WWBN / **AVideo** Public

Code Issues 13 Pull requests Actions Projects Wiki Security a

Commit 5e2b897

Daniel Neto committed last week · ✓ 11 / 11

```
fix: Refactor CORS preflight handling for improved security and clarity

GHSA-ff5q-cc22-fgp4
```

master

1 parent caf705f commit 5e2b897

1 file changed +16 -14 lines changed

Top

Filter files…

plugin/API

router.php

1 file changed +16 -14 lines changed

Search within code

plugin/API/router.php

```
@@ -1,20 +1,22 @@
<?php

- // CORS handling - must be done before any other processing
- $HTTP_ORIGIN = empty($_SERVER['HTTP_ORIGIN']) ? @$_SERVER['HTTP_REFERER'] :
  $_SERVER['HTTP_ORIGIN'];
- if (empty($HTTP_ORIGIN)) {
-     header('Access-Control-Allow-Origin: *');
- } else {
-     header("Access-Control-Allow-Origin: " . $HTTP_ORIGIN);
- }
- header("Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS, HEAD");
```

```
11      - header("Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-
          With, ua-resolution, APISecret, Origin, Accept, Access-Control-Request-Method,
          Access-Control-Request-Headers");
12      - header('Access-Control-Allow-Private-Network: true');
13      -
14      - // Handle preflight OPTIONS request immediately
      3 + // CORS preflight handling.
      4 + // OPTIONS preflights are cross-origin by definition (same-origin requests are
          never
      5 + // preflighted by browsers). Returning Access-Control-Allow-Origin: * without
      6 + // Access-Control-Allow-Credentials is safe:
      7 + //   - External API clients using APISecret (non-credentialed) proceed normally.
      8 + //   - Credentialed attacker requests are blocked: the browser sees no
      9 + //     Allow-Credentials:true in the preflight and aborts the actual request,
     10 + //     so session cookies are never sent.
     11 + // Actual GET/POST responses are handled by allowOrigin(true) in
          get/set.json.php
     12 + // which enforces same-origin-only credentials (fixed in commit 986e64aad).
15   13   if ($_SERVER['REQUEST_METHOD'] === 'OPTIONS') {
16      -     header("Access-Control-Max-Age: 86400"); // Cache preflight for 24 hours
17      -     http_response_code(200);
     14 +     header('Access-Control-Allow-Origin: *');
     15 +     header('Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS,
          HEAD');
     16 +     header('Access-Control-Allow-Headers: Content-Type, Authorization, X-
          Requested-With, ua-resolution, APISecret, Origin, Accept, Access-Control-
          Request-Method, Access-Control-Request-Headers');
     17 +     header('Access-Control-Allow-Private-Network: true');
     18 +     header('Access-Control-Max-Age: 86400');
     19 +     http_response_code(204);
18   20       exit;
19   21   }
20   22
```

Comments 0

Please sign in to comment.