

ZeroX Analyser Scan Report

File: vulnerable_code\assert.php

Vulnerability: Remote Command Execution

Line: 9

Code Snippet: "strpos('templates/' . \$page . '.php', '..')

File: vulnerable_code\assert.php

Vulnerability: Remote Command Execution

Line: 12

Code Snippet: "file_exists('templates/' . \$page . '.php')

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 3

Code Snippet: define("PASSWORD","pwd123*")

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 8

Code Snippet: \$DB_PASS="password"

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 11

Code Snippet: \$secret_flag="a2"

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 12

Code Snippet: \$token="1213144142353962062"

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 13

Code Snippet: \$pwd="mysuper_cr3dz"

File: vulnerable_code\configuration.php

Vulnerability: Hardcoded Credential

Line: 15

Code Snippet: \$Pass="case!nsenSitiveP@ss"

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 17

Code	Snippet:
\$base64="TXITdXBldBhc3N3b3JkT3lganVzdCBhbm90aGVyIGJhY2tkb29yIGluIHlvdXlY29kZSB5b3Ugd2FudCB0byBiZSBkZXRIY3RIZAo="	

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 18

Code	Snippet:
\$hex="4d79537570657250617373776f72644f72206a75737420616e6f74686572206261636b646f6f7220696e20796f757220636f646520796f752077616e7420746f2062652064657465637465640a"	

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 19

Code Snippet: \$fakeAPI1="Alzad8e8fca2dc0f896fd7cb4cb0031ba249123"

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 20

Code Snippet: \$fakeAPI2="AKIAD8E8FCA2DC0F896F"

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 21

Code Snippet: \$hash2="\$1\$VnG/6ABB\$t6w9bQFxvI9tf0sFJf2TR."

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 22

Code Snippet: \$hash3="d8e8fca2dc0f896fd7cb4cb0031ba249"

File: vulnerable_code\configuration.php

Vulnerability: High Entropy String

Line: 24

Code	Snippet:
if(\$pass=="\$6\$q8C1F6tv\$zTP/eEVixqyQBEfsSbTidUJfnaE2ojNIpTwTHava/UhFORv3V4ehyTOGdQEoFo1d EVG6UcXwhG.UHvyQyERz01"	

File: vulnerable_code\exec.php

Vulnerability: Cross Site Scripting

Line: 3

Code Snippet: "Nouvelle fonction anonyme : \$newfunc \n"

File: vulnerable_code\exec.php

Vulnerability: Cross Site Scripting

Line: 4

Code Snippet: \$newfunc (2, M_E

File: vulnerable_code\exec.php

Vulnerability: Remote Command Execution

Line: 17

Code Snippet: 'ping ' . \$target

File: vulnerable_code\exec.php

Vulnerability: Remote Command Execution

Line: 17

Code Snippet: 'ping ' . \$target

File: vulnerable_code\include.php

Vulnerability: File Inclusion

Line: 10

Code Snippet: \$mail

File: vulnerable_code\ldap.php

Vulnerability: Cross Site Scripting

Line: 11

Code Snippet: "<p>There are " . \$info ["count"] . " entries for that search:<p>"

File: vulnerable_code\ldap.php

Vulnerability: Cross Site Scripting

Line: 15

Code Snippet: "common name: " . \$info [\$i]["cn"][0] . "
"

File: vulnerable_code\ldap.php

Vulnerability: Cross Site Scripting

Line: 16

Code Snippet: "telephone: " . \$info [\$i]["telephoneNumber"][0] . "
"

File: vulnerable_code\ldap.php

Vulnerability: Cross Site Scripting

Line: 17

Code Snippet: "email: " . \$info [\$i]["mail"][0] . "
<hr />"

File: vulnerable_code\require.php

Vulnerability: File Inclusion

Line: 6

Code Snippet: \$which .'noparenthesis.php'

File: vulnerable_code\require.php

Vulnerability: File Inclusion

Line: 7

Code Snippet: \$which .'parenthesis.php'

File: vulnerable_code\sql-ip.php

Vulnerability: SQL Injection

Line: 5

Code Snippet: "SELECT * from toot where ip= \$cip "

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 25

Code Snippet: ""

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 25

Code Snippet: ""

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 26

Code Snippet: "<p id='spec'>". \$phone ['name']. "".nl2br(\$phone['specifications'])"

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 26

Code Snippet: "<p id='spec'>". \$phone ['name']. "".nl2br(\$phone['specifications'])"

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 38

Code Snippet: "".\$phone['name']. ""

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 38

Code Snippet: "".\$phone['name']. ""

File: vulnerable_code\sqli.php

Vulnerability: Cross Site Scripting

Line: 38

Code Snippet: "".\$phone['name']. ""

File: vulnerable_code\sqli2.php

Vulnerability: Cross Site Scripting

Line: 20

Code Snippet: "Welcome ". \$data ['username']."
"

File: vulnerable_code\ssti.php

Vulnerability: Server Side Template Injection

Line: 20

Code Snippet: \$name

File: vulnerable_code\ssti.php

Vulnerability: Server Side Template Injection

Line: 27

Code Snippet: "record", \$record

File: vulnerable_code\tainted-filename.php

Vulnerability: File Inclusion / Path Traversal

Line: 5

Code Snippet: 'sha1', \$tainted

File: vulnerable_code\tainted-filename.php

Vulnerability: File Inclusion / Path Traversal

Line: 8

Code Snippet: \$tainted

File: vulnerable_code\tainted-filename.php

Vulnerability: File Inclusion / Path Traversal

Line: 11

Code Snippet: \$tainted , 'file.txt'

File: vulnerable_code\tainted-filename.php

Vulnerability: File Inclusion / Path Traversal

Line: 14

Code Snippet: `dirname($tainted`

File: vulnerable_code\tainted-filename.php

Vulnerability: File Inclusion / Path Traversal

Line: 18

Code Snippet: `basename($tainted`

File: vulnerable_code\xss.php

Vulnerability: Cross Site Scripting

Line: 5

Code Snippet: `"<p>The mail ". $mail ." has been registered in our database.</p>"`
