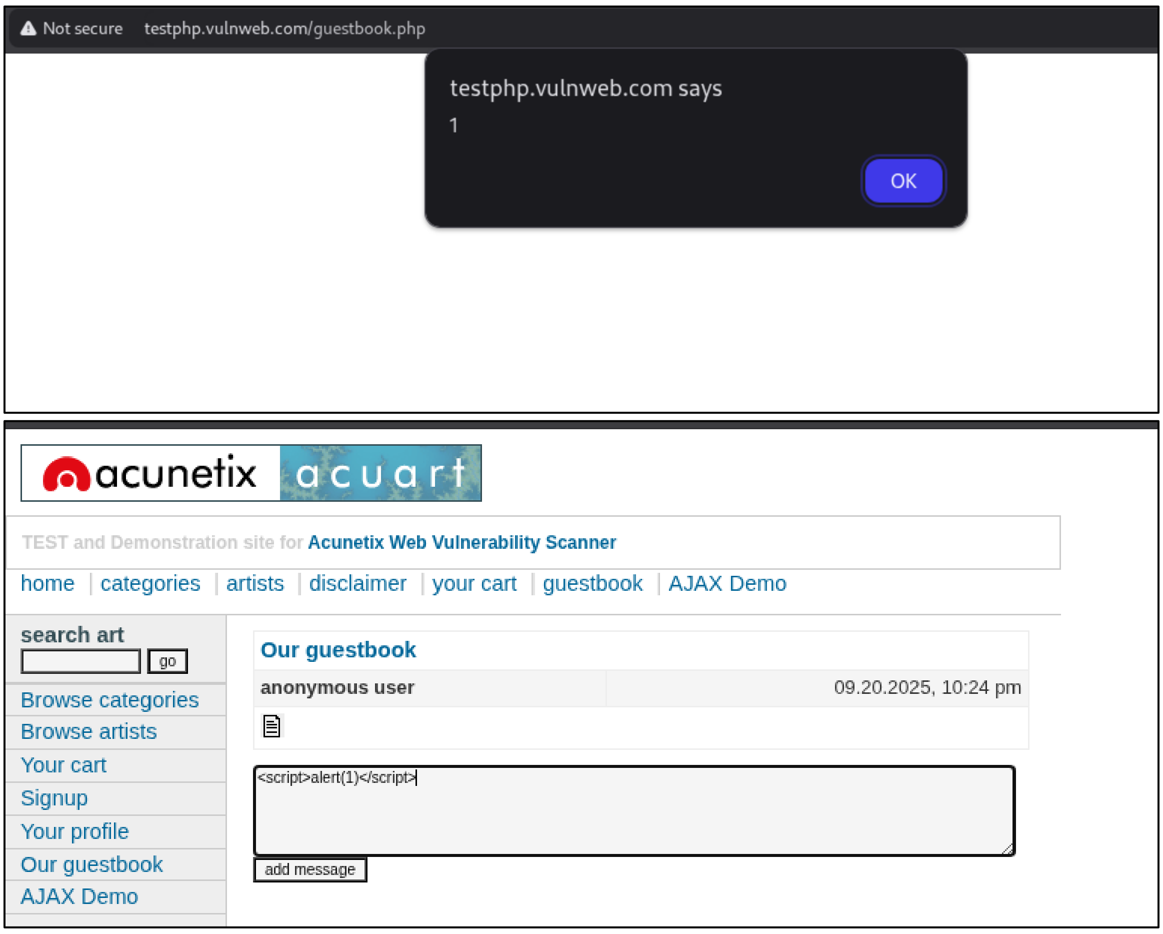
**Target:** testphp.vulnweb.com
author : Mohmmad AL ahmad

The findings of a web application vulnerability assessment conducted on testphp.vulnweb.com are documented in this report.

Finding common vulnerabilities (such as SQL Injection, XSS, and Hidden Directories) and offering suggestions to strengthen security were the goals.

| No. | URL | Vulnerability | Payload Used | Result | severity | rec |
|---|---|---|---|---|---|---|
| 1 | Testphp.vulneb.com/guestbook.php | Reflected XSS | <script> alert(1) <script> | Alert box excuted | medium | Sanitize input, encode output. |
| 2 | Testphp.vulneb.com/login.php | SQL injection | 1' OR 1=1# | Logged in to the account without a password | High | Use prepared statements, validate input. |
| 3 | Testphp.vulneb.com | Hidden links | Used Buster Tools | Found many hidden links and database name | High | Secure hidden directories with authentication. |

1



Not secure testphp.vulnweb.com/guestbook.php

testphp.vulnweb.com says

1

OK

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

**search art** go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

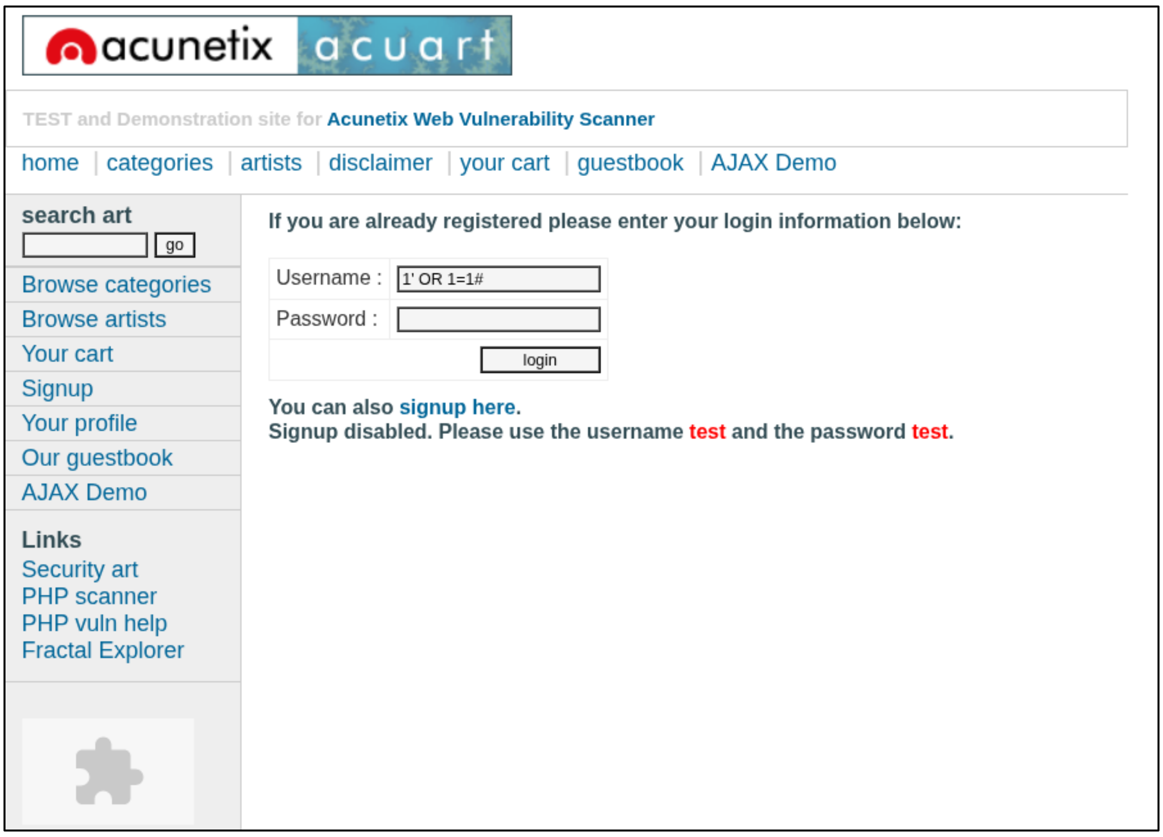
**Our guestbook**

| **anonymous user** | 09.20.2025, 10:24 pm |
|---|---|

```
<script>alert(1)</script>
```

add message

2:



acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

**search art** go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

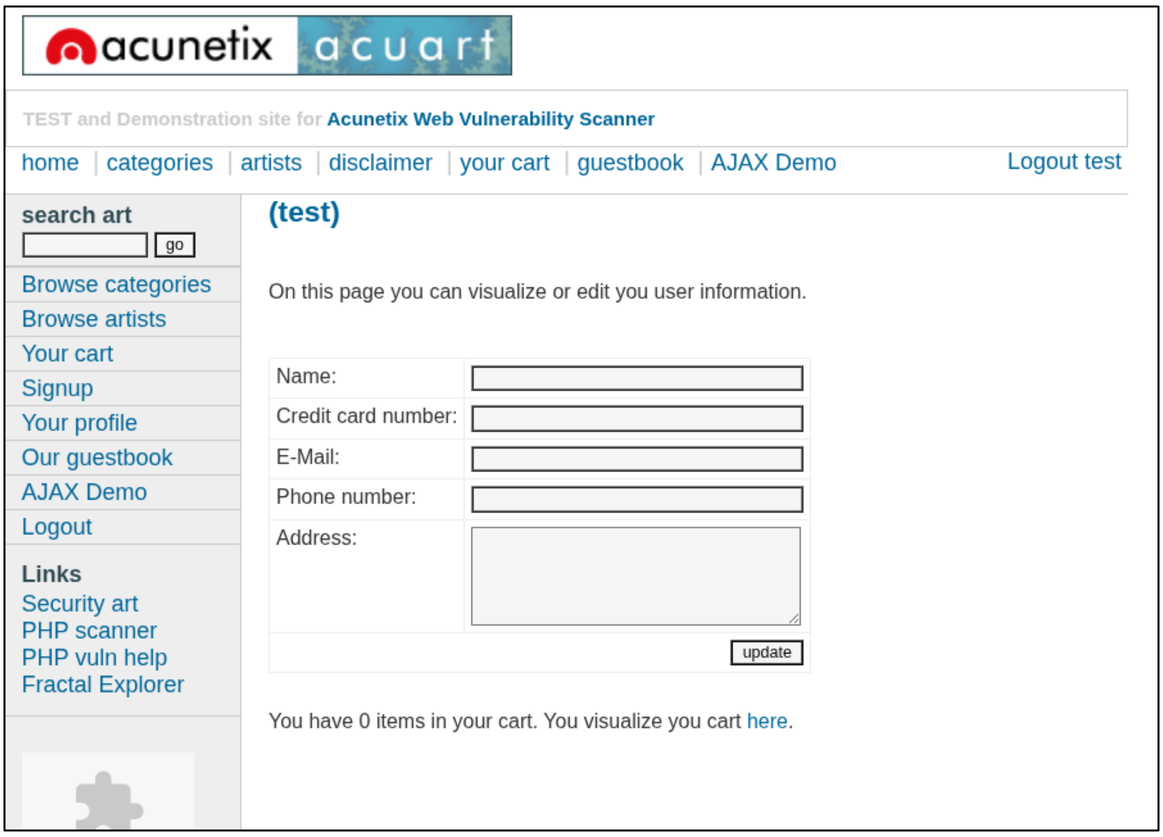
**Links**
Security art
PHP scanner
PHP vuln help
Fractal Explorer

**If you are already registered please enter your login information below:**

| | |
|---|---|
| Username : | 1' OR 1=1# |
| Password : | |

login

**You can also signup here.**
**Signup disabled. Please use the username test and the password test.**


acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo    Logout test

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

**Links**
Security art
PHP scanner
PHP vuln help
Fractal Explorer

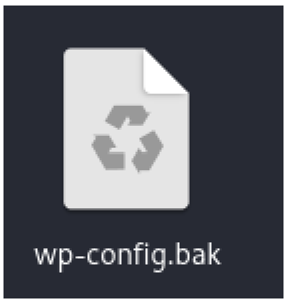
**(test)**

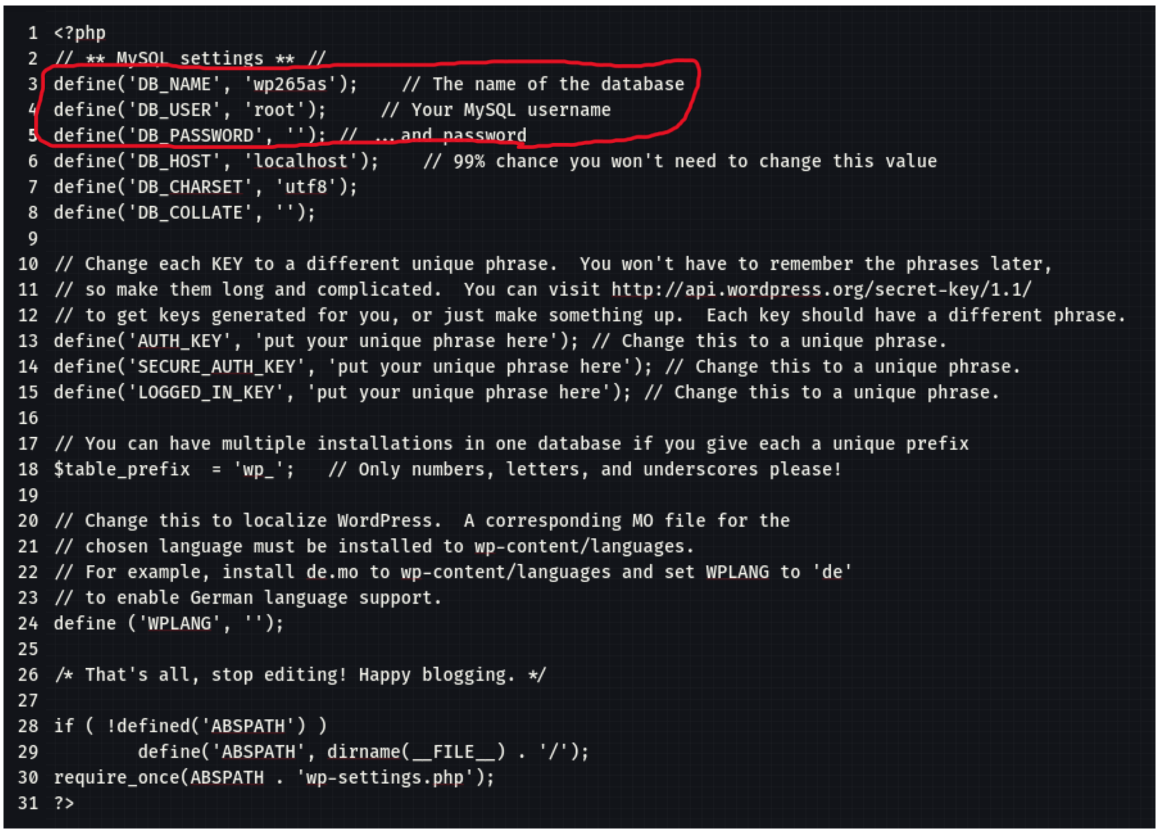
On this page you can visualize or edit you user information.

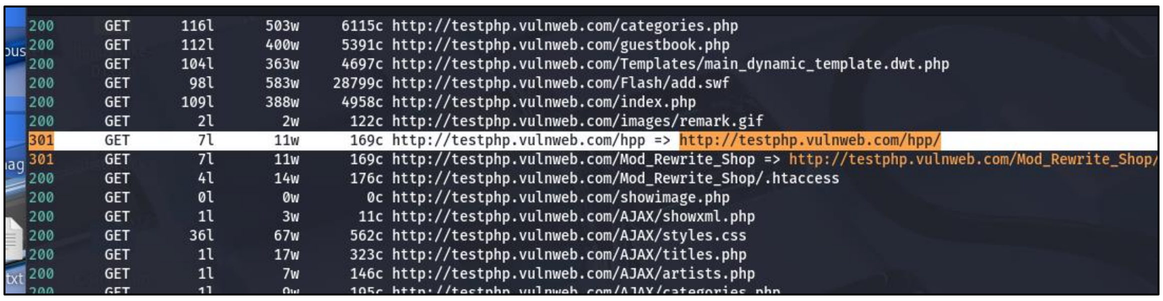
| | |
|---|---|
| Name: | |
| Credit card number: | |
| E-Mail: | |
| Phone number: | |
| Address: | |
| | update |

You have 0 items in your cart. You visualize you cart here.

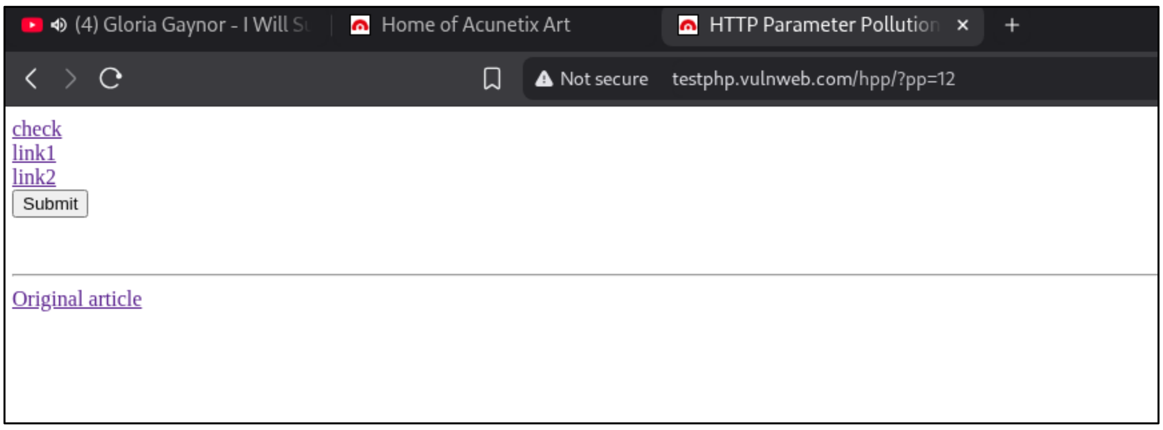
3:


wp-config.bak


```php
<?php
// ** MySQL settings ** //
define('DB_NAME', 'wp265as');    // The name of the database
define('DB_USER', 'root');     // Your MySQL username
define('DB_PASSWORD', ''); // ...and password
define('DB_HOST', 'localhost');    // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase.  You won't have to remember the phrases later,
// so make them long and complicated.  You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up.  Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix  = 'wp_';   // Only numbers, letters, and underscores please!

// Change this to localize WordPress.  A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
        define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');
?>
```

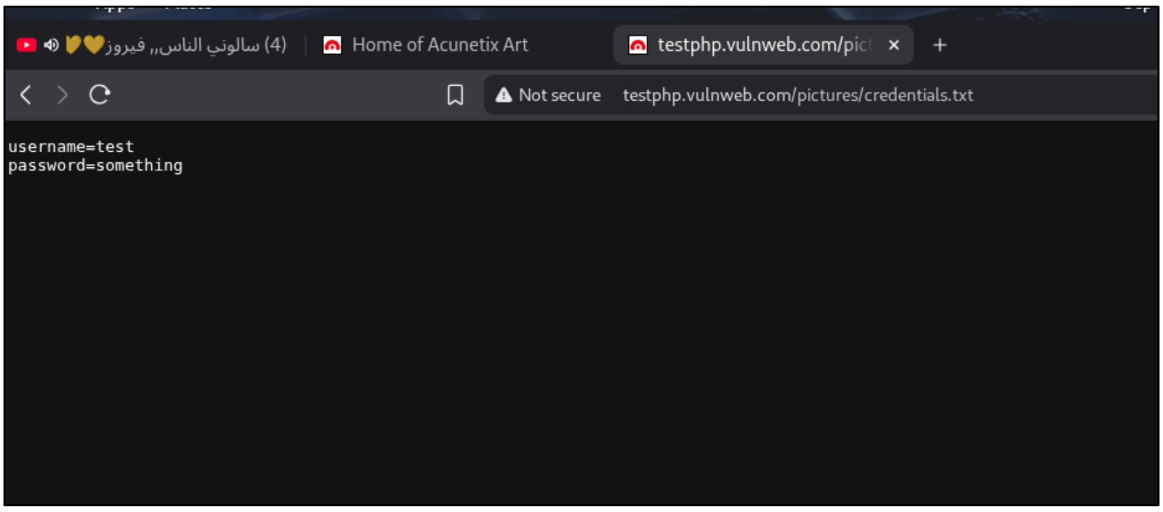


```
200      GET      116l      503w      6115c http://testphp.vulnweb.com/categories.php
200      GET      112l      400w      5391c http://testphp.vulnweb.com/guestbook.php
200      GET      104l      363w      4697c http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
200      GET       98l      583w     28799c http://testphp.vulnweb.com/Flash/add.swf
200      GET      109l      388w      4958c http://testphp.vulnweb.com/index.php
200      GET        2l        2w       122c http://testphp.vulnweb.com/images/remark.gif
301      GET        7l       11w       169c http://testphp.vulnweb.com/hpp => http://testphp.vulnweb.com/hpp/
301      GET        7l       11w       169c http://testphp.vulnweb.com/Mod_Rewrite_Shop => http://testphp.vulnweb.com/Mod_Rewrite_Shop/
200      GET        4l       14w       176c http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
200      GET        0l        0w         0c http://testphp.vulnweb.com/showimage.php
200      GET        1l        3w        11c http://testphp.vulnweb.com/AJAX/showxml.php
200      GET       36l       67w       562c http://testphp.vulnweb.com/AJAX/styles.css
200      GET        1l       17w       323c http://testphp.vulnweb.com/AJAX/titles.php
200      GET        1l        7w       146c http://testphp.vulnweb.com/AJAX/artists.php
200      GET        1l        0w       195c http://testphp.vulnweb.com/AJAX/categories.php
```

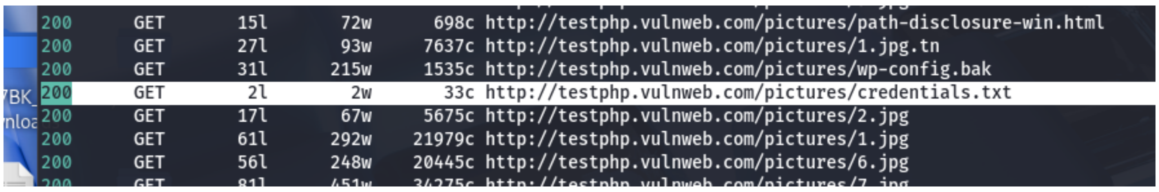


check
link1
link2
Submit

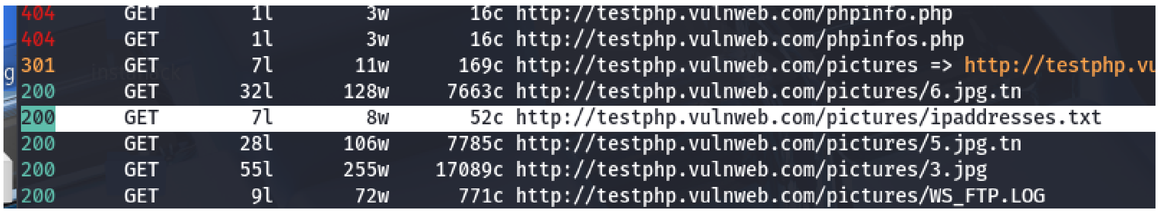
Original article


(4) سالوني الناس,, فيروز 💛💛
Home of Acunetix Art
testphp.vulnweb.com/pict
Not secure
testphp.vulnweb.com/pictures/credentials.txt

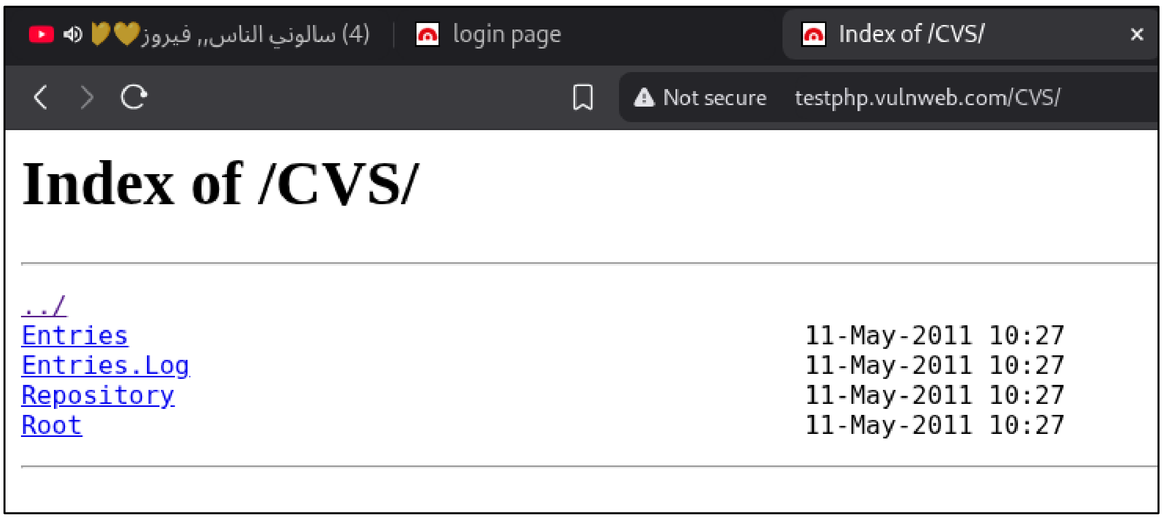
```
username=test
password=something
```



```
200      GET       15l       72w       698c http://testphp.vulnweb.com/pictures/path-disclosure-win.html
200      GET       27l       93w      7637c http://testphp.vulnweb.com/pictures/1.jpg.tn
200      GET       31l      215w      1535c http://testphp.vulnweb.com/pictures/wp-config.bak
200      GET        2l        2w        33c http://testphp.vulnweb.com/pictures/credentials.txt
200      GET       17l       67w      5675c http://testphp.vulnweb.com/pictures/2.jpg
200      GET       61l      292w     21979c http://testphp.vulnweb.com/pictures/1.jpg
200      GET       56l      248w     20445c http://testphp.vulnweb.com/pictures/6.jpg
200      GET       81l      451w     34275c http://testphp.vulnweb.com/pictures/7.jpg
```

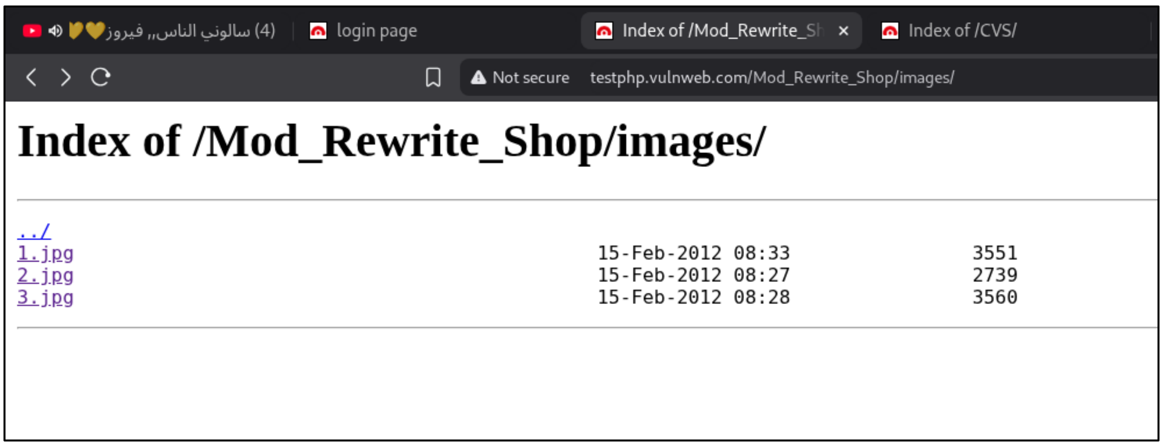


```
404      GET        1l        3w        16c http://testphp.vulnweb.com/phpinfo.php
404      GET        1l        3w        16c http://testphp.vulnweb.com/phpinfos.php
301      GET        7l       11w       169c http://testphp.vulnweb.com/pictures => http://testphp.vu
200      GET       32l      128w      7663c http://testphp.vulnweb.com/pictures/6.jpg.tn
200      GET        7l        8w        52c http://testphp.vulnweb.com/pictures/ipaddresses.txt
200      GET       28l      106w      7785c http://testphp.vulnweb.com/pictures/5.jpg.tn
200      GET       55l      255w     17089c http://testphp.vulnweb.com/pictures/3.jpg
200      GET        9l       72w       771c http://testphp.vulnweb.com/pictures/WS_FTP.LOG
```



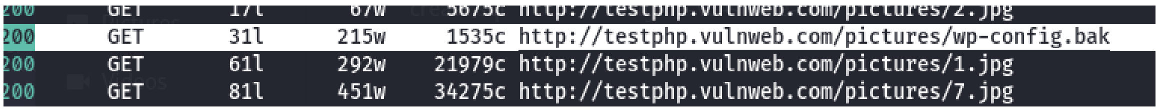
# Index of /CVS/

```
../
Entries                                           11-May-2011 10:27
Entries.Log                                       11-May-2011 10:27
Repository                                        11-May-2011 10:27
Root                                              11-May-2011 10:27
```


(4) سالوني الناس,, فيروز 💛💛
login page
Index of /Mod_Rewrite_Sh
Index of /CVS/
Not secure
testphp.vulnweb.com/Mod_Rewrite_Shop/images/

# Index of /Mod_Rewrite_Shop/images/

```
../
1.jpg                                              15-Feb-2012 08:33                3551
2.jpg                                              15-Feb-2012 08:27                2739
3.jpg                                              15-Feb-2012 08:28                3560
```



```
200      GET      17l      67w     5675c http://testphp.vulnweb.com/pictures/2.jpg
200      GET      31l     215w     1535c http://testphp.vulnweb.com/pictures/wp-config.bak
200      GET      61l     292w    21979c http://testphp.vulnweb.com/pictures/1.jpg
200      GET      81l     451w    34275c http://testphp.vulnweb.com/pictures/7.jpg
```

In conclusion, the assessment of testphp.vulnweb.com has indicated there were several vulnerabilities present. Reflected XSS was indicated on the page /guestbook.php using the payload alert(1), which was able to create an alert box successfully (Medium severity). Sanitising input and encoding output is our recommendation. SQL Injection was also indicated on /ogin.php with the payload 1' OR 1=1#, which allowed login with no password (High severity). Using prepared statements and sanitizing input is our recommendation. Additionally, multiple hidden links throughout the site were also ndicated using directory busting tools, including exposing the name of a database (High severity). Hiding the directories with authentication is our recommendation. Overall, we were able to ermine the site was vulnerable to the execution of scripts, bypassing authentication, and exposure of sensitive information. Implementing our recommendations will greatly increase the security posture of the site.