



SQL

SQL `add_post_meta();` `INSERT INTO wp_postmeta...`

`table` not found or type unknown

xkcd

SQL WordPress

`$wpdb` `$wpdb->prepare()`

SQL `$wpdb->prepare()` `sql_query()` `sql_query()`

```
$wpdb->get_var( $wpdb->prepare(
    "SELECT something FROM table WHERE foo = %s and status = %d",
    $name, // an unescaped string (function will do the sanitization for you)
    $status // an untrusted integer (function will do the sanitization for you)
) );
```

(XSS)

JavaScript (XSS)

XSS

URL

```

```

HTML HTML

```
$allowed_html = array(
    'a' => array(
        'href' => array(),
        'title' => array()
    ),
    'br' => array(),
    'em' => array(),
    'strong' => array(),
);

echo wp_kses( $custom_content, $allowed_html );
```

(CSRF)

CSRF sea-surf Web Work

HTML HTTP

```
<form method="post">
    <!-- some inputs here ... -->
    <?php wp_nonce_field( 'name_of_my_action', 'name_of_nonce_field' ); ?>
</form>
```

- [WordPress](#)
- [WordPress](#)
- [Web](#) (OWASP) 10

#2

Vcanson 20 2023 11:09:00

Vcanson 26 2023 15:34:10