How to Create a Custom Response Page

https://campus.barracuda.com/doc/45025648/

The Barracuda Web Application Firewall provides a predefined set of HTML pages that are used by the relevant modules as responses. The response pages are used in the following modules:

- **SECURITY POLICIES > Global ACLs** - if **Deny Response** is set to **Response Page**.
- **SECURITY POLICIES > Action Policy** - if **Deny Response** is set to **Send Response**.
- **WEBSITES > Allow/Deny > URL : Allow/Deny Rules** - if **Deny Response** is set to **Response Page**.
- **ACCESS CONTROL > Authentication Policies** - To capture user login credentials, or to handle various error conditions.

These response pages can be customized according to your requirement, or you can create a response page with a custom message (i.e. error message, attack information, a unique ID, etc.) to display to users. A custom response page can be configured in the **ADVANCED > Libraries** > **Response Pages** section, and then associated with the appropriate module. A response page can include:

- An error message if a user violates a configured security policy.
- A login/challenge page to authenticate/authorize a user.
- A CAPTCHA and challenging the user to respond.

Steps to Create a Custom Response Page

1. Go to the **ADVANCED > Libraries** page, **Response Pages** section and click **Add Response Page**.
2. On the **Add Response Page** window, specify values for the following:
   - **Response Page Name** – Enter a name for the response page.
   - **Type** – Select the type of response page you want to create.
     - **Error Pages** – Response pages displayed in relevant modules when the request is blocked due to violation of configured security policies.
     - **CAPTCHA Pages** – Response pages displayed in relevant modules where the user needs to be challenged with a CAPTCHA.
     - **Access Control Pages** – Response pages displayed when authentication and authorization is enabled for a service.
     - **Other Pages** – Response pages to use in any module.
   - **Status Code** – Enter an HTTP status code for the response page. Examples: 404 Not Found, 200 OK, 302 Found, etc.
   - **Headers** – Enter the response headers for the response page. Examples:
     - Allow - Request method (GET, POST, etc.) the server supports.
     - Content-type - Content type of the resource (such as text/HTML).
     - Connection - Options specified for a particular connection that must not be

communicated by proxies over further connections.
        - Location - Location for client to retrieve the document.
        - Refresh - Refresh time in seconds the browser asks for an updated page.
        - X-Frame-Options - Set the header value to DENY or SAMEORIGIN to enable clickjacking protection for the response page.
        - X-Content-Type-Options - Set the header value to text or HTML or nosniff to enable clickjacking protection for the response page.
    - **Body** – Response body for the response page. This is the HTML source of the response page that will be displayed to the client.

      -This feature is applicable ONLY for error pages.
      -The maximum number of characters that can be added to the response body is 65535.

      The following macros are supported when you create an error response page. When the error response page displays, these macros are replaced by the following information:
        1. %action-id - attack ID of the violation which resulted in the response page displaying.
        2. %host - host header which sent the request.
        3. %s - URL of the request which caused the violation.
        4. %client-ip - Client IP of the request which caused the violation.
        5. %attack-time - time at which the violation occurred.
        6. %attack-name - attack name of the violation resulting in the response page displaying.
        7. %log-id - unique ID of the Web Firewall Log, generated due to a violation in the request. The client is presented with a response page including the unique ID.
3. Click **Save**.

Additional Information

You can also embed an image in the response page. The image size to be embedded in the response page should not exceed 12 KB. To embed an image, do the following:

- Convert the image to base64 using openssl or any other utility
    - For eg: openssl base64 -in barracuda.jpg -out barracuda-jpg.b64
- Embed the base64 encoded image into a html with the "img" tag.
    - For eg: <html><img src="data:image/jpeg;base64,[BASE64 ENCODED IMAGE] alt="Test"/></html>

To use your trademark, copyright, or registered symbol in the response page, use the following HTML codes:

- &reg; - Registered
- &#8482; - Trademark
- &copy; - Copyright

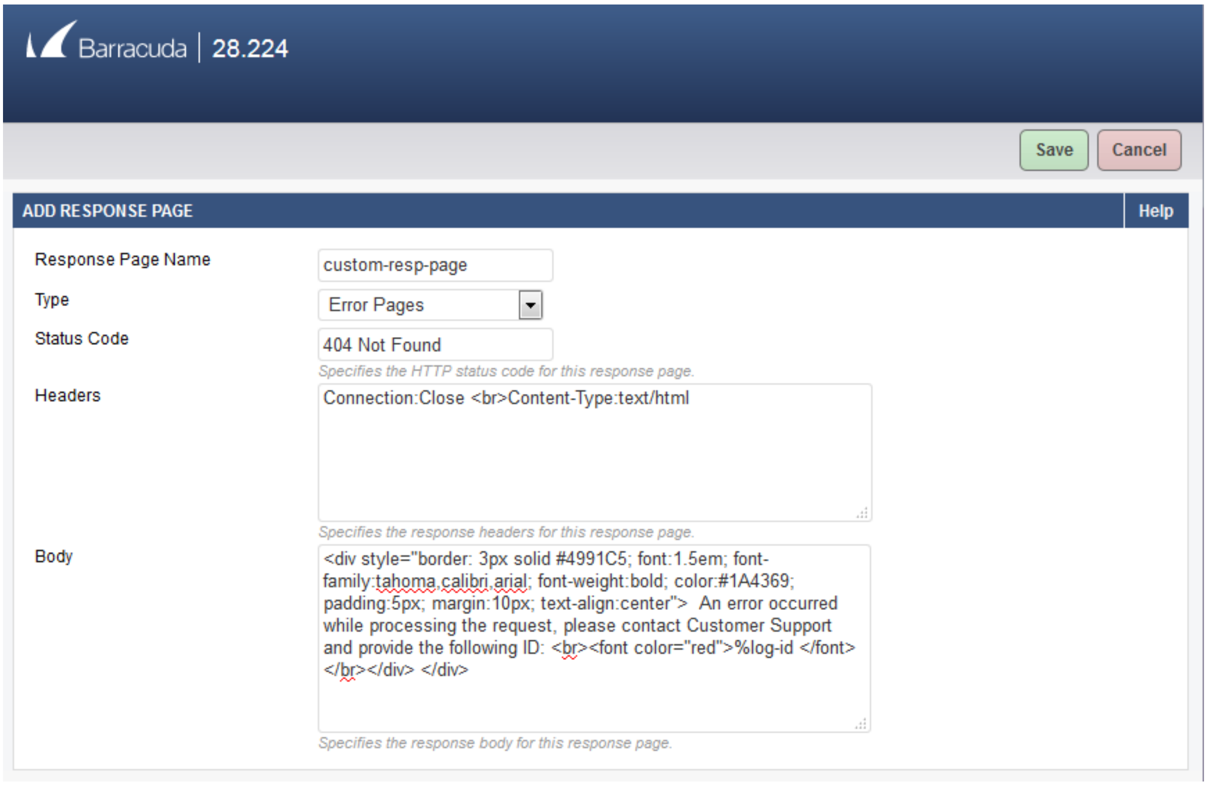
When editing the response pages for CAPTCHA related pages, note that the captcha.gif, captcha_resp, and captcha_resp_txt are internally recognized hard coded resources and should not be changed for the CAPTCHA functionality to work properly.

Example:

Scenario: You want to present a custom response page to the user if a cross site scripting error is detected by a service using the **default security policy** of the Barracuda Web Application Firewall.

In this example, we create a custom response page named **custom-resp-page** associated with the **Cross-Site Scripting Parameter** attack under the default policy on the **SECURITY POLICIES > Action Policy** page. In this example, the default policy is associated with the service (www.test.com). If a request injected with a client-side script is sent to the service (test.com), the Barracuda Web Application Firewall detects the attack and sends the response page associated with the violation.

1. Go to the **ADVANCED > Libraries** page, **Response Pages** section and click **Add Response Page**.
2. On the **Add Response Page** window, specify values for the following fields:
   1. **Response Page Name** - custom-resp-page
   2. **Type** - Error Pages
   3. **Status Code** - 404 Not Found
   4. **Headers** - Connection:Close &lt;br&gt;Content-Type:text/html
   5. **Body** - *<div style="border: 3px solid #4991C5; font:1.5em; font-family:tahoma,calibri,arial; font-weight:bold; color:#1A4369; padding:5px; margin:10px; text-align:center"> An error occurred while processing the request, please contact Customer Support and provide the following ID: <br><font color="red">%log-id </font></br></div> </div>*
3. Click **Save**.



Response Page Name: custom-resp-page

Type: Error Pages

Status Code: 404 Not Found

Specifies the HTTP status code for this response page.

Headers: `Connection:Close <br>Content-Type:text/html`

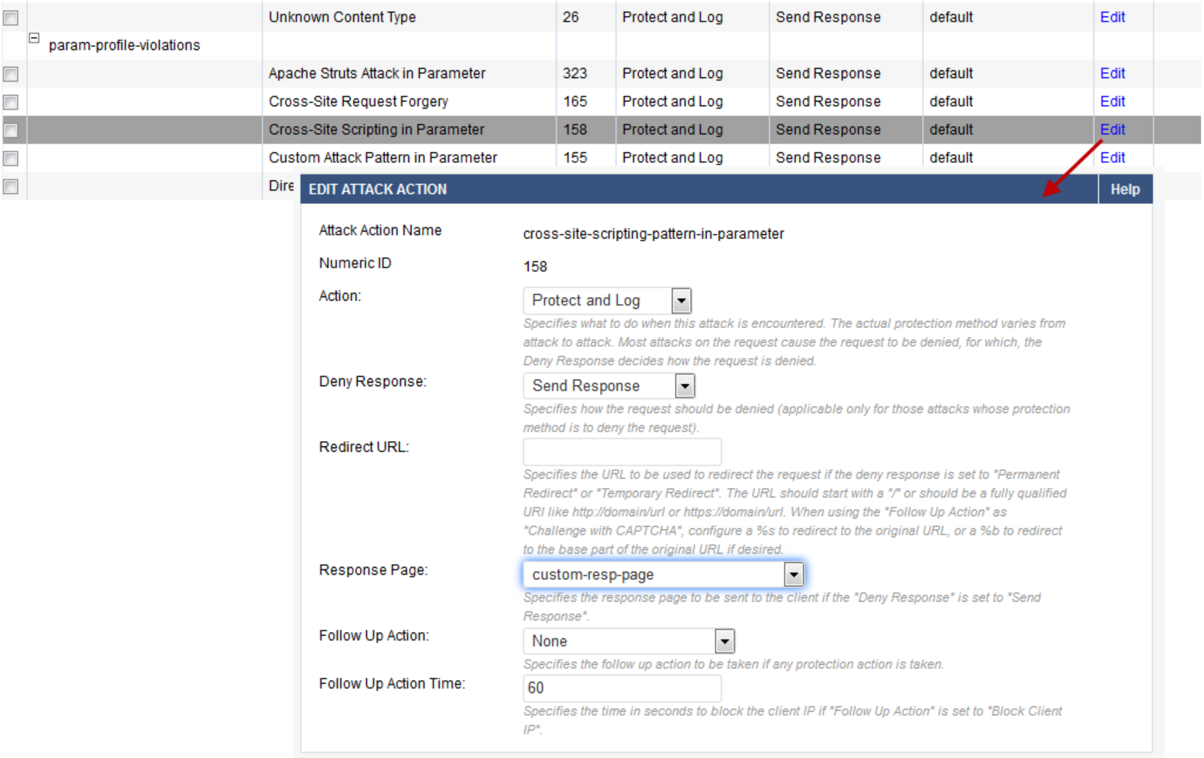
Specifies the response headers for this response page.

Body:

```
<div style="border: 3px solid #4991C5; font:1.5em; font-family:tahoma,calibri,arial; font-weight:bold; color:#1A4369; padding:5px; margin:10px; text-align:center">  An error occurred while processing the request, please contact Customer Support and provide the following ID: <br><font color="red">%log-id </font></br></div> </div>
```

Specifies the response body for this response page.

4. Go to the **SECURITY POLICIES > Action Policy** page, and click **Edit** next to **Cross-Site Scripting in Parameter**.
5. On the **Edit Attack Action** window:
    1. **Action** – Select Protect and Log.
    2. **Deny Response** – Select Send Response.
    3. **Response Page** – Select the response page (custom-resp-page) you created in step **2**.
    4. Click **Save**.



☐		Unknown Content Type	26	Protect and Log	Send Response	default	Edit
	⊟ param-profile-violations						
☐		Apache Struts Attack in Parameter	323	Protect and Log	Send Response	default	Edit
☐		Cross-Site Request Forgery	165	Protect and Log	Send Response	default	Edit
☐		Cross-Site Scripting in Parameter	158	Protect and Log	Send Response	default	Edit
☐		Custom Attack Pattern in Parameter	155	Protect and Log	Send Response	default	Edit
☐		Dire					

EDIT ATTACK ACTION Help

Attack Action Name: cross-site-scripting-pattern-in-parameter

Numeric ID: 158

Action: Protect and Log

Specifies what to do when this attack is encountered. The actual protection method varies from attack to attack. Most attacks on the request cause the request to be denied, for which, the Deny Response decides how the request is denied.

Deny Response: Send Response

Specifies how the request should be denied (applicable only for those attacks whose protection method is to deny the request).

Redirect URL:

Specifies the URL to be used to redirect the request if the deny response is set to "Permanent Redirect" or "Temporary Redirect". The URL should start with a "/" or should be a fully qualified URI like http://domain/url or https://domain/url. When using the "Follow Up Action" as "Challenge with CAPTCHA", configure a %s to redirect to the original URL, or a %b to redirect to the base part of the original URL if desired.

Response Page: custom-resp-page

Specifies the response page to be sent to the client if the "Deny Response" is set to "Send Response".

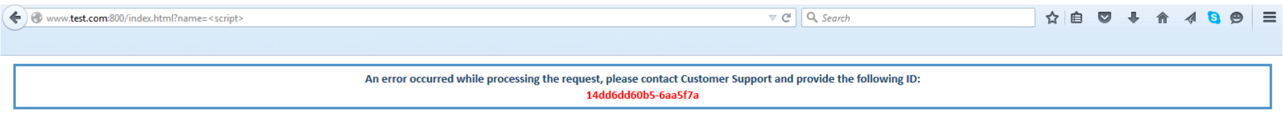
Follow Up Action: None

Specifies the follow up action to be taken if any protection action is taken.

Follow Up Action Time: 60

Specifies the time in seconds to block the client IP if "Follow Up Action" is set to "Block Client IP".

6. Repeat step **5** for other cross site scripting attacks (i.e. Cross-Site Scripting in Header, Cross-Site Scripting in URL and Cross Site Scripting in JSON Data) on the **SECURITY POLICIES > Action Policy** page.
7. Now, open a web browser and type http://www.test.com:800/index.html?name=<script>
8. You will see the configured response page.



www.test.com:800/index.html?name=<script>

An error occurred while processing the request, please contact Customer Support and provide the following ID:
14dd6dd60b5-6aa5f7a

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.