

# **WordPress security in examples**

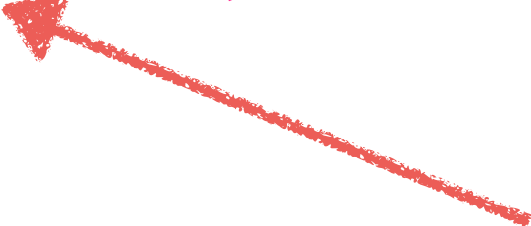
Kacper Szurek

<http://security.szurek.pl>

<https://twitter.com/kacperszurek>

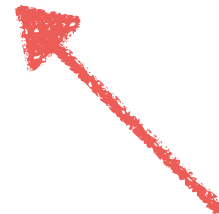
# Secure by default

```
function add_magic_quotes( $array ) {  
    foreach ( (array) $array as $k => $v ) {  
        if ( is_array( $v ) ) {  
            $array[$k] = add_magic_quotes( $v );  
        } else {  
            $array[$k] = addslashes( $v );  
        }  
    }  
    return $array;  
}  
  
$_GET      = add_magic_quotes( $_GET      );  
$_POST     = add_magic_quotes( $_POST     );  
$_COOKIE   = add_magic_quotes( $_COOKIE   );  
$_SERVER   = add_magic_quotes( $_SERVER   );
```



# addslashes

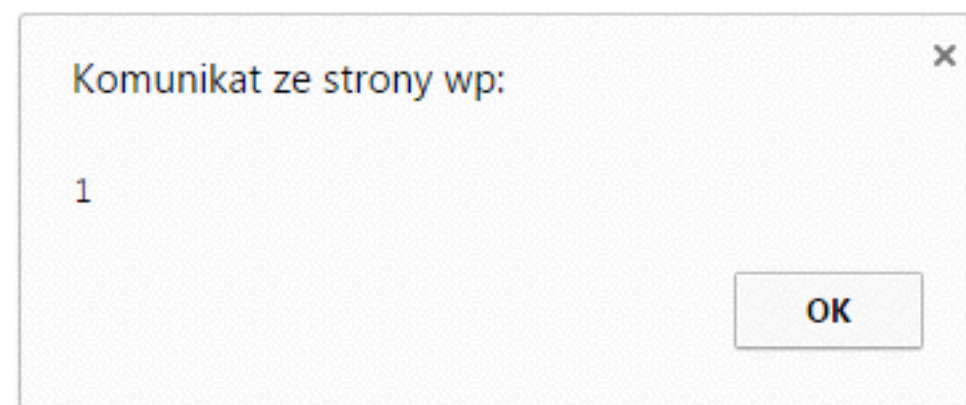
C:\Users\Directory\



# Reflected XSS

```
<input value="<?php echo $_GET['email']; ?>">
```

```
<input value="\ "><script>alert(1);</script>">
```



# XSS - esc\_attr

" → &quot;

' → &#039;

< → &lt;

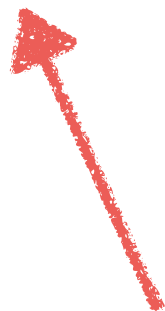
> → &gt;

# esc\_attr

`<input value="<?php echo esc_attr($_GET['email']); ?>">` ✓

`<input value='<?php echo esc_attr($_GET['email']); ?>'>` ✓

`<input value=<?php echo esc_attr($_GET['email']); ?>>` ✗



`<input value=aaa\\ onmouseover=alert(1)>`

# esc\_attr vs URL

`<a href="<?php echo esc_attr($_GET['email']); ?>">URL</a>` ❌

`<a href="<?php echo esc_url($_GET['email']); ?>">URL</a>` ✓



execute javascript from url

`<a href="javascript:alert(1)">URL</a>`

# Url problem

`<a href="<?php echo esc_url_raw($_GET['url']); ?>">Click</a>` ✗

`<a href="<?php echo esc_url($_GET['url']); ?>">Click</a>` ✓

`echo wp_remote_get(esc_url_raw($_GET['url']));` ✓

`$url = 'http://example.com?param=value&param2=value2';`

`esc_url = http://example.com?param=value&#038;param2=value2`

`esc_url_raw = http://example.com?param=value&param2=value2`



# XSS - own solution

```
<input value="<?php echo strip_tags($_GET['email']); ?>">
```

<code>\$input</code>	<code>strip_tags(\$input)</code>
<code>&lt;script&gt;alert(1);&lt;/script&gt;</code>	<code>alert(1);</code>
<code>&lt;input value="a" onmouseover=alert(1)&gt;</code>	<code>&lt;input value="a" onmouseover=alert(1)&gt;</code>
<code>\ " onmouseover=alert(1)</code>	<code>\ " onmouseover=alert(1)</code>

# XSS - wrong flag

```
<input value='<?php echo htmlspecialchars($_GET['email']); ?>'>
```

Flag	Description
ENT_NOQUOTES	Leave ' and " unconverted
ENT_COMPAT (default)	Convert "
ENT_QUOTES	Convert ' and "

# XSS - RTFM

```
$.post('http://wp/', {  
    id: '<?php echo json_encode(array('id' => $_GET['id'])); ?>'  
}); ✗
```

```
$.post('http://wp/', {  
    id: "<?php echo json_encode(array('id' => $_GET['id'])); ?>"  
}); ✗ SyntaxError: Unexpected identifier
```

```
$.post('http://wp/', {  
    id: <?php echo json_encode(array('id' => $_GET['id'])); ?>  
}); ✓
```

# Upload

xss.swf - <http://github.com/evilcos/xss.swf>

[http://example.com/xss.swf?a=eval&c=alert\(document.domain\)](http://example.com/xss.swf?a=eval&c=alert(document.domain))

'accept\_file\_types' => '\.(gif|jpe?g|png|bmp|mp3|wav|**zip**)\$/i'



Extract file to temporary directory

# Download

```
readfile('../some/dir/' . $_GET['file']);
```

```
readfile('../some/dir/../../wp-config.php');
```

```
readfile('../some/dir/' . basename($_GET['file'])); ✓
```

```
readfile(' ../some/dir/' . str_replace("../", "", $_GET['file'])); ❌
```

```
$_GET['file'] = '..././..././'
```

# Strange path

[http://example.com/our\\_secret\\_dir/strange\\_path/secret.html](http://example.com/our_secret_dir/strange_path/secret.html)

Deny from all

Options -Indexes

## **Forbidden**

You don't have  
permission to access  
/wp/ on this server.

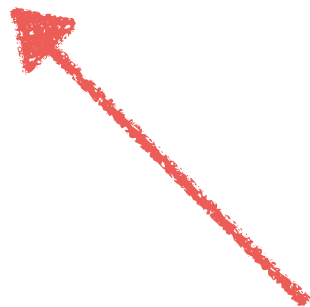
## **Index of /wp-content/uploads**

- Parent Directory
- 2015/
- 2014/

# Save redirect

```
if ( $_GET['password'] != 'our_secret_password' ) {  
    wp_redirect('Location: index.php'); ✗  
}
```

```
if ( $_GET['password'] != 'our_secret_password' ) {  
    wp_redirect('Location: index.php');  
    die(); ✓  
}
```



**wp\_redirect** does not exit automatically

# example.com

```
$_GET['url'] = "http://google.com";
```

```
wp_redirect($_GET['url']);
```

 ✖

```
header("Location: http://google.com");
```

```
wp_safe_redirect($_GET['url']);
```

 ✔

```
header("Location: http://example.com/wp-admin/");
```



# Contact form

```
wp_mail($_GET['to'], $_GET['subject'], $_GET['message']);
```



make it static

```

```

123456

# SQL Injection

```
$query = 'SELECT * FROM table WHERE id='.$_GET['id'];  
$results = $wpdb->get_results($query); ❌
```

```
$query = 'SELECT * FROM table WHERE id=0 UNION SELECT  
user_pass FROM wp_users WHERE ID=1';
```

# Always escape

```
$q = 'SELECT * FROM table WHERE id= 1 LIMIT '.$_GET['limit'];
```

```
$q = 'SELECT * FROM table WHERE id= 1 LIMIT 1,1 PROCEDURE  
analyse((select extractvalue(rand(),concat(0x3a,(IF(MID(version()),  
1,1) LIKE 5, BENCHMARK(5000000,SHA1(1)),1))))),1)';
```

<https://rateip.com/blog/sql-injections-in-mysql-limit-clause/>

# esc\_sql

`$q = 'SELECT * FROM tbl WHERE id=' . $_GET['id'];` ✗

`$q = 'SELECT * FROM tbl WHERE id=' . esc_sql($_GET['id']);` ✗

`$q = 'SELECT * FROM tbl WHERE id="' . esc_sql($_GET['id']) . "'';` ✓

`$q = "SELECT * FROM tbl WHERE id='" . esc_sql($_GET['id']) . "'";` ✓

`$wpdb->prepare('SELECT * FROM tbl WHERE id = %d', $_GET['id'])` ✓

# Regular expressions

```
$id = 0;  
if (preg_match("#[a-zA-Z0-9]+#", $_GET['id'])) {  
    $id = $_GET['id']; ✗  
}
```

```
if (preg_match("#^[a-zA-Z0-9]+$#", $_GET['id'])) {  
    $id = $_GET['id']; ✓  
}
```

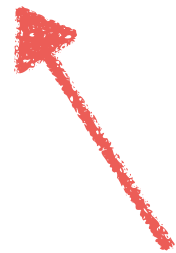
^ - beginning of the line

\$ - end of the line

# Ajax

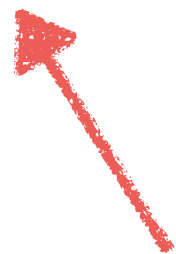
```
add_action('wp_ajax_nowa_akcja', 'nowa_akcja_funkcja');
```

```
do_action("wp_ajax_".$_REQUEST['action']);
```



For logged-in users

```
do_action("wp_ajax_nopriv_".$_REQUEST['action']);
```



For logged-out users

# Check capability

- `current_user_can()`
- `user_can()`
- `is_super_admin()`

# Strange names

**is\_admin()**

- <http://example.com/wp-admin/>

**is\_network\_admin()**

- <http://example.com/wp-admin/network/>



# 10 characters

```
if (current_user_can('delete_posts')) {  
    wp_delete_post($_GET['post_id'], TRUE ); ✗  
}
```

```

```

```
if (current_user_can('delete_posts')) {  
    check_ajax_referer('delete_post', $_GET['post_id']);  
    wp_delete_post($_GET['post_id'], TRUE ); ✓  
}
```



@kacperszurek

kacperszurek@gmail.com

http://security.szurek.pl