RIT Web Environment | **Web Form Security Standard**

Summary ITS receives thousands of spam and malicious upload attempts on the RIT Web Environment. As the Administrator of the RIT Web Environment, ITS has developed the following policy applicable to any website hosted on the RIT Web Hosting Environment. ITS reserves the right to temporarily or permanently disable any website that does not meet the required, specific criteria outlined in this document.

If your website has been disabled, it is likely due to one or more of the following reasons:

- It is victim to external or internal spamming or phishing.
- It has been deemed by or reported to ITS as a security risk.
- It does not properly implement the reCAPTCHA service and/or Honeypot Technique
- It does not properly restrict file type uploads for anonymous users
- It violates the criteria outlined in this document.

1. Overview

To mitigate spam attempts ITS has approved and adopted the use of the following technologies:

- reCAPTCHA
  - reCAPTCHA is a free service that protects your website from spam and abuse that uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities on your site.
- Honeypot Technique
  - The honeypot technique is a fast, effective way to prevent spambots from submitting web forms. Spambots love form input fields and when they encounter one they will fill it out, even if the field is hidden from the user interface. To leverage this, you can create a form field that should be left blank, but hide it from human users. When the form is submitted you can check to see if there's a value for the field and if there is, block the form submission.

To mitigate malicious file uploads ITS has limited the types of files that may be uploaded as part of a web form submission by **anonymous** (not authenticated) users. The following file types are **not allowed:**

- gif,jpg,png
- bmp,eps,tif,pict,psd
- txt,rtf,html,odt,ppt,pptx,odp,xls,xlsx,ods,xml
- avi,mov,mp3,ogg,wav
- Bz2,dmg,gz,jar,rar,sit,tar,zip

The following file types are allowed for anonymous users:

- Pdf,doc,docx

Web forms that require a user to authenticate before submitting have no file type restrictions.

What is considered a web form on the RIT Web Environment, thus requiring use of an approved spam or malicious upload mitigation technique? Web forms include but are not limited to:

- Any input field that a user may fill out and submit through your site
- E-mail or newsletter sign-up fields
- Contact forms
- Cart/Checkout forms

What is not considered a input field web form?

- Search text field

2. Web Form Security Standard

As the Administrator of the RIT Web Environment, ITS requires that all websites under the rit.edu domain using a web form follow the requirements outlined in this document, and reserves the right to disable any site that falls victim to spam and/or poses a security risk. Other methods may be implemented after ITS assessment and approval.

3. Drupal Websites on the RIT Web Hosting Environment

As of January 12, 2017, reCAPTCHA and Honeypot have been configured on all Drupal websites for web forms on the RIT Web Environment.
As of January 1, 2018, all web forms that allow anonymous users to submit must restrict the file type uploads to the list referred to in section 1.

Actions taken by ITS:

1. All current Staging and Production Drupal websites using web forms are now secured. No action is needed from Web Developers or Site Owners
2. All new Drupal websites created after January 12, 2017 will automatically have reCAPTCHA and Honeypot configured in Staging and Production environments.

4. All Other Websites on the RIT Web Hosting Environment

As of January 12, 2017, reCAPTCHA and Honeypot **must be** configured on web forms in all websites on the RIT Web Environment.

If your site is reported to be non-compliant or is targeted by spambots, **ITS reserves the right to disable your site until approved spam mitigation technology and techniques are implemented.** Web Developers and/or Site Owners may be responsible for configuration and implementation themselves. Refer the Site Owner's Rights and Responsibilities or ITS Web Environment Statement of Service for more information.

Version	Date Created	Author	Comments
Draft 0.3	01/05/2018	C. Nairn	Title change, File type uploads for anon, forms added
Draft 0.2	01/27/2017	C. Nairn	Draft edits
Draft 0.1	01/27/2017	J. Hoeltke	Initial Draft