New issue

Jump to bottom

Reflected Xss #44

⊘ Closed **Tr3jer** opened this issue on May 21, 2020 · 3 comments

---

Tr3jer commented on May 21, 2020 • edited ▾

Hi Team

I found a reflected xss vulnerability.

routes/base.py

```
def query_string():
    """Returns a sanitized query string."""

    rejected_keys = [
        'space_id',
        'delivery_token',
        'preview_token',
        'editorial_features'
    ]
    args = {k: v for k, v
            in request.args.items()
            if k not in rejected_keys}

    if not args:
        return ''
    return '?{0}'.format(
        '&'.join(
            '{0}={1}'.format(k, v) for k, v
            in args.items()
        )
    )
```

Proof of concept:

```
https://the-example-app-py.contentful.com/?cda'"<evil><script>alert(1)</script>&locale=locale=de-DE


{'api': 'cda\'"<script>alert(1)</script>', 'locale': 'en-US'}


Searching 24 files for "{{ query_string }}" (regex)

/Users/CongRong/github/the-example-app.py/views/course.dhtml:
   17                    <div class="table-of-contents__item">
   18                        <a
   19:                           href="/courses/{{ course.slug }}{{ query_string }}"
   20                            class="table-of-contents__link {{ 'visited' if course.id in visited_lessons else '' }} {{ 'active' if not lesson else '' }}"
   21                            >{{ 'courseOverviewLabel'|trans(current_locale.code) }}</a>
   ..
   26                        <div class="table-of-contents__item">
   27                            <a
   28:                               href="/courses/{{ course.slug }}/lessons/{{ course_lesson.slug }}{{ query_string }}"
   29                                class="table-of-contents__link {{ 'visited' if course_lesson.id in visited_lessons else '' }} {{ 'active' if lesson and
course_lesson.id == lesson.id else '' }}"
   30                                >{{ course_lesson.title }}</a>
   ..
   76                        <div class="course__overview-cta-wrapper">
   77                            <a
   78:                               href="/courses/{{ course.slug}}/lessons/{{ next_lesson.slug }}{{ query_string }}"
   79                                class="course__overview-cta cta"
   80                                >{{ 'startCourseLabel'|trans(current_locale.code) }}</a>

/Users/CongRong/github/the-example-app.py/views/course.html:
   17                    <div class="table-of-contents__item">
   18                        <a
   19:                           href="/courses/{{ course.slug }}{{ query_string }}"
   20                            class="table-of-contents__link {{ 'visited' if course.id in visited_lessons else '' }} {{ 'active' if not lesson else '' }}"
   21                            >{{ 'courseOverviewLabel'|trans(current_locale.code) }}</a>
   ..
   25                        <div class="table-of-contents__item">
   26                            <a
   27:                               href="/courses/{{ course.slug }}/lessons/{{ course_lesson.slug }}{{ query_string }}"
   28                                class="table-of-contents__link {{ 'visited' if course_lesson.id in visited_lessons else '' }} {{ 'active' if lesson and course_lesson.id
== lesson.id else '' }}"
   29                                >{{ course_lesson.title }}</a>
   ..
   74                        <div class="course__overview-cta-wrapper">
   75                            <a
   76:                               href="/courses/{{ course.slug}}/lessons/{{ next_lesson.slug }}{{ query_string }}"
   77                                class="course__overview-cta cta"
   78                                >{{ 'startCourseLabel'|trans(current_locale.code) }}</a>

/Users/CongRong/github/the-example-app.py/views/courses.dhtml:
   16                    <ul class="sidebar-menu__list">
   17                        <li class="sidebar-menu__item">
   18:                           <a href="/courses{{ query_string }}" class="sidebar-menu__link {{ '' if current_category else 'active' }}">{{
'allCoursesLabel'|trans(current_locale.code) }}</a>
   19                        </li>
   20
   ..
   22                        <li class="sidebar-menu__item">
```

```
    23                              <a
    24:                                 href="/courses/categories/{{ category.slug }}{{ query_string }}"
    25                                  class="sidebar-menu__link {{ 'active' if current_category and current_category.id == category.id else '' }}"
    26                              >{{ category.title }}</a>

/Users/CongRong/github/the-example-app.py/views/courses.html:
    16                      <ul class="sidebar-menu__list">
    17                          <li class="sidebar-menu__item">
    18:                              <a href="/courses{{ query_string }}" class="sidebar-menu__link {{ '' if current_category else 'active' }}">{{
        'allCoursesLabel'|trans(current_locale.code) }}</a>
    19                          </li>
    20

    ..
    22                              <li class="sidebar-menu__item">
    23                                  <a
    24:                                     href="/courses/categories/{{ category.slug }}{{ query_string }}"
    25                                      class="sidebar-menu__link {{ 'active' if current_category and current_category.id == category.id else '' }}"
    26                                  >{{ category.title }}</a>

/Users/CongRong/github/the-example-app.py/views/layout.dhtml:
    147
    148            <div class="header__upper-menu">
    149:             <a href="/settings{{ query_string }}">{{ 'settingsLabel'|trans(current_locale.code) }}</a>
    150            </div>
    151          </div>
    ...
    155        <div class="header__lower layout-centered">
    156          <div class="header__logo">
    157:           <a class="header__logo-link" href="/{{ query_string }}">
    158              <img src="{{ url_for('static', filename='images/the-example-app-logo-python.svg') }}" alt="{{ 'logoAlt'|trans(current_locale.code) }}" />
    159            </a>
    ...
    163            <ul>
    164              <li>
    165:               <a class="{{ 'active' if current_path == '/' else '' }}" href="/{{ query_string }}">{{ 'homeLabel'|trans(current_locale.code) }}</a>
    166              </li>
    167              <li>
    168:               <a class="{{ 'active' if current_path.startswith('/courses') else '' }}" href="/courses{{ query_string }}">{{ 'coursesLabel'|trans(current_locale.code) }}</a>
    169              </li>
    170            </ul>
    ...
    186            <ul>
    187              <li>
    188:               <a class="{{ 'active' if current_path == '/' else '' }}" href="/{{ query_string }}">{{ 'homeLabel'|trans(current_locale.code) }}</a>
    189              </li>
    190              <li>
    191:               <a class="{{ 'active' if current_path.startswith('/courses') else '' }}" href="/courses{{ query_string }}">{{ 'coursesLabel'|trans(current_locale.code) }}</a>
    192              </li>
    193            </ul>
    ...
    216              {{ 'footerDisclaimer'|trans(current_locale.code) }} 
    217              <a href="https://github.com/contentful/the-example-app.php" target="_blank" rel="noopener">{{ 'viewOnGithub'|trans(current_locale.code) }}</a>. 
    218              <a href="/imprint{{ query_string }}">{{ 'imprintLabel'|trans(current_locale.code) }}</a>. 
    219              <a href="https://www.contentful.com/contact/">{{ 'contactUsLabel'|trans(current_locale.code) }}</a>.
    220            </p>

/Users/CongRong/github/the-example-app.py/views/partials/breadcrumb.dhtml:
     3          {% for crumb in breadcrumbs -%}
     4            <li>
     5:             <a href="{{ crumb['url'] }}{{ query_string }}">{{ crumb['label'] }}</a>
     6            </li>
     7          {%- endfor %}

/Users/CongRong/github/the-example-app.py/views/partials/breadcrumb.html:
     3          {% for crumb in breadcrumbs -%}
     4            <li>
     5:             <a href="{{ crumb['url'] }}{{ query_string }}">{{ crumb['label'] }}</a>
     6            </li>
     7          {%- endfor %}

/Users/CongRong/github/the-example-app.py/views/partials/courseCard.dhtml:
     4          {% for category in course.categories %}
     5            <div class="course-card__category">
     6:             <a class="course-card__category-link" href="/courses/categories/{{ category.slug }}{{ query_string }}">{{ category.title }}</a>
     7            </div>
     8          {% endfor %}
     .
    11
    12      <h2 class="course-card__title">
    13:       <a href="/courses/{{ course.slug }}{{ query_string }}">{{ course.title }}</a>
    14        {% if should_show_entry_state(course, current_api['id']) %}
    15          <div class='editorial-features'>
    ..
    22
    23      <div class="course-card__link-wrapper">
    24:       <a href="/courses/{{ course.slug }}{{ query_string }}" class="course-card__link">{{ 'viewCourseLabel'|trans(current_locale.code) }}</a>
    25      </div>
    26  </div>

/Users/CongRong/github/the-example-app.py/views/partials/lesson.dhtml:
    35
    36      {% if next_lesson %}
    37:       <a href="/courses/{{ course.slug }}/lessons/{{ next_lesson.slug }}{{ query_string }}" class="lesson__cta cta">{{ 'nextLessonLabel'|trans(current_locale.code) }}</a>
    38      {% endif %}
    39  </div>

/Users/CongRong/github/the-example-app.py/views/partials/lesson.html:
    35
    36      {% if next_lesson %}
    37:       <a href="/courses/{{ course.slug }}/lessons/{{ next_lesson.slug }}{{ query_string }}" class="lesson__cta cta">{{ 'nextLessonLabel'|trans(current_locale.code) }}</a>
    38      {% endif %}
    39  </div>

/Users/CongRong/github/the-example-app.py/views/partials/moduleCopy.dhtml:
    14      <div class="module-copy__second{{ style }}">
    15          {% if module.cta_title and module.cta_link %}
    16:             <a href="{{ module.cta_link }}{{ query_string }}" class="cta module-copy__cta{{ style }}">{{ module.cta_title }}</a>
    17          {% endif %}
    18      </div>

/Users/CongRong/github/the-example-app.py/views/partials/moduleHighlightedCourse.dhtml:
     9              <div class="module-highlighted-course__categories">
    10                  {% for category in course.categories %}
```

```
   11:                          <a href="/courses/categories/{{ category.slug }}{{ query_string }}" class="module-highlighted-course__category">{{ category.title }}</a>
   12                        {% endfor %}
   13                  </div>
   ..
   15
   16            <h2 class="module-highlighted-course__title">
   17:              <a href="/courses/{{ course.slug }}{{ query_string }}">{{ course.title }}</a>
   18            </h2>
   19

   ..
   23
   24            <div class="module-highlighted-course__link-wrapper">
   25:              <a href="/courses/{{ course.slug }}{{ query_string }}" class="module-highlighted-course__link">{{ 'viewCourseLabel'|trans(current_locale.code) }}</a>
   26            </div>
   27        </div>

   /Users/CongRong/github/the-example-app.py/views/settings.dhtml:
   86                          </p>
   87
   88:                          <form method="post" action="/settings/reset{{ query_string }}">
   89                              <p>
   90                                  <strong>{{ "applicationCredentialsLabel"|trans(current_locale.code) }}:</strong><br />
   ..
  102        {% endif %}
  103
  104:      <form action="/settings{{ query_string }}" method="POST" class="form">
  105          <div class='form-item'>
  106              <label for="input-space-id">{{ 'spaceIdLabel'|trans(current_locale.code) }}</label>

   30 matches across 13 files
```

---

gkijko mentioned this issue on Jun 16, 2020

Contrib/fix xss url args #45
〔⤷ Merged〕

---

gkijko commented on Jun 17, 2020   〔Contributor〕

@Tr3jer Could you check this pull request: #42 to validate that it fixes this issue?

Tr3jer commented on Jun 17, 2020   〔Author〕

@gkijko Yes, it has been fixed.

Tr3jer closed this as completed on Jun 17, 2020

---

gkijko commented on Jun 17, 2020   〔Contributor〕

@Tr3jer the PR is not yet merged or reviewed though.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants