openedx / **openedx-platform** Public

Code | Issues 350 | Pull requests 166 | Actions | Security and quality 10

Commit 76462f1

feanil authored 4 days ago · 46 / 46 · Verified

```
Merge commit from fork

The view_survey endpoint accepted a redirect_url GET parameter and passed
it directly to HttpResponseRedirect() with no validation. If a non-existent
survey name was requested, this produced an immediate 302 to an
attacker-controlled URL. If a valid survey was requested, the same URL was
embedded in a hidden _redirect_url form field; after submission, submit_answers
echoed it back in JSON and client-side JS used it as location.href — a second
unvalidated redirect path.

Fix both by ignoring user-supplied redirect URLs entirely:
- view_survey no longer reads redirect_url from GET params
- submit_answers always redirects to reverse('dashboard') rather than
  reading _redirect_url from the POST body

Note: view_student_survey retains its redirect_url parameter because it is
also called from the courseware view (courseware/views/views.py), which passes
a server-controlled course_home_url. That call path is unaffected.

Fixes: GHSA-2843-x998-f8r2

BREAKING CHANGE: The redirect_url GET parameter on /survey/<name>/ is no longer
honored. Requests that previously redirected to a caller-specified URL after
survey completion will now always redirect to the dashboard.
```

master

1 parent 9b642be commit 76462f1

1 file changed +2 -6 lines changed

Top

Filter files…

lms/djangoapps/survey

views.py

1 file changed +2 -6 lines changed

Search within code

lms/djangoapps/survey/views.py

```
@@ -26,9 +26,7 @@ def view_survey(request, survey_name):
26 26       """
27 27       View to render the survey to the end user
28 28       """
29    -     redirect_url = request.GET.get('redirect_url')
30    -
31    -     return view_student_survey(request.user, survey_name,
      redirect_url=redirect_url)
   29 +     return view_student_survey(request.user, survey_name)
32 30
33 31
34 32   def view_student_survey(user, survey_name, course=None, redirect_url=None,
      is_required=False, skip_redirect_url=None):
@@ -88,9 +86,7 @@ def submit_answers(request, survey_name):
88 86           array_val = request.POST.getlist(key)
89 87           answers[key] = request.POST[key] if len(array_val) == 0 else
      ','.join(array_val)
90 88
91    -     # the URL we are supposed to redirect to is
92    -     # in a hidden form field
93    -     redirect_url = answers['_redirect_url'] if '_redirect_url' in answers else
      reverse('dashboard')
   89 +     redirect_url = reverse('dashboard')
94 90
95 91       course_key = CourseKey.from_string(answers['course_id']) if 'course_id' in
      answers else None
96 92
```

Comments 0

Please sign in to comment.