

Home

Security analysis of the file

</var/www/html/test/guessnum4.php>

2 vulnerabilities found in 0.02 seconds!

Choose another file

Vulnerable Variables

Show

Count: 2

#	index	name	object	scope	variable_function	exist_destroyed	code_type	input	output	function	file	line	tainted	vulnerability	start_index	end_i
0	23	\$query		local	variable	exist	php code	regular	output	function	0	32	tainted	SQL Injection	99	99
1	34	\$query		local	variable	exist	php code	regular	output	function	0	37	tainted	SQL Injection	142	142

Output Variables

Hide

Count: 11

#	index	name	object	scope	variable_function	exist_destroyed	code_type	input	output	function	file	line	tainted	vulnerability	start_index	end_index
0	23	\$query		local	variable	exist	php code	regular	output	function	0	32	tainted	SQL Injection	99	
1	25	\$query		local	variable	exist	php code	regular	output	function	0	32	tainted	Cross Site Scripting	106	
2	26	mysql_error		local	function	exist	php code	regular	output	function	0	32	untainted	unknown	112	
3	34	\$query		local	variable	exist	php code	regular	output	function	0	37	tainted	SQL Injection	142	
4	36	\$query		local	variable	exist	php code	regular	output	function	0	37	tainted	Cross Site Scripting	149	
5	37	mysql_error		local	function	exist	php code	regular	output	function	0	37	untainted	unknown	155	
6	39	\$connection		local	variable	exist	php code	regular	output	function	0	43	untainted	unknown	175	
7	44	\$row[0]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	192	
8	45	\$row[1]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	197	
9	46	\$row[2]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	202	
10	47	\$row[3]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	207	

Parser Variables

Hide

Count: 48

#	name	object	scope	variable_function	exist_destroyed	code_type	input	output	function	file	line	tainted	vulnerability	start_index	end_index
0	\$name		local	variable	exist	php code	regular	regular	function	0	11	tainted	unknown	2	
1	\$_COOKIE['Milano']		local	variable	exist	php code	input	regular	function	0	11	tainted	unknown	6	
2	\$_COOKIE['Milano']		local	function	exist	php code	regular	regular	function	0	11	tainted	unknown	5	
3	\$cnt		local	variable	exist	php code	regular	regular	function	0	12	tainted	unknown	14	
4	\$_COOKIE['Brussels']		local	variable	exist	php code	input	regular	function	0	12	tainted	unknown	18	
5	\$_COOKIE['Brussels']		local	function	exist	php code	regular	regular	function	0	12	tainted	unknown	17	

11/30/2015phpSAFE - PHP Security Analysis For Everyone

6	\$guess		local	variable	exist	php code	regular	regular	function	0	13	tainted	unknown	26
7	\$_COOKIE['Geneva']		local	variable	exist	php code	input	regular	function	0	13	tainted	unknown	30
8	\$_COOKIE['Geneva']		local	function	exist	php code	regular	regular	function	0	13	tainted	unknown	29
9	\$lessthan		local	variable	exist	php code	regular	regular	function	0	24	untainted	unknown	41
10	\$lessthan		local	variable	exist	php code	regular	regular	function	0	25	untainted	unknown	49
11	\$name		local	variable	exist	php code	regular	regular	function	0	25	tainted	unknown	51
12	\$lessthan, \$name		local	function	exist	php code	regular	regular	function	0	25	tainted	unknown	48
13	\$name		local	variable	exist	php code	regular	regular	function	0	26	untainted	unknown	58
14	\$cnt		local	variable	exist	php code	regular	regular	function	0	26	untainted	unknown	62
15	\$connection		local	variable	exist	php code	regular	regular	function	0	27	untainted	unknown	67
16	mysql_connect		local	function	exist	php code	regular	regular	function	0	27	untainted	unknown	70
17	\$connection		local	variable	exist	php code	regular	regular	function	0	29	untainted	unknown	82
18	\$connection		local	function	exist	php code	regular	regular	function	0	29	untainted	unknown	79
19	\$query		local	variable	exist	php code	regular	regular	function	0	31	tainted	unknown	85
20	\$name		local	variable	exist	php code	regular	regular	function	0	31	untainted	unknown	89
21	\$guess		local	variable	exist	php code	regular	regular	function	0	31	tainted	unknown	91
22	\$result		local	variable	exist	php code	regular	regular	function	0	32	tainted	unknown	95
23	\$query		local	variable	exist	php code	regular	output	function	0	32	tainted	SQL Injection	99
24	mysql_query		local	function	exist	php code	input	regular	function	0	32	tainted	unknown	98
25	\$query		local	variable	exist	php code	regular	output	function	0	32	tainted	Cross Site Scripting	106
26	mysql_error		local	function	exist	php code	regular	output	function	0	32	untainted	unknown	112
27	\$result		local	variable	exist	php code	regular	regular	function	0	34	tainted	unknown	120
28	\$result		local	function	exist	php code	regular	regular	function	0	34	tainted	unknown	119
29	\$query		local	variable	exist	php code	regular	regular	function	0	36	tainted	unknown	126
30	\$name		local	variable	exist	php code	regular	regular	function	0	36	untainted	unknown	130
31	\$guess		local	variable	exist	php code	regular	regular	function	0	36	tainted	unknown	132
32	\$cnt		local	variable	exist	php code	regular	regular	function	0	36	untainted	unknown	134
33	\$result		local	variable	exist	php code	regular	regular	function	0	37	tainted	unknown	138
34	\$query		local	variable	exist	php code	regular	output	function	0	37	tainted	SQL Injection	142
35	mysql_query		local	function	exist	php code	input	regular	function	0	37	tainted	unknown	141
36	\$query		local	variable	exist	php code	regular	output	function	0	37	tainted	Cross Site Scripting	149
37	mysql_error		local	function	exist	php code	regular	output	function	0	37	untainted	unknown	155
38	\$result		local	variable	exist	php code	regular	regular	function	0	42	tainted	unknown	169
39	\$connection		local	variable	exist	php code	regular	output	function	0	43	untainted	unknown	175
40	mysql_query		local	function	exist	php code	input	regular	function	0	42	tainted	unknown	172
41	\$row		local	variable	exist	php code	regular	regular	function	0	45	tainted	unknown	180
42	\$result		local	variable	exist	php code	regular	regular	function	0	45	tainted	unknown	184
43	mysql_fetch_array		local	function	exist	php code	input	regular	function	0	45	tainted	unknown	183
44	\$row[0]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	192
45	\$row[1]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	197
46	\$row[2]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	202
47	\$row[3]		local	variable	exist	php code	regular	output	function	0	47	untainted	unknown	207

File Functions

Hide

Count: 1

#	name	file	executed	start_line	end_line	start_index	end_index	parameters						
0	function	0	executed	0	52	0	219		substr 11	substr 12	substr 13	preg_match 25	print 26	mysc

Used Functions

Hide Count: 11

#	name	user_defined	input	output	vulnerability	filter	revert_filter	other
0	substr	not user defined	not input	not output	none	not filter	not revert filter	other
1	preg_match	not user defined	not input	not output	none	not filter	not revert filter	other
2	print	not user defined	not input	output	Cross Site Scripting	not filter	not revert filter	not other
3	mysql_connect	not user defined	not input	not output	none	not filter	not revert filter	other
4	mysql_select_db	not user defined	not input	not output	none	not filter	not revert filter	other
5	mysql_query	not user defined	input	output	SQL Injection	not filter	not revert filter	not other
6	die	not user defined	not input	output	Cross Site Scripting	not filter	not revert filter	not other
7	mysql_error	not user defined	not input	not output	none	not filter	not revert filter	other
8	mysql_num_rows	not user defined	not input	not output	none	not filter	not revert filter	other
9	echo	not user defined	not input	output	Cross Site Scripting	not filter	not revert filter	not other
10	mysql_fetch_array	not user defined	input	not output	none	not filter	not revert filter	not other

Show All Hide All Default All

Show/Hide Parser Debug (0)

Show/Hide Vulnerable Variables (2)

```
[0] ...
[index] => 23
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 99
[end_index] => 99
[dependencies_index] ...
  [0] => 19
[variable_filter] ...
[variable_revert_filter] ...
[1] ...
[index] => 34
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 142
[end_index] => 142
[dependencies_index] ...
  [0] => 29
[variable_filter] ...
[variable_revert_filter] ...
```

☒ Show/Hide Output Variables (11)

```
[0] ...
[index] => 23
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 99
[end_index] => 99
[dependencies_index] ...
  [0] => 19
[variable_filter] ...
[variable_revert_filter] ...

[1] ...
[index] => 25
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => Cross Site Scripting
[start_index] => 106
[end_index] => 106
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...

[2] ...
[index] => 26
[name] => mysql_error
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 112
[end_index] => 113
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...

[3] ...
[index] => 34
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 142
[end_index] => 142
[dependencies_index] ...
  [0] => 29
[variable_filter] ...
[variable_revert_filter] ...

[4] ...
[index] => 36
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => Cross Site Scripting
[start_index] => 149
```

```

[end_index] => 149
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[5] ...
[index] => 37
[name] => mysql_error
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 155
[end_index] => 156
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[6] ...
[index] => 39
[name] => $connection
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 43
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 175
[end_index] => 175
[dependencies_index] ...
    [0] => 17
[variable_filter] ...
[variable_revert_filter] ...
[7] ...
[index] => 44
[name] => $row[0]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 192
[end_index] => 195
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[8] ...
[index] => 45
[name] => $row[1]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 197
[end_index] => 200
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[9] ...
[index] => 46
[name] => $row[2]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 202
[end_index] => 205
[dependencies_index] ...
[variable_filter] ...

```

```

[variable_revert_filter] ...
[10] ...
[index] => 47
[name] => $row[3]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 207
[end_index] => 210
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...

```

☒ Show/Hide Parser Variables (48)

```

[0] ...
[name] => $name
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 11
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 2
[end_index] => 2
[dependencies_index] ...
  [0] => 2
[variable_filter] ...
[variable_revert_filter] ...
[1] ...
[name] => $_COOKIE['Milano']
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0
[line] => 11
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 6
[end_index] => 9
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[2] ...
[name] => $_COOKIE['Milano']
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 11
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 5
[end_index] => 12
[dependencies_index] ...
  [0] => 1
[variable_filter] ...
[variable_revert_filter] ...
[3] ...
[name] => $cnt
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 12
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 14

```

```

[end_index] => 14
[dependencies_index] ...
[0] => 5
[variable_filter] ...
[variable_revert_filter] ...
[4] ...
[name] => $_COOKIE['Brussels']
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0
[line] => 12
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 18
[end_index] => 21
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[5] ...
[name] => $_COOKIE['Brussels']
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 12
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 17
[end_index] => 24
[dependencies_index] ...
[0] => 4
[variable_filter] ...
[variable_revert_filter] ...
[6] ...
[name] => $guess
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 13
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 26
[end_index] => 26
[dependencies_index] ...
[0] => 8
[variable_filter] ...
[variable_revert_filter] ...
[7] ...
[name] => $_COOKIE['Geneva']
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0
[line] => 13
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 30
[end_index] => 33
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[8] ...
[name] => $_COOKIE['Geneva']
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 13
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 29
[end_index] => 36
[dependencies_index] ...
[0] => 7
[variable_filter] ...
[variable_revert_filter] ...
[9] ...

```

```

[name] => $lessthan
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 24
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 41
[end_index] => 41
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[10] ...
[name] => $lessthan
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 25
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 49
[end_index] => 49
[dependencies_index] ...
  [0] => 9
[variable_filter] ...
[variable_revert_filter] ...
[11] ...
[name] => $name
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 25
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 51
[end_index] => 51
[dependencies_index] ...
  [0] => 0
[variable_filter] ...
[variable_revert_filter] ...
[12] ...
[name] => $lessthan, $name
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 25
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 48
[end_index] => 52
[dependencies_index] ...
  [0] => 10
  [1] => 11
[variable_filter] ...
[variable_revert_filter] ...
[13] ...
[name] => $name
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 26
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 58
[end_index] => 58
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[14] ...
[name] => $cnt
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist

```



```

[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 26
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 62
[end_index] => 62
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[15] ...
[name] => $connection
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 27
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 67
[end_index] => 67
[dependencies_index] ...
    [0] => 16
[variable_filter] ...
[variable_revert_filter] ...
[16] ...
[name] => mysql_connect
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 27
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 70
[end_index] => 76
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[17] ...
[name] => $connection
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 29
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 82
[end_index] => 82
[dependencies_index] ...
    [0] => 15
[variable_filter] ...
[variable_revert_filter] ...
[18] ...
[name] => $connection
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 29
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 79
[end_index] => 83
[dependencies_index] ...
    [0] => 17
[variable_filter] ...
[variable_revert_filter] ...
[19] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 31

```

```
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 85
[end_index] => 85
[dependencies_index] ...
  [0] => 20
  [1] => 21
[variable_filter] ...
[variable_revert_filter] ...
[20] ...
[name] => $name
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 31
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 89
[end_index] => 89
[dependencies_index] ...
  [0] => 13
[variable_filter] ...
[variable_revert_filter] ...
[21] ...
[name] => $guess
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 31
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 91
[end_index] => 91
[dependencies_index] ...
  [0] => 6
[variable_filter] ...
[variable_revert_filter] ...
[22] ...
[name] => $result
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 95
[end_index] => 95
[dependencies_index] ...
  [0] => 24
[variable_filter] ...
[variable_revert_filter] ...
[23] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 99
[end_index] => 99
[dependencies_index] ...
  [0] => 19
[variable_filter] ...
[variable_revert_filter] ...
[24] ...
[name] => mysql_query
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 98
```

```

[end_index] => 98
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[25] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => tainted
[vulnerability] => Cross Site Scripting
[start_index] => 106
[end_index] => 106
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[26] ...
[name] => mysql_error
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 32
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 112
[end_index] => 113
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[27] ...
[name] => $result
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 34
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 120
[end_index] => 120
[dependencies_index] ...
[0] => 22
[variable_filter] ...
[variable_revert_filter] ...
[28] ...
[name] => $result
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 34
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 119
[end_index] => 121
[dependencies_index] ...
[0] => 27
[variable_filter] ...
[variable_revert_filter] ...
[29] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 36
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 126
[end_index] => 126
[dependencies_index] ...
[0] => 30
[1] => 31
[2] => 32
[variable_filter] ...
[variable_revert_filter] ...

```

```
[30] ...
[name] => $name
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 36
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 130
[end_index] => 130
[dependencies_index] ...
[0] => 20
[variable_filter] ...
[variable_revert_filter] ...

[31] ...
[name] => $guess
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 36
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 132
[end_index] => 132
[dependencies_index] ...
[0] => 21
[variable_filter] ...
[variable_revert_filter] ...

[32] ...
[name] => $cnt
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 36
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 134
[end_index] => 134
[dependencies_index] ...
[0] => 14
[variable_filter] ...
[variable_revert_filter] ...

[33] ...
[name] => $result
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 138
[end_index] => 138
[dependencies_index] ...
[0] => 35
[variable_filter] ...
[variable_revert_filter] ...

[34] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => SQL Injection
[start_index] => 142
[end_index] => 142
[dependencies_index] ...
[0] => 29
[variable_filter] ...
[variable_revert_filter] ...

[35] ...
[name] => mysql_query
[object] ...
[scope] => local
```

```

[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 141
[end_index] => 141
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[36] ...
[name] => $query
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => tainted
[vulnerability] => Cross Site Scripting
[start_index] => 149
[end_index] => 149
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[37] ...
[name] => mysql_error
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 37
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 155
[end_index] => 156
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[38] ...
[name] => $result
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => regular
[function] => function
[file] => 0
[line] => 42
[tainted] => tainted
[vulnerability] => unknown
[start_index] => 169
[end_index] => 169
[dependencies_index] ...
[0] => 40
[variable_filter] ...
[variable_revert_filter] ...
[39] ...
[name] => $connection
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 43
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 175
[end_index] => 175
[dependencies_index] ...
[0] => 17
[variable_filter] ...
[variable_revert_filter] ...
[40] ...
[name] => mysql_query
[object] ...
[scope] => local
[variable_function] => function
[exist_destroyed] => exist
[code_type] => php code
[input] => input
[output] => regular
[function] => function
[file] => 0

```

```

[ ] [line] => 42
[ ] [tainted] => tainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 172
[ ] [end_index] => 172
[ ] [dependencies_index] ...
[ ] [variable_filter] ...
[ ] [variable_revert_filter] ...
[41] ...
[ ] [name] => $row
[ ] [object] ...
[ ] [scope] => local
[ ] [variable_function] => variable
[ ] [exist_destroyed] => exist
[ ] [code_type] => php code
[ ] [input] => regular
[ ] [output] => regular
[ ] [function] => function
[ ] [file] => 0
[ ] [line] => 45
[ ] [tainted] => tainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 180
[ ] [end_index] => 180
[ ] [dependencies_index] ...
[ ] [0] => 43
[ ] [variable_filter] ...
[ ] [variable_revert_filter] ...
[42] ...
[ ] [name] => $result
[ ] [object] ...
[ ] [scope] => local
[ ] [variable_function] => variable
[ ] [exist_destroyed] => exist
[ ] [code_type] => php code
[ ] [input] => regular
[ ] [output] => regular
[ ] [function] => function
[ ] [file] => 0
[ ] [line] => 45
[ ] [tainted] => tainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 184
[ ] [end_index] => 184
[ ] [dependencies_index] ...
[ ] [0] => 38
[ ] [variable_filter] ...
[ ] [variable_revert_filter] ...
[43] ...
[ ] [name] => mysql_fetch_array
[ ] [object] ...
[ ] [scope] => local
[ ] [variable_function] => function
[ ] [exist_destroyed] => exist
[ ] [code_type] => php code
[ ] [input] => input
[ ] [output] => regular
[ ] [function] => function
[ ] [file] => 0
[ ] [line] => 45
[ ] [tainted] => tainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 183
[ ] [end_index] => 183
[ ] [dependencies_index] ...
[ ] [variable_filter] ...
[ ] [variable_revert_filter] ...
[44] ...
[ ] [name] => $row[0]
[ ] [object] ...
[ ] [scope] => local
[ ] [variable_function] => variable
[ ] [exist_destroyed] => exist
[ ] [code_type] => php code
[ ] [input] => regular
[ ] [output] => output
[ ] [function] => function
[ ] [file] => 0
[ ] [line] => 47
[ ] [tainted] => untainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 192
[ ] [end_index] => 195
[ ] [dependencies_index] ...
[ ] [variable_filter] ...
[ ] [variable_revert_filter] ...
[45] ...
[ ] [name] => $row[1]
[ ] [object] ...
[ ] [scope] => local
[ ] [variable_function] => variable
[ ] [exist_destroyed] => exist
[ ] [code_type] => php code
[ ] [input] => regular
[ ] [output] => output
[ ] [function] => function
[ ] [file] => 0
[ ] [line] => 47
[ ] [tainted] => untainted
[ ] [vulnerability] => unknown
[ ] [start_index] => 197
[ ] [end_index] => 200
[ ] [dependencies_index] ...
[ ] [variable_filter] ...

```

```

[variable_revert_filter] ...
[46] ...
[name] => $row[2]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 202
[end_index] => 205
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...
[47] ...
[name] => $row[3]
[object] ...
[scope] => local
[variable_function] => variable
[exist_destroyed] => exist
[code_type] => php code
[input] => regular
[output] => output
[function] => function
[file] => 0
[line] => 47
[tainted] => untainted
[vulnerability] => unknown
[start_index] => 207
[end_index] => 210
[dependencies_index] ...
[variable_filter] ...
[variable_revert_filter] ...

```

☒ Show/Hide Files Functions (1)

```

[0] ...
[name] => function
[file] => 0
[executed] => executed
[start_line] => 0
[end_line] => 52
[start_index] => 0
[end_index] => 219
[parameters] ...
[called_functions] ...
[0] ...
[name] => substr
[line] => 11
[1] ...
[name] => substr
[line] => 12
[2] ...
[name] => substr
[line] => 13
[3] ...
[name] => preg_match
[line] => 25
[4] ...
[name] => print
[line] => 26
[5] ...
[name] => mysql_connect
[line] => 27
[6] ...
[name] => mysql_select_db
[line] => 29
[7] ...
[name] => mysql_query
[line] => 32
[8] ...
[name] => die
[line] => 32
[9] ...
[name] => mysql_error
[line] => 32
[10] ...
[name] => mysql_num_rows
[line] => 34
[11] ...
[name] => mysql_query
[line] => 37
[12] ...
[name] => die
[line] => 37
[13] ...
[name] => mysql_error
[line] => 37
[14] ...
[name] => print
[line] => 39
[15] ...

```

```

        [name] => echo
        [line] => 41
    [16] ...
        [name] => mysql_query
        [line] => 42
    [17] ...
        [name] => mysql_fetch_array
        [line] => 45
    [18] ...
        [name] => print
        [line] => 47
    [19] ...
        [name] => print
        [line] => 49
[start_parameter_index] => -1
[end_parameter_index] => -1

```

☒ Show/Hide Used Functions (11)

```

[0] ...
[name] => substr
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => other
[1] ...
[name] => preg_match
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => other
[2] ...
[name] => print
[user_defined] => not user defined
[input] => not input
[output] => output
[vulnerability] => Cross Site Scripting
[filter] => not filter
[revert_filter] => not revert filter
[other] => not other
[3] ...
[name] => mysql_connect
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => other
[4] ...
[name] => mysql_select_db
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => other
[5] ...
[name] => mysql_query
[user_defined] => not user defined
[input] => input
[output] => output
[vulnerability] => SQL Injection
[filter] => not filter
[revert_filter] => not revert filter
[other] => not other
[6] ...
[name] => die
[user_defined] => not user defined
[input] => not input
[output] => output
[vulnerability] => Cross Site Scripting
[filter] => not filter
[revert_filter] => not revert filter
[other] => not other
[7] ...
[name] => mysql_error
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => other
[8] ...
[name] => mysql_num_rows
[user_defined] => not user defined
[input] => not input
[output] => not output
[vulnerability] => none
[filter] => not filter

```



```

[revert_filter] => not revert filter
[other] => other
[9] ...
[name] => echo
[user_defined] => not user defined
[input] => not input
[output] => output
[vulnerability] => Cross Site Scripting
[filter] => not filter
[revert_filter] => not revert filter
[other] => not other
[10] ...
[name] => mysql_fetch_array
[user_defined] => not user defined
[input] => input
[output] => not output
[vulnerability] => none
[filter] => not filter
[revert_filter] => not revert filter
[other] => not other

```

☒ Show/Hide Files Include Require (0)

☒ Show/Hide Files Tokens (1)

```

[0] ...
[0] ...
[0] => 312
[1] =>

[2] => 1
[1] ...
[0] => 374
[1] => 10
[2] ...
[0] => 310
[1] => $name
[2] => 11
[3] => =
[4] ...
[0] => 308
[1] => substr
[2] => 11
[5] => (
[6] ...
[0] => 310
[1] => $_COOKIE
[2] => 11
[7] => [
[8] ...
[0] => 316
[1] => 'Milano'
[2] => 11
[9] => ]
[10] => ,
[11] ...
[0] => 306
[1] => 14
[2] => 11
[12] => )
[13] => ;
[14] ...
[0] => 310
[1] => $cnt
[2] => 12
[15] => =
[16] ...
[0] => 308
[1] => substr
[2] => 12
[17] => (
[18] ...
[0] => 310
[1] => $_COOKIE
[2] => 12
[19] => [
[20] ...
[0] => 316
[1] => 'Brussels'
[2] => 12
[21] => ]
[22] => ,
[23] ...
[0] => 306
[1] => 14
[2] => 12

```

```

[24] => )
[25] => ;
[26] ...
[0] => 310
[1] => $guess
[2] => 13
[27] => =
[28] ...
[0] => 308
[1] => substr
[2] => 13
[29] => (
[30] ...
[0] => 310
[1] => $_COOKIE
[2] => 13
[31] => [
[32] ...
[0] => 316
[1] => 'Geneva'
[2] => 13
[33] => ]
[34] => ,
[35] ...
[0] => 306
[1] => 14
[2] => 13
[36] => )
[37] => ;
[38] ...
[0] => 376
[1] => ?>

[2] => 14
[39] ...
[0] => 312
[1] =>

```



```

[2] => 15
[40] ...
[0] => 374
[1] => 22
[41] ...
[0] => 310
[1] => $lessthan
[2] => 24
[42] => =
[43] ...
[0] => 316
[1] => "/\ 24
[44] => ;
[45] ...
[0] => 302
[1] => if
[2] => 25
[46] => (
[47] ...
[0] => 308
[1] => preg_match
[2] => 25
[48] => (
[49] ...
[0] => 310
[1] => $lessthan
[2] => 25
[50] => ,
[51] ...
[0] => 310
[1] => $name
[2] => 25
[52] => )
[53] => )
[54] => {
[55] ...
[0] => 266
[1] => print
[2] => 26
[56] ...
[0] => 316
[1] => "

```

name changed to unknown

"

```

[2] => 26
[57] => ;
[58] ...

```

```
[0] => 310
[1] => $name
[2] => 26
[59] => =
[60] ...
[0] => 316
[1] => "unknown"
[2] => 26
[61] => ;
[62] ...
[0] => 310
[1] => $cnt
[2] => 26
[63] => =
[64] ...
[0] => 306
[1] => 99
[2] => 26
[65] => ;
[66] => }
[67] ...
[0] => 310
[1] => $connection
[2] => 27
[68] => =
[69] ...
[0] => 308
[1] => mysql_connect
[2] => 27
[70] => (
[71] ...
[0] => 316
[1] => "localhost"
[2] => 27
[72] => ,
[73] ...
[0] => 316
[1] => "root"
[2] => 27
[74] => ,
[75] ...
[0] => 316
[1] => "vicnum"
[2] => 27
[76] => )
[77] => ;
[78] ...
[0] => 308
[1] => mysql_select_db
[2] => 29
[79] => (
[80] ...
[0] => 316
[1] => "vicnum"
[2] => 29
[81] => ,
[82] ...
[0] => 310
[1] => $connection
[2] => 29
[83] => )
[84] => ;
[85] ...
[0] => 310
[1] => $query
[2] => 31
[86] => =
[87] => "
```

```
[88] ...
    [0] => 315
    [1] => SELECT name,count,tod FROM guessnumresults WHERE name = '
    [2] => 31
[89] ...
    [0] => 310
    [1] => $name
    [2] => 31
[90] ...
    [0] => 315
    [1] => ' AND guess = '
    [2] => 31
[91] ...
    [0] => 310
    [1] => $guess
    [2] => 31
[92] ...
    [0] => 315
    [1] => '
    [2] => 31
[93] => "
[94] => ;
[95] ...
    [0] => 310
    [1] => $result
    [2] => 32
[96] => =
[97] ...
    [0] => 308
    [1] => mysql_query
    [2] => 32
[98] => (
[99] ...
    [0] => 310
    [1] => $query
    [2] => 32
[100] => )
[101] ...
    [0] => 263
    [1] => or
    [2] => 32
[102] ...
    [0] => 301
    [1] => die
    [2] => 32
[103] => (
[104] => "
[105] ...
    [0] => 315
    [1] => ERROR in
    [2] => 32
[106] ...
    [0] => 310
    [1] => $query
    [2] => 32
[107] => "
[108] => .
[109] ...
    [0] => 316
    [1] => " "
    [2] => 32
[110] => .
[111] ...
    [0] => 308
    [1] => mysql_error
    [2] => 32
[112] => (
[113] => )
```

```
[114] => )
[115] => ;
[116] ...
    [0] => 302
    [1] => if
    [2] => 34
[117] => (
[118] ...
    [0] => 308
    [1] => mysql_num_rows
    [2] => 34
[119] => (
[120] ...
    [0] => 310
    [1] => $result
    [2] => 34
[121] => )
[122] => <
[123] ...
    [0] => 306
    [1] => 1
    [2] => 34
[124] => )
[125] => {
[126] ...
    [0] => 310
    [1] => $query
    [2] => 36
[127] => =
[128] => "
[129] ...
    [0] => 315
    [1] => INSERT INTO guessnumresults(name,guess,count) VALUES(\"
    [2] => 36
[130] ...
    [0] => 310
    [1] => $name
    [2] => 36
[131] ...
    [0] => 315
    [1] => \",
    [2] => 36
[132] ...
    [0] => 310
    [1] => $guess
    [2] => 36
[133] ...
    [0] => 315
    [1] => ,
    [2] => 36
[134] ...
    [0] => 310
    [1] => $cnt
    [2] => 36
[135] ...
    [0] => 315
    [1] => )
    [2] => 36
[136] => "
[137] => ;
[138] ...
    [0] => 310
    [1] => $result
    [2] => 37
[139] => =
[140] ...
    [0] => 308
    [1] => mysql_query
```

```

    [2] => 37
[141] => (
[142] ...
    [0] => 310
    [1] => $query
    [2] => 37
[143] => )
[144] ...
    [0] => 263
    [1] => or
    [2] => 37
[145] ...
    [0] => 301
    [1] => die
    [2] => 37
[146] => (
[147] => "
[148] ...
    [0] => 315
    [1] => ERROR in
    [2] => 37
[149] ...
    [0] => 310
    [1] => $query
    [2] => 37
[150] => "
[151] => .
[152] ...
    [0] => 316
    [1] => " "
    [2] => 37
[153] => .
[154] ...
    [0] => 308
    [1] => mysql_error
    [2] => 37
[155] => (
[156] => )
[157] => )
[158] => ;
[159] ...
    [0] => 266
    [1] => print
    [2] => 39
[160] ...
    [0] => 316
    [1] => "

```

Your Results have been stored in our database.\nBelow please find the top 10 Guessnum playe

"

```

    [2] => 39
[161] => ;
[162] => }
[163] ...
    [0] => 304
    [1] => else
    [2] => 41
[164] => {
[165] ...
    [0] => 317
    [1] => echo
    [2] => 41
[166] ...

```

```
[0] => 316
[1] => "
```

Duplicate names with the same guess value are not allowed!

Below find the top 10 scores for legitimate Guessnum players.

"

```

    [2] => 41
[167] => ;
[168] => }
[169] ...
    [0] => 310
    [1] => $result
    [2] => 42
[170] => =
[171] ...
    [0] => 308
    [1] => mysql_query
    [2] => 42
[172] => (
[173] ...
    [0] => 316
    [1] => "SELECT name,guess,count,tod FROM
                        guessnumresults where count > 0 order by count,tod limit 10"
    [2] => 42
[174] => ,
[175] ...
    [0] => 310
    [1] => $connection
    [2] => 43
[176] => )
[177] => ;
[178] ...
    [0] => 319
    [1] => while
    [2] => 45
[179] => (
[180] ...
    [0] => 310
    [1] => $row
    [2] => 45
[181] => =
[182] ...
    [0] => 308
    [1] => mysql_fetch_array
    [2] => 45
[183] => (
[184] ...
    [0] => 310
    [1] => $result
    [2] => 45
[185] => ,
[186] ...
    [0] => 308
    [1] => MYSQL_NUM
    [2] => 45
[187] => )
[188] => )
[189] => {
[190] ...
    [0] => 266
    [1] => print
    [2] => 47
[191] => "
```

```
[192] ...
      [0] => 310
      [1] => $row
      [2] => 47
[193] => [
[194] ...
      [0] => 311
      [1] => 0
      [2] => 47
[195] => ]
[196] ...
      [0] => 315
      [1] => \t has guessed
      [2] => 47
[197] ...
      [0] => 310
      [1] => $row
      [2] => 47
[198] => [
[199] ...
      [0] => 311
      [1] => 1
      [2] => 47
[200] => ]
[201] ...
      [0] => 315
      [1] => in
      [2] => 47
[202] ...
      [0] => 310
      [1] => $row
      [2] => 47
[203] => [
[204] ...
      [0] => 311
      [1] => 2
      [2] => 47
[205] => ]
[206] ...
      [0] => 315
      [1] => guess(es) on
      [2] => 47
[207] ...
      [0] => 310
      [1] => $row
      [2] => 47
[208] => [
[209] ...
      [0] => 311
      [1] => 3
      [2] => 47
[210] => ]
[211] ...
      [0] => 315
      [1] => \n
      [2] => 47
[212] => "
[213] => ;
[214] => }
[215] ...
      [0] => 266
      [1] => print
      [2] => 49
[216] ...
      [0] => 316
      [1] => "
```

Click [here](#) to play again. You can also search for your favorite Guessnum player by entering

and then clicking on the SEARCH button.

Guessnum Player:

```
[2] => 49
[217] => ;
[218] ...
[0] => 376
[1] => ?>

[2] => 51
[219] ...
[0] => 312
[1] =>
```

Guessnum is part of the Vicnum project which was developed for educational purposes to demonstrate common web vulnerabilities.
For comments please visit the [OWASP project page](#).

[2] => 52
