

## - DISCLOSED VULNERABILITY REPORT -

By Prv | [mail](#) | [github](#) | [bugcrowd](#) |

**Name:** Broken Link Hijacking vector due to expired link shortening service

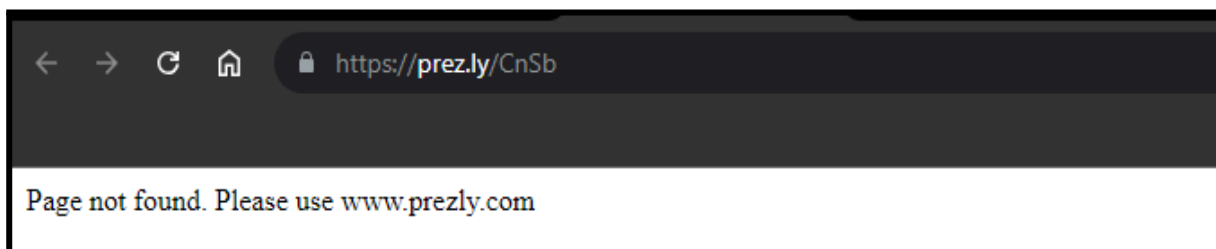
**Vulnerability type:** Server side injection | Recurring Broken link hijack ([BLH](#))

**Severity:** **Medium**

### Overview:

This vulnerability was discovered when a link shown at the main page of a popular crypto currency trading platform, led to a 404 error linked to an external service.

Although the links themselves on the material of the website where valid, the shortening service used on the website had become invalidated, leading to a 404 Error page:



These links were found throughout the index page of the website, and had all came from the same expired service used to host the external Resources:

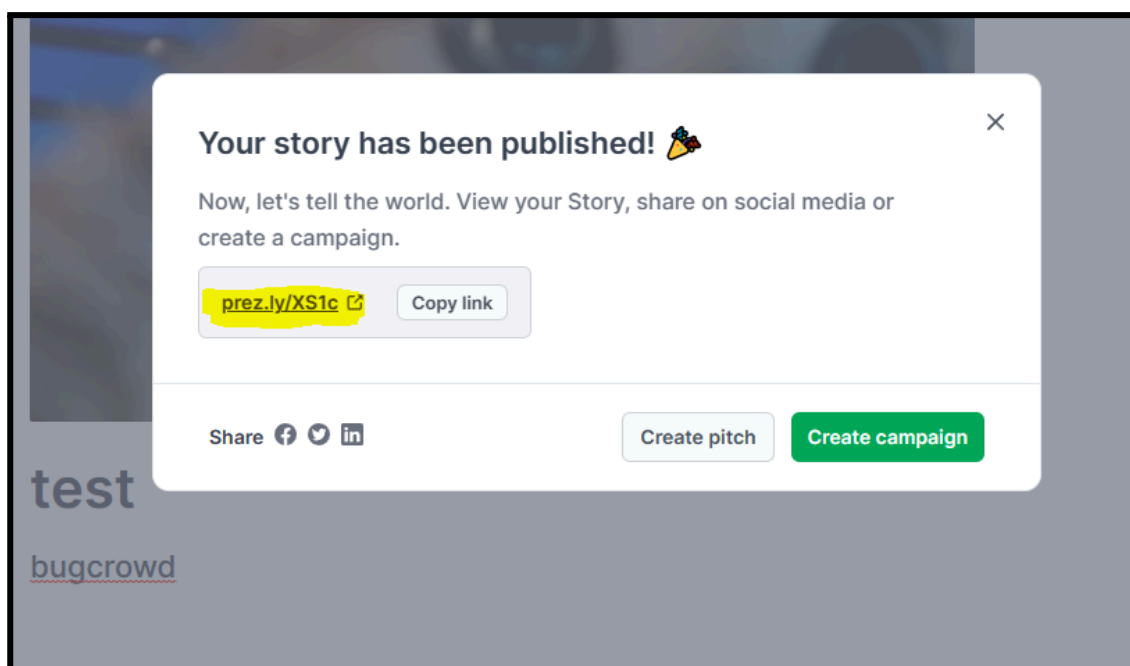
```

<!DOCTYPE html>
<html lang="en-GB" prefix="og: http://ogp.me/ns#" class="no-js">
  <head> ... </head>
  <body class="home page-template page-template-template-home page-template-template-home-php page page-id-2 page-sample-page">
    <!-- Google Tag Manager (noscript) -->
    <noscript> ... </noscript>
    <!-- End Google Tag Manager (noscript) -->
    <noscript> ... </noscript>
    <div class="get-app"> ... </div>
    <div class="jp_topbar" style="flex"
      <span data-id="1" style="display: none;" id="msg_1" class="jp_topmsgs">
        "PlayStation Network (PSN) is now available in the ETN App. "
        <a href="http://prez.ly/fb0b" target="_blank">(Full details)</a>
        "&nbsp;"
      </span>
      <span data-id="2" style="display: none;" id="msg_2" class="jp_topmsgs">
        "Apple iTunes and App Store is now available in the ETN App. "
        <a href="http://prez.ly/H40b" target="_blank">(Full details)</a>
        "&nbsp;"
      </span>
      <span data-id="3" style="display: none;" id="msg_3" class="jp_topmsgs">
        "Xbox is now available in the ETN App. "
        <a href="http://prez.ly/YN0b" target="_blank">(Full details)</a>
        "&nbsp;"
      </span>
      <span data-id="4" style="display: none;" id="msg_4" class="jp_topmsgs">
        "Amazon is now available in the ETN App. "
        <a href="http://prez.ly/cn5b" target="_blank">(Full details)</a>
        "&nbsp;"
      </span>
      <span data-id="5" style="display: none;" id="msg_5" class="jp_topmsgs"> ... </span>
      <span data-id="6" style="display: none;" id="msg_6" class="jp_topmsgs"> ... </span>
      <span data-id="7" style="display: block;" id="msg_7" class="jp_topmsgs"> ... </span>
      <span data-id="8" style="display: none;" id="msg_8" class="jp_topmsgs"> ... </span> == $0
      <span class="close" id="closetop">...</span>
      <input type="hidden" id="allmsgs" value="8">
      <!-- The Modal -->
    </div>
    <!-- DIV ADDED BY JOOMLAPRO FOR TOP MODAL - START -->
    <div id="jpModal" class="jpmodal"> ... </div>
    <!-- DIV ADDED BY JOOMLAPRO FOR TOP MODAL - END -->
    <div class="wrapper invisible"> ... </div>
    <div class="download fullscreen-popup"> ... </div> (flex)
    <script type="text/javascript"> ... </script>
  </body>
</html>

```

Upon further digging, I found that the links were for a communication and PR management tool called 'prezly', which could generate short links to services which aid developers add content to a web page.

So, I decided to attempt to register my own links on 'prezly', in hopes I could register or 'hijack' the broken links found on the website:

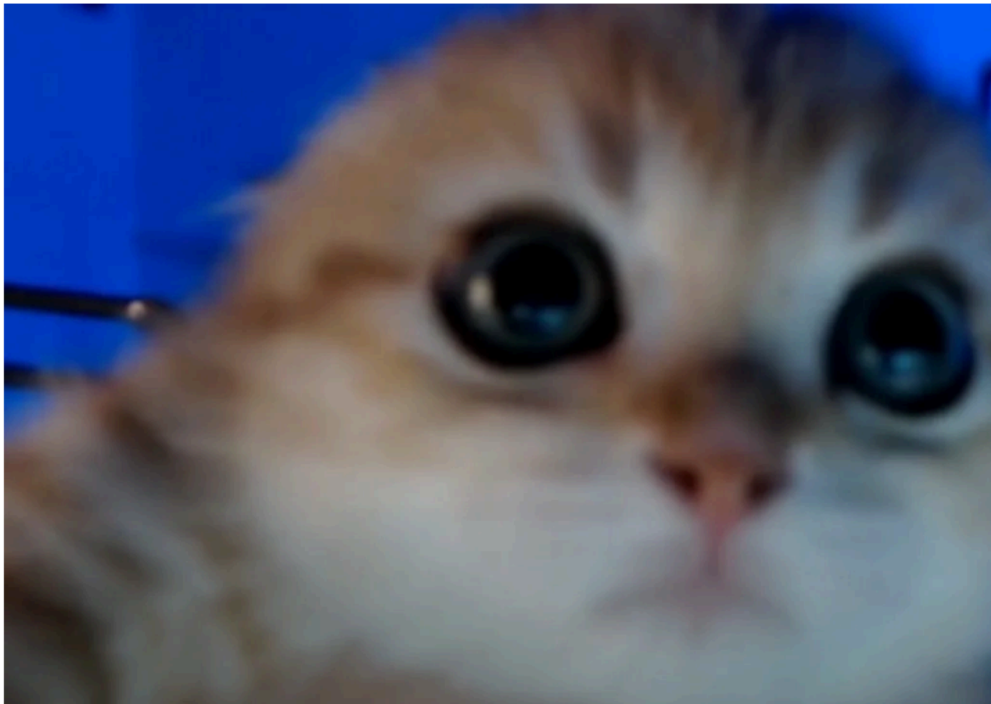


To my surprise, the links generated from this service could be customisable, allowing me to register the exact links used on the cryptocurrency site, theoretically allowing me to implement my own material embedded into the page:

**gdf**

fd

June 25, 2023



Due to me being able to register links that had expired, but still remained on the application, this allowed me as an attacker to potentially trick users of the site into viewing material made by me, and due to the nature of the finding, could have easily redirected users into a phishing or malware ridden page.

### **Resolution:**

A report was filed upon being able to inject potentially malicious material into the website's page, and this issue was fixed in quick time.

Monetary compensation was awarded to me for finding and disclosing this vulnerability and additional protection against this had been put in place to mitigate this issue from arising again.

---

This document is a disclosed vulnerability report by a practised security researcher, all vulnerabilities and issues mentioned in this report have been released under the permission of the owner and/or have been mitigated against and fixed before this report was written, if by any chance the contents of this report can be replicated this is due to another vulnerability or mere coincidence, please report any issues or regards: [prv@anche.no](mailto:prv@anche.no)

---