WWBN / AVideo Public

Code Issues 13 Pull requests Actions Projects Wiki Security a

Commit bf1c769

Daniel Neto committed last week · 11 / 11

fix: Improve captcha generation and validation logic for enhanced security

GHSA-hg7g-56h5-5pqr

master

1 parent ca70288 commit bf1c769

2 files changed +22 -19 lines changed

Top

Filter files...

objects

captcha.php

getCaptcha.php

2 files changed +22 -19 lines changed

Search within code

objects/captcha.php

```
@@ -29,9 +29,12 @@ public function getCaptchaImage()
29 29           $branco = imagecolorallocate($imagem, 255, 255, 255); // define a cor branca
30 30
31 31           // define a palavra conforme a quantidade de letras definidas no parametro $quantidade_letras
32    -          //$letters = 'AaBbCcDdEeFfGgHhIiJjKkLlMmNnPpQqRrSsTtUuVvYyXxWwZz23456789';
33 32           $letters = 'AaBbCcDdEeFfGgHhIiJjKkLlMmNnPpQqRrSsTtUuVvYyXxWwZz23456789';
34    -          $palavra = substr(str_shuffle($letters), 0, ($this->quantidade_letras));
   33 +          $len = strlen($letters);
   34 +          $palavra = '';
```

```
      35  +         for ($j = 0; $j < $this->quantidade_letras; $j++) {
      36  +             $palavra .= $letters[random_int(0, $len - 1)];
      37  +         }
35    38            if (User::isAdmin() && empty($_REQUEST['forceCaptcha'])) {
36    39                $palavra = "admin";
37    40            }
          @@ -57,19 +60,19 @@ public function getCaptchaImage()
57    60
58    61        public static function validation($word)
59    62        {
60        -         if (User::isAdmin() && $_SESSION["palavra"] === 'admin') {
61        -             return true;
62        -         }
63    63            _session_start();
64    64            if (empty($_SESSION["palavra"])) {
65    65                _error_log("Captcha validation Error: you type ({$word}) and session is empty - session_name ". session_name()." session_id: ". session_id());
66    66                return false;
67    67            }
68        -         $validation = (strcasecmp($word, $_SESSION["palavra"]) == 0);
      68  +         $stored = $_SESSION["palavra"];
      69  +         unset($_SESSION["palavra"]); // always consume on any attempt to prevent brute-force
      70  +         if (User::isAdmin() && $stored === 'admin') {
      71  +             return true;
      72  +         }
      73  +         $validation = (strcasecmp($word, $stored) === 0);
69    74            if (!$validation) {
70        -             _error_log("Captcha validation Error: you type ({$word}) and session is ({$_SESSION["palavra"]})- session_name ". session_name()." session_id: ". session_id());
71        -         } else {
72        -             unset($_SESSION["palavra"]); // Consume the captcha token to prevent reuse within the same session
      75  +             _error_log("Captcha validation Error: you type ({$word}) and session is ({$stored})- session_name ". session_name()." session_id: ". session_id());
73    76            }
74    77            return $validation;
75    78        }
      ...
```

objects/getCaptcha.php

```
@@ -1,10 +1,10 @@
- <?php
- require_once 'captcha.php';
-
- $largura = empty($_GET['l']) ? 120 : $_GET['l']; // recebe a largura
- $altura = empty($_GET['a']) ? 40 : $_GET['a']; // recebe a altura
- $tamanho_fonte = empty($_GET['tf']) ? 18 : $_GET['tf']; // recebe o tamanho da fonte
- $quantidade_letras = empty($_GET['ql']) ? 5 : $_GET['ql']; // recebe a quantidade de letras que o captcha terá
-
- $capcha = new Captcha($largura, $altura, $tamanho_fonte, $quantidade_letras);
- $capcha->getCaptchaImage();
+ <?php
+ require_once 'captcha.php';
+
+ $largura       = isset($_GET['l']) ? max(80,  min(400, (int)$_GET['l'])) : 120;
+ $altura        = isset($_GET['a']) ? max(20,  min(200, (int)$_GET['a'])) : 40;
+ $tamanho_fonte = isset($_GET['tf']) ? max(10,  min(40,  (int)$_GET['tf'])) : 18;
+ $quantidade_letras = isset($_GET['ql']) ? max(5, min(8, (int)$_GET['ql'])) : 5;
+
+ $capcha = new Captcha($largura, $altura, $tamanho_fonte, $quantidade_letras);
+ $capcha->getCaptchaImage();
```

Comments 0

Please sign in to comment.