[RESEARCH] - CVE-2026-95166 - Stored XSS in Bacularis 1.0.0 - 6.5.1 - Pool LabelFormat field



@

Summary

Stored XSS affects users with the administrator role or a with a role with the `PoolList` and `PoolView` resources assigned via the `LabelFormat` field. In the `Pools / Add pool`, add the XSS payload in the `labelFormat` field. The payload gets executed when clicking on the pool details and running `Update pool`.

General information

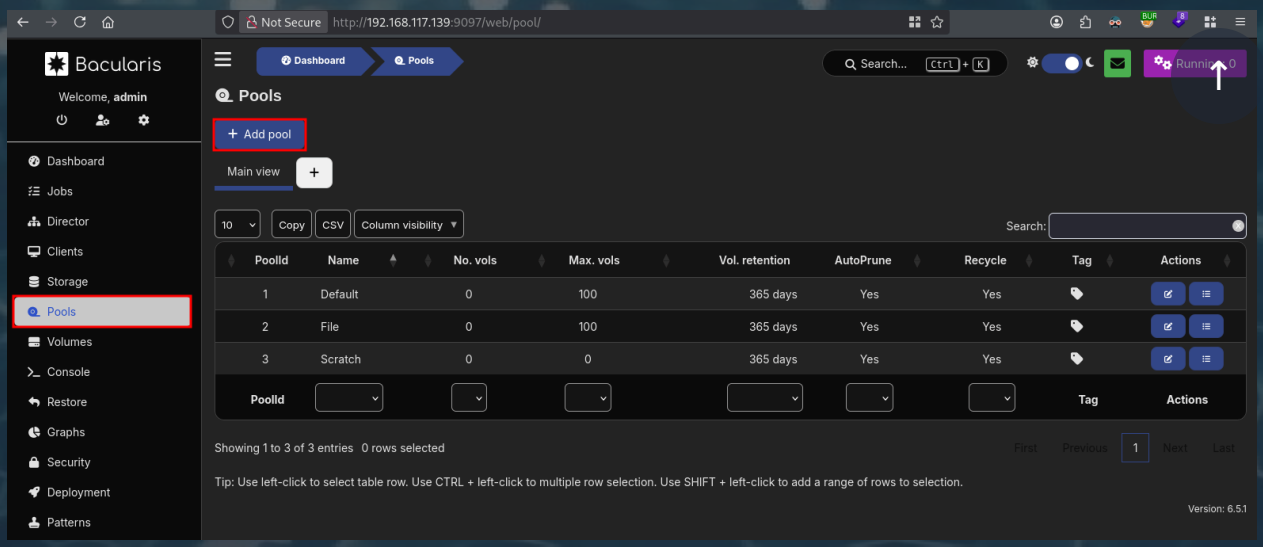
Description: The `LabelFormat` field within `Pools / Add pool` is vulnerable to Stored Cross-Site Scripting (XSS).

HEKK

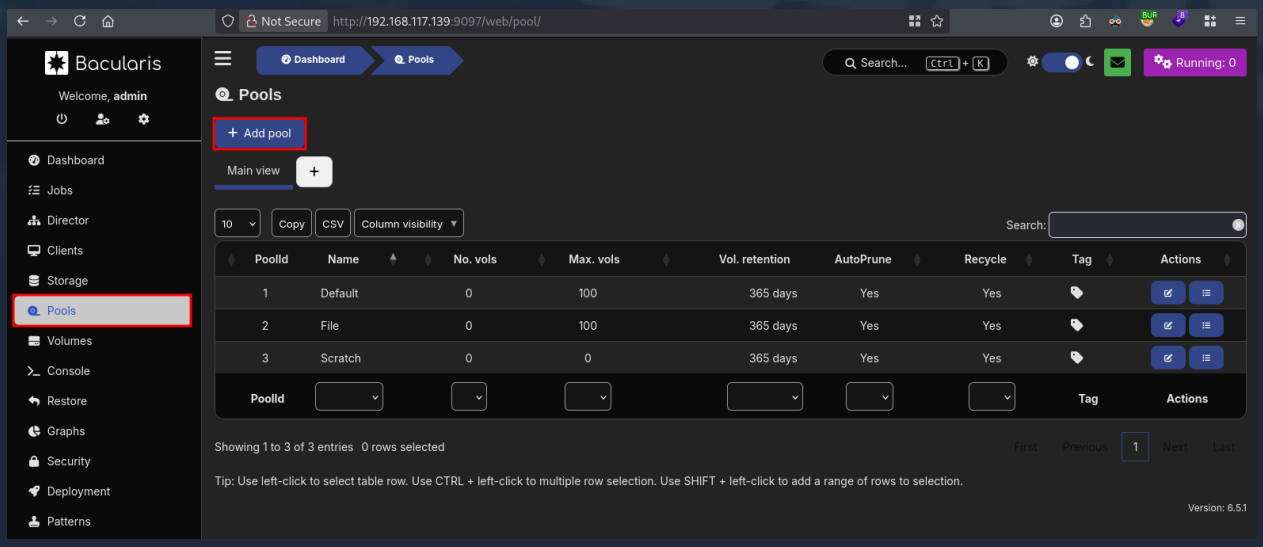
Versions Affected: 1.0.0 through 6.5.1
Version Fixed: 6.5.2
Researcher: HEKK.ONE

Proof-of-Concept (POC) Exploit

Go to `Pools` and click on `Add pool`.

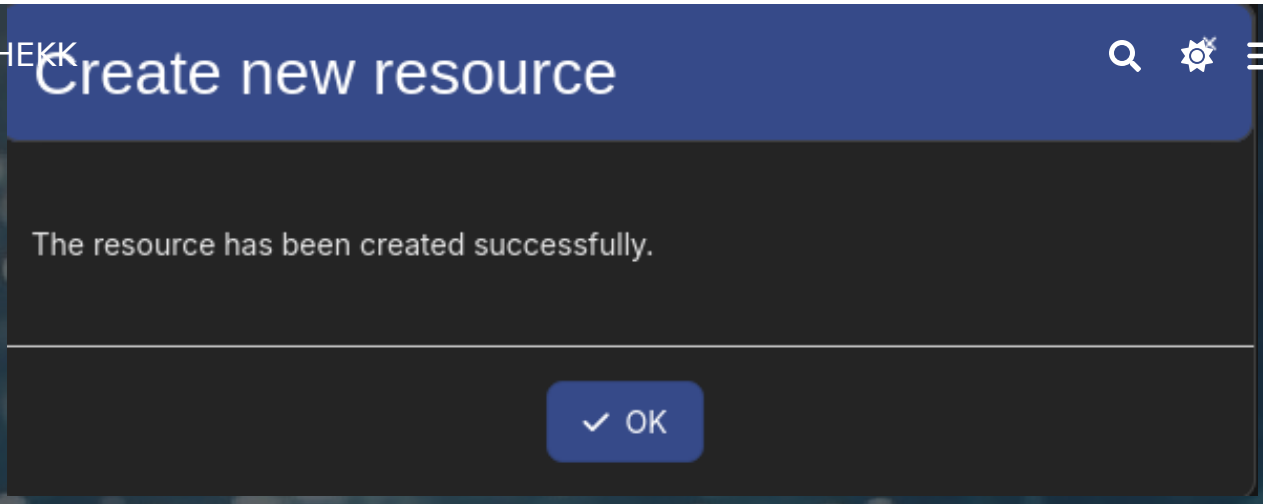


Now give the pool a name (ex. `name)` ,select a pooltype and add the XSS payload in the LabelFormat field, ex. `<script>prompt()</script>`. Now click on `Create`.

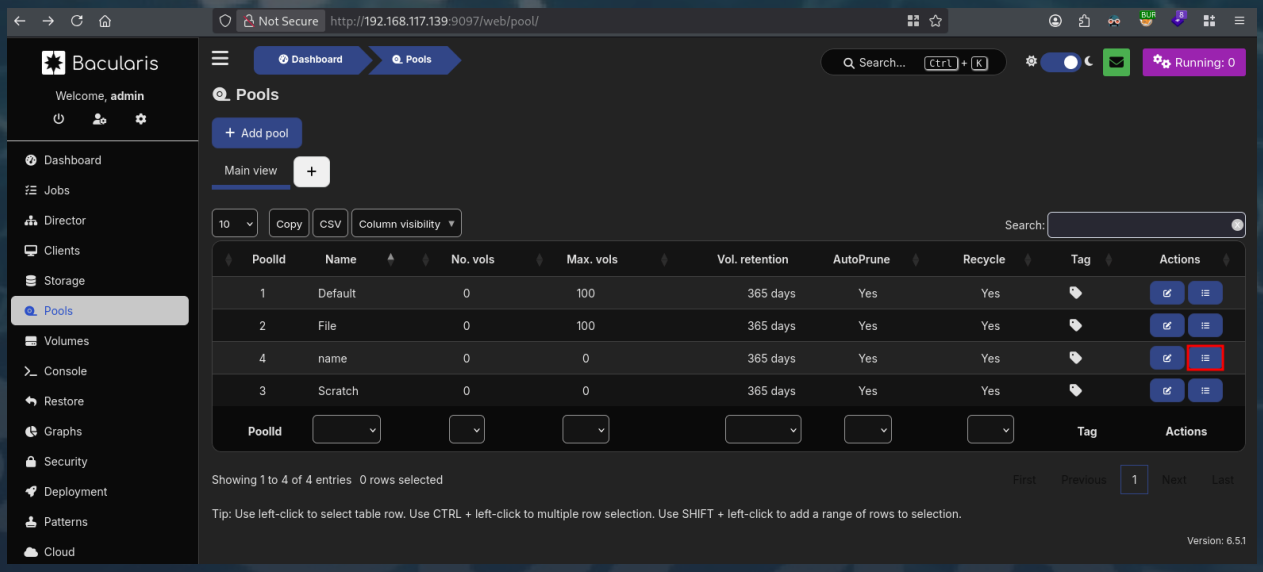


The pool is created, click `OK`.

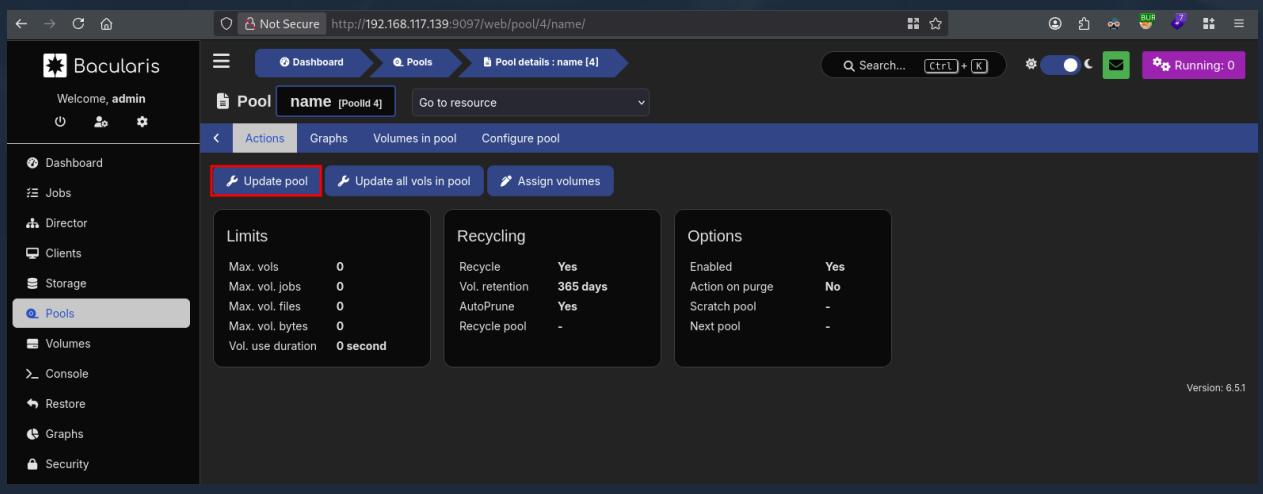
HEKK

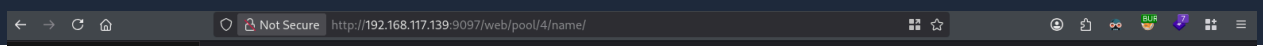


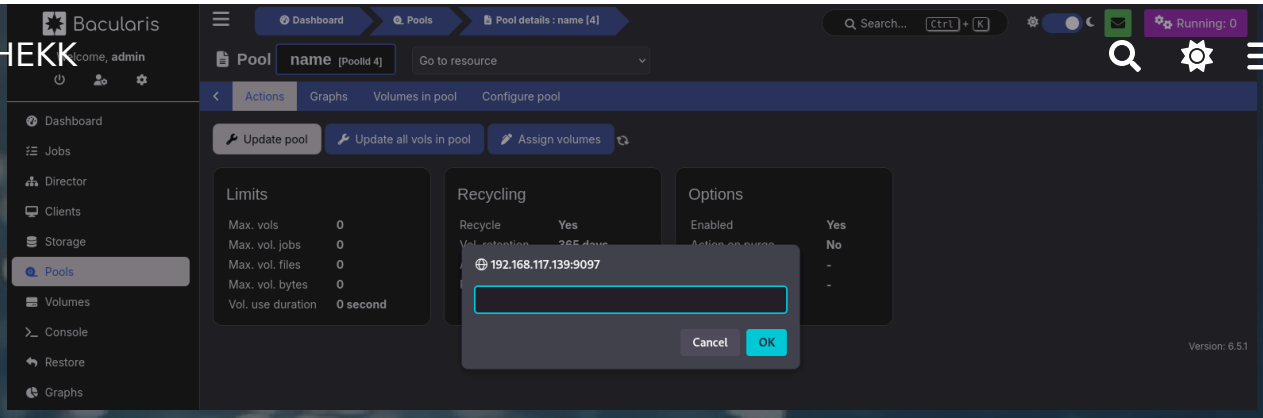
Click on the `Details` button of newly created pool `name`.



Now click on `Update pool` to execute the XSS payload.







This vulnerability works for users with the administrator role or a with a role with the `PoolList` and `PoolView` resources assigned.

Related



[RESEARCH] - CVE-2026-95165 - Stored XSS in Bacularis 5.4.0 - 6.5.1 - Organization name

30 September 2026 · 226 words · 2 mins

RESEARCH CVE-2026-95165 BACULARIS

Stored XSS affects all users via the organization name. Add an organization under Security / Organizations with an XSS



[RESEARCH] - CVE-2026-88742 - Stored Cross Site Scripting (XSS) in Bacularis 1.0.0 - 6.5.0 client address

11 September 2026 · 266 words · 2 mins

RESEARCH CVE-2026-88742 BACULARIS

A stored XSS affects all users who can view client details. Add a client with the XSS

payload; it executes when any user clicks its linked logout button.

payload in the address field, save it, then click Details to execute the payload.



[RESEARCH] - CVE-2026-88743 - Stored XSS in Bacularis 4.7.0 - 6.5.0 - director tags

11 September 2026 · 446 words · 3 mins

RESEARCH CVE-2026-88743 BACULARIS

Stored XSS affects all users via globally accessible tags. Add a global tag in JobDefs and set its value to an XSS payload. Once assigned, it executes for every user who can view jobs.



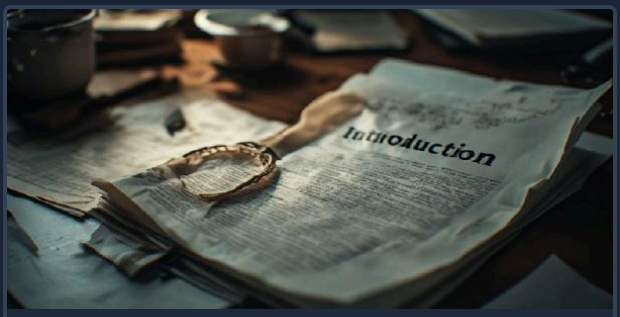
[RESEARCH] - CVE-2026-78738 - Stored XSS Silverpeas Core 6.4.6 - File upload feature

5 September 2026 · 384 words · 2 mins

RESEARCH CVE-2026-78738 SILVERPEAS

Stored XSS in Silverpeas Document Management. By modifying the X-FULL-PATH header during file upload with an XSS payload, the payload executes when the file’s preview button is clicked.





[RESEARCH] - CVE-2026-78741 - Stored XSS in wysiwyg-CKEditor image upload feature (Silverpeas <= 6.4.6)

5 September 2026 · 235 words · 2 mins

RESEARCH CVE-2026-78741 SILVERPEAS

Stored XSS in Silverpeas' CKEditor image upload feature allows attackers to replace the filename with a JavaScript payload that executes after the file is uploaded.

[RESEARCH] - CVE-2026-78742 - Stored Cross Site Scripting (XSS) in introduction Multimedia library application (Silverpeas Core <=6.4.6)

5 September 2026 · 343 words · 2 mins

RESEARCH CVE-2026-78742 SILVERPEAS

Stored XSS in the Multimedia library introduction allows attackers to inject a JavaScript payload via the editor1 parameter, executing when users visit the application.