Detecting website defacement using Application Layer Health Check

https://campus.barracuda.com/doc/79465572/

The Application Layer Health check is configured to detect possible changes to the website content that may occur due to defacement. For configuring this, perform the following steps:

1. On the **BASIC > Services** page, click **Edit** next to the server. The **Server Configuration** window appears.
2. Navigate to the **Application Layer Health Checks** section and configure the following fields:
    1. **URL** - Enter the URL for which you want to monitor the health of the server. For example, /index.html is recommended which is the main page of the website.
    2. **Method** – Select the HTTP method to be used for the request from the drop-down list.
    3. **Additional Headers** – Enter any additional headers you want to send with the OOB HTTP request. The headers should be specified with the following format: *<header name>: <header value>*. The Barracuda Web Application Firewall inserts the specified headers in the request while sending OOB HTTP requests to the server. Each header should be added on a separate line. For example:
    <header1>: <value1>
    <header2>: <value2>.
    4. **Status Code** – Specify the expected HTTP response status code when accessing the URL. Any other status code is considered to be unsuccessful, and will result in setting the server as 'out-of-service'. Typically, a status code of 200 is used to indicate a successful response, but in some cases, 300, 301 and 302 may also be considered successful (these status codes indicate redirect responses).
    5. **Match Content String** – Enter a string that is found in the response page of a specific URL. This string can be any text that is in the response. The absence of this string is considered as defacement. When the configured string is not returned in the server response, WAF detects that the page has been defaced and mark the server down. An error page can be configured that gets displayed when the page is marked down to avoid displaying of the defaced webpage.
    1. **Domain** – Enter the SNI domain to be used to access the back-end server for application level health check. This connection is established only when the field “Enable SNI” is set to “Yes”.