Rails XSS & Security Cheat-sheet

XSS Vulnerabilities in Rails applications

In a typical Rails application, indiscriminate use of the `html_safe` method is one of the most common causes of stored XSS vulnerabilities.

Using `html_safe` directly on user input should be avoided. Use `sanitize` instead

DO NOT:
```
<%= @user_input.html_safe %>
```

DO:
```
<%= sanitize(@user_input, tags: %w(strong) %>
```

If you need to use `html_safe` to incorporate styling to strings derived from user input, make sure you only mark trusted strings as `html_safe`

DO NOT:
```
<%= link_to "<i class='fa fa-user'></i> #
{user.name}”.html_safe, users_path(user) %>
```

DO:
```
<%= link_to "<i class='fa fa-user'></i> ".html_safe + "#
{user.name}", users_path(user) %>
```

Keep In Mind: A `<script>` tag is just one of the many ways Javascript can be inserted into your app. HTML attributes offer another huge attack surface for XSS. Attributes like `onmouseover`, `onclick`, and others can just as easily trigger malicious Javascript if exploited.

What about HTTPOnly?
By default, Rails sets the HTTPOnly flag on session cookies. This flag will prevent Javascript from accessing the cookie with `document.cookie`. While this might seem like all the protection you need against XSS attacks, consider the fact that via an XSS vulnerability an attacker can induce a logged-in user to perform any action on the site via Javascript. For example, a logged-in admin can be forced to upgrade the attacker's user account to 'admin'.

General Security Recommendations

- Run `bundler-audit` regularly
- Before you run `bundler-audit`, run `bundle-audit update`. This will ensure that the latest security advisories are accounted for.
- Run brakeman regularly
- Install Rack Attack
- Incorporate bundler-audit and brakeman into your CI
- Finally, invest some time on a regular basis (perhaps a couple of hours a week) learning something new about security. A good way to get started: load up a Rails application with a known vulnerability and figure out how you can exploit it!

Interested in learning more about security in Rails? Email me at sidk@ducktypelabs.com and let me know what you'd like to learn about.