WWBN / AVideo Public

Code Issues 13 Pull requests Actions Projects Wiki Security a

Commit bcba324

Daniel Neto committed last week · 11 / 11

```
fix: Enhance duration validation and output encoding to prevent XSS
vulnerabilities

GHSA-8pv3-29pp-pf8f
```

master

1 parent a0156a6 commit bcba324

3 files changed +12 -7 lines changed

Top

Filter files…

- objects
  - video.php
- view
  - include
    - playlist.php
    - trending.php

3 files changed +12 -7 lines changed

Search within code

objects/video.php

```
@@ -915,7 +915,10 @@ static function isValidDuration($duration)
915  915              if (empty($duration) || strtolower($duration) == "ee:ee:ee" ||
                      $duration == '0:00:00' || $duration == '00:00:00' || $duration ==
                      "0:00:00.000000") {
916  916                  return false;
917  917              }
```

```
918     -             return preg_match('/^[0-9]{1,2}:[0-9]{1,2}:[0-9]{1,2}/', $duration);
        918 +             // SECURITY: $ anchor is required — without it, arbitrary content after a valid
        919 +             // HH:MM:SS prefix passes validation and can be stored/rendered as XSS.
        920 +             // Optional decimal-seconds suffix (e.g. 00:01:23.456) is allowed.
        921 +             return preg_match('/^[0-9]{1,2}:[0-9]{1,2}:[0-9]{1,2}(\.[0-9]+)?$/', $duration);
919     922               }
920     923
921     924               public function getDuration()
        @@ -3477,7 +3480,9 @@ public static function getCleanDuration($duration = "")
3477    3480                  } elseif (count($durationParts) == 2) {
3478    3481                      return '0:' . static::addZero($durationParts[0]) . ':' . static::addZero($durationParts[1]);
3479    3482                  }
3480    -                 return $duration;
        3483 +                 // Reconstruct from parts instead of returning the raw string — defense in depth
        3484 +                 // against any malformed duration that may already be stored in the database.
        3485 +                 return static::addZero($durationParts[0]) . ':' . static::addZero($durationParts[1]) . ':' . static::addZero($durationParts[2]);
3481    3486              }
3482    3487              }
3483    3488
```

view/include/playlist.php

```
        @@ -69,7 +69,7 @@
69      69                width: 250px;
70      70                height: 100px;
71      71                margin-left: 5px;
72      -                 position: relative;
        72 +              position: relative;
73      73                display: flex;
```

```
74  74          justify-content: center;
75  75      }
        @@ -156,7 +156,7 @@
156 156                             <?php
157 157                             if ($value['type'] !== 'pdf' && $value['type'] !== 'article' && $value['type'] !== 'serie') {
158 158                             ?>
159     -                               <time class="duration"><?php echo Video::getCleanDuration(@$value['duration']); ?></time>
    159 +                               <time class="duration"><?php echo htmlspecialchars(Video::getCleanDuration(@$value['duration']), ENT_QUOTES, 'UTF-8'); ?></time>
160 160                               <div class="progress" style="height: 3px; margin-bottom: 2px;">
161 161                                   <div class="progress-bar progress-bar-danger" role="progressbar" style="width: <?php echo $value['progress']['percent'] ?>%;" aria-valuenow="<?php echo $value['progress']['percent'] ?>" aria-valuemin="0" aria-valuemax="100"></div>
162 162                               </div>
        @@ -235,4 +235,4 @@
235 235                 });
236 236             }
237 237         }
238     - </script>
    238 + </script>
```

view/trending.php

```
        @@ -69,7 +69,7 @@
69  69                                  <img src="<?php echo ImagesPlaceHolders::getVideoPlaceholder(ImagesPlaceHolders::$RETURN_URL); ?>" data-src="<?php echo $imgGif; ?>" style="position: absolute; top: 0; display: none;" alt="<?php echo str_replace('"', '', $value['title']); ?>" id="thumbsGIF<?php echo $value['id']; ?>" class="thumbsGIF img-responsive" height="196" />
70  70                                  <?php }
71  71                                  ?>
```

```
72      -                                   <time class="duration"><?php echo Video::getCleanDuration($value['duration']); ?></time>
        72  +                               <time class="duration"><?php echo htmlspecialchars(Video::getCleanDuration($value['duration']), ENT_QUOTES, 'UTF-8'); ?></time>
73      73                                  </div>
74      74                                  <div class="progress" style="height: 3px; margin-bottom: 2px;">
75      75                                      <div class="progress-bar progress-bar-danger" role="progressbar" style="width: <?php echo $value['progress']['percent'] ?>%;" aria-valuenow="<?php echo $value['progress']['percent'] ?>" aria-valuemin="0" aria-valuemax="100"></div>
        @@ -245,4 +245,4 @@
245     245     </script>
246     246     <?php
247     247     $_page->print();
248     -   ?>
        248 +   ?>
```

Comments 0

Please sign in to comment.