- DISCLOSED VULNERABILITY REPORT -

By Prv | mail | github | bugcrowd |

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

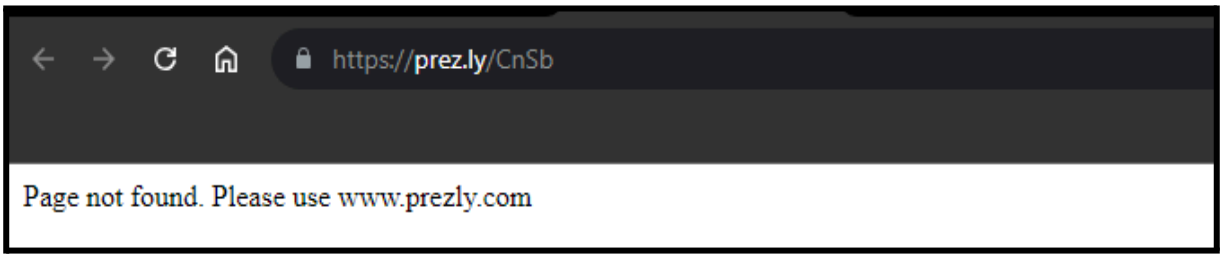
Vulnerability type: **Server side injection | Recurring Broken link hijack (BLH)**

Severity: **Medium**

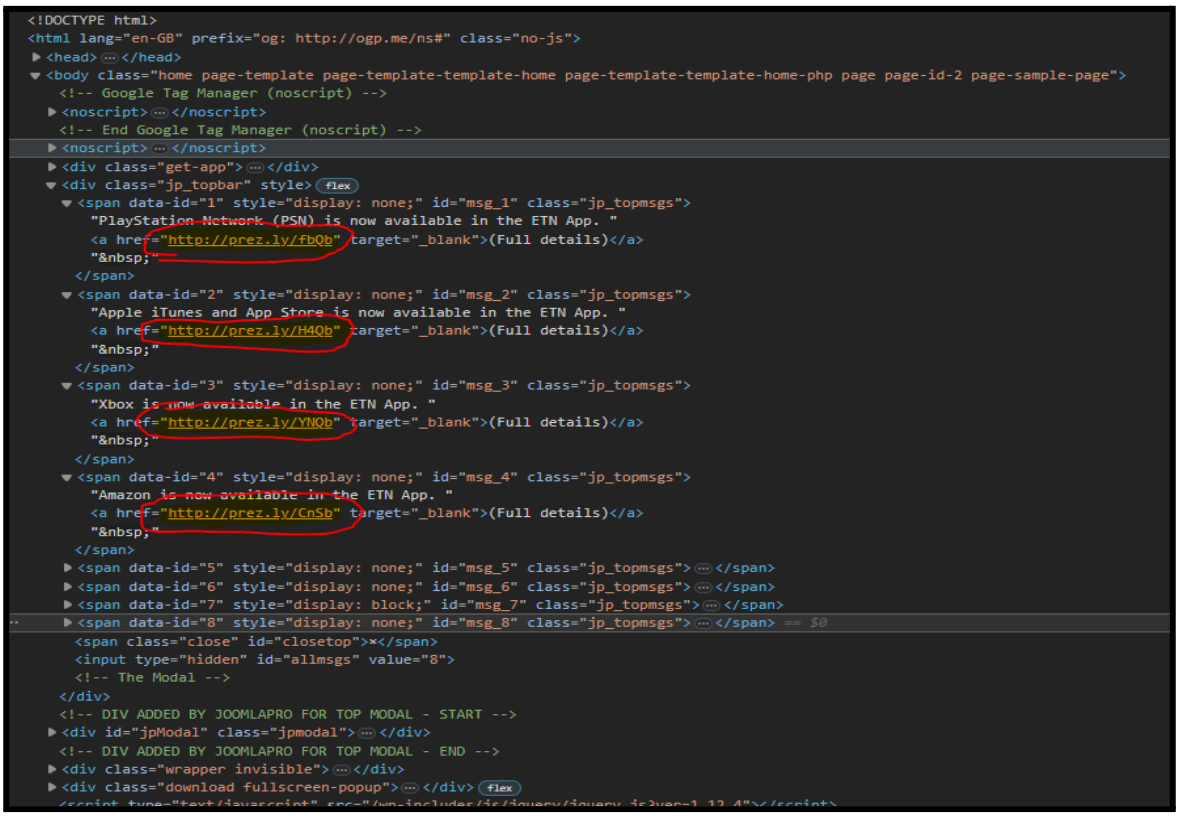
Overview:

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:

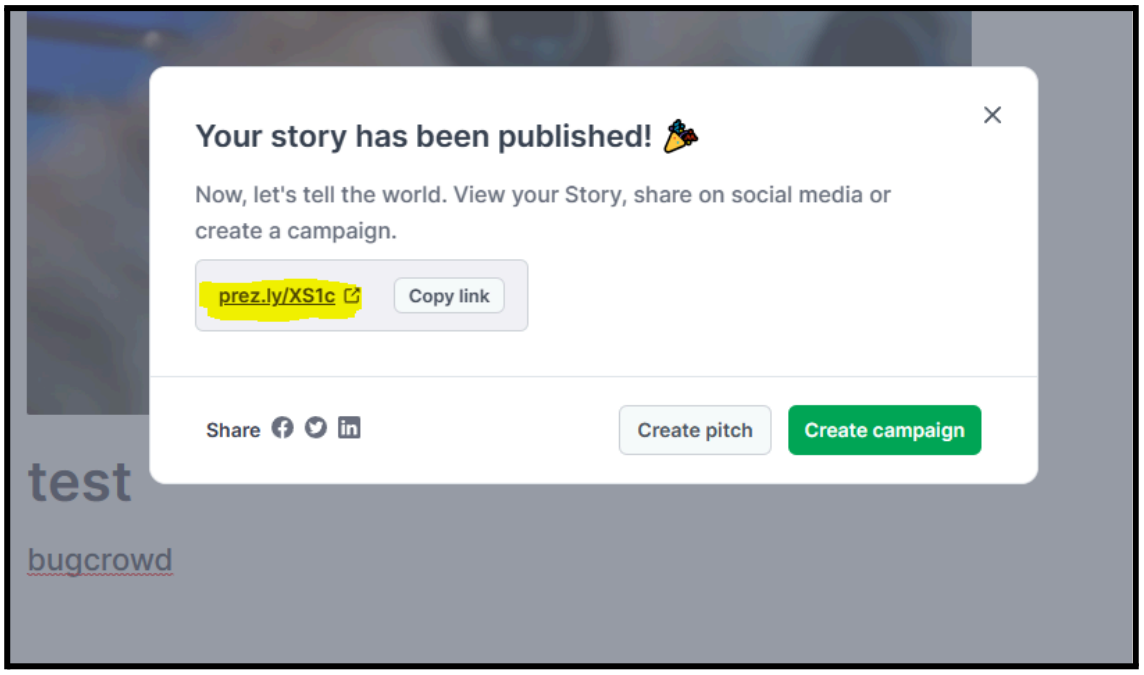


These links were found throughout the index page of the website, and had all came from the same expired service used to host the external Resources:

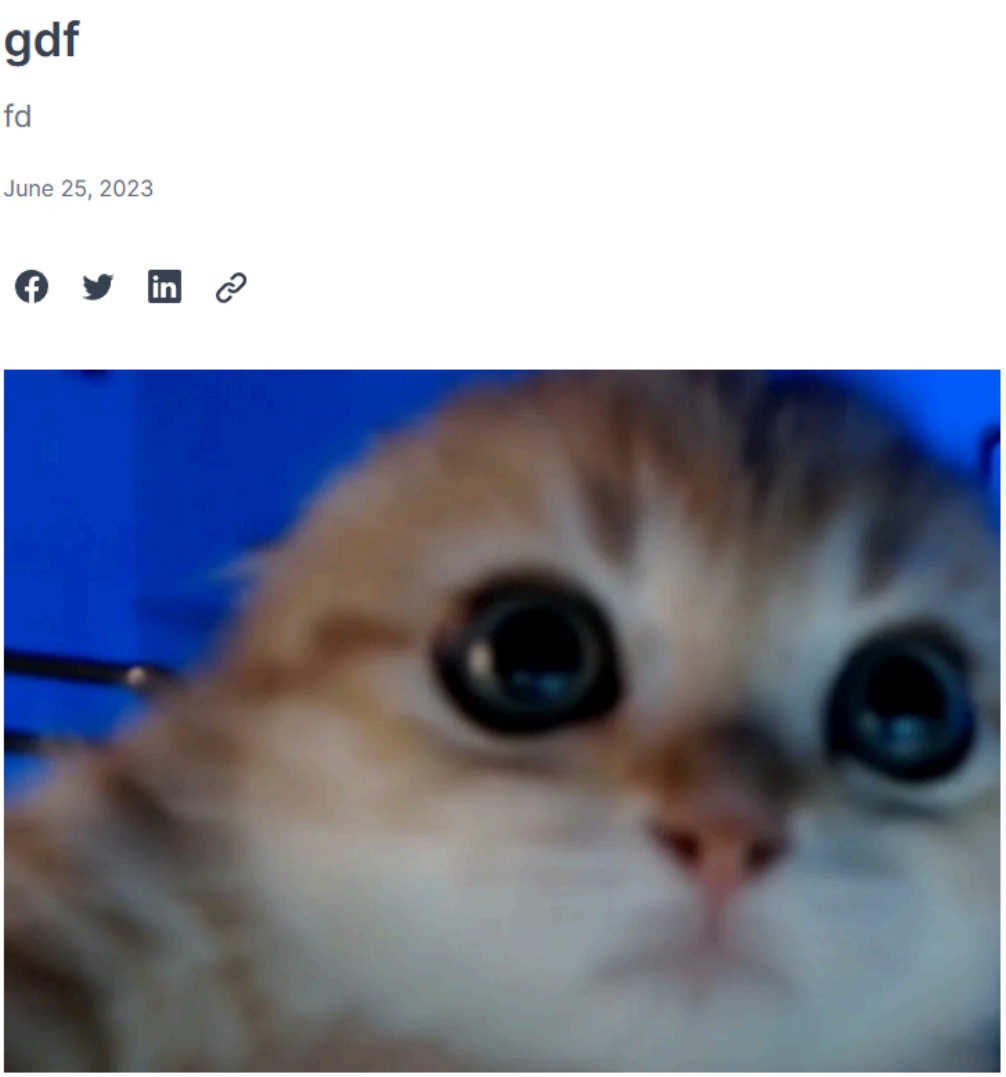


Upon further digging, I found that the links were for a communication and PR management tool called 'prezly', which could generate short links to services which aid developers add content to a web page.

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:



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.
