http://midas/parentainment.com/spro_view_profile.php?mem_id=2

$_SERVER['HTTP_HOST'] ⇒ midas

$_SERVER['REQUEST_URI'] ⇒
/parentainment.com/spro_view_profile.php?mem_id=2

$_SERVER['SCRIPT_NAME'] ⇒
/parentainment.com/spro_view_profile.php

$_SERVER['PHP_SELF'] ⇒
/parentainment.com/spro_view_profile.php

$_SERVER['QUERY_STRING'] ⇒ mem_id=2

$_SERVER['HTTP_REFERER'] ⇒

phpinfo()

Outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

phpinfo() is also a valuable debugging tool as it contains all EGPCS (Environment, GET, POST, Cookie, Server) data.

getcwd()

Returns the current working directory.

uniqid()

Gives unique identifier based on the current time in microseconds.

Example:

```
$better_token = md5(uniqid(rand(),true));
(more better way to get a unique identifier)
```

nl2br()

Returns string with '
' inserted before all newlines.

Example:

```
<html><head></head><body>jitendra isn't<br>jitu</body></html>
```

Output:

jitendra isn't
jitu

```
<body><?php echo "jitendra isn't\n jitu"; ?></body>
```

Output: jitendra isn't jitu

```
<body><?php echo nl2br("jitendra isn't\n jitu");
```

Output:

jitendra isn't
jitu

```
<body><?php echo "jitendra isn't<br>jitu"; ?></body>
```

Output:

jitendra isn't
jitu

File Upload

```
if($_FILES['my_image']['name'] != '')
{
    list($width, $height, $image_type, $wh)
    = getimagesize($_FILES['my_image']['tmp_name']);
    if($image_type != '')
    {
        .....
        unlink();
        $file_tmp_name = $_FILES['my_image']['tmp_name'];
        $file_name = $_FILES['my_image']['name'];
        $file_path = md5(uniqid(rand(), true)).$file_name;
        copy($file_tmp_name, $file_path);
      or
        move_uploaded_file($file_tmp_name, $file_path);
    }
}
```

```
<form — enctype="multipart/form-data">
  <input type="file" name="my_image">
</form>
```

define()

Defines a named constant at runtime.

Example:

```
<?php
define("CONSTANT", "Hello world.");
echo CONSTANT;
echo Constant;
?>
```

Output:

```
Hello world.
Constant
```

Date
25/02/2017

XSS

If you embed strings within HTML markup, we must escape it with htmlspecialchars(). This means that every single echo or print statement (for ex. in zend framework for layout & template i.e. for every .phtml file) should use htmlspecialchars().