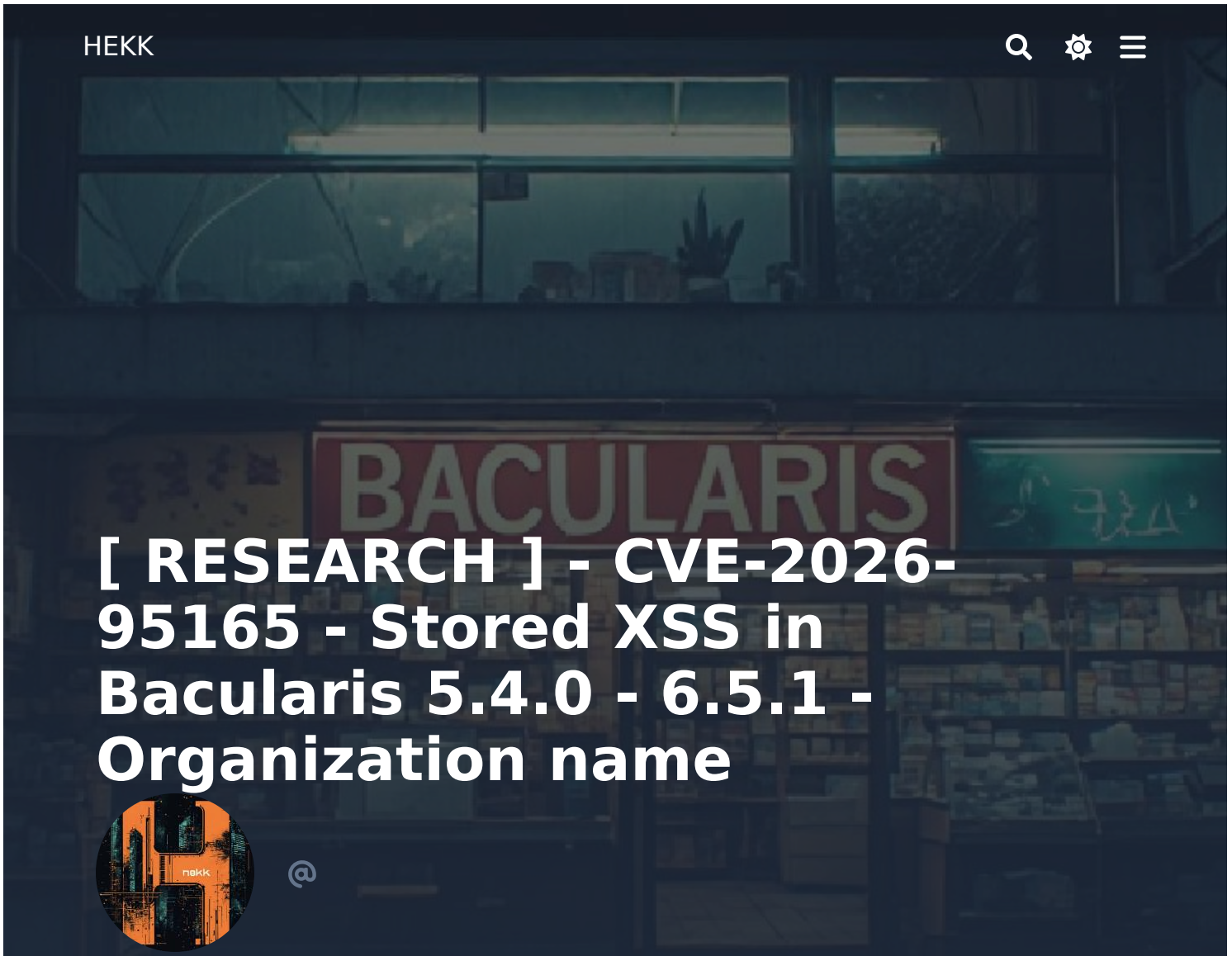


[RESEARCH] - CVE-2026-95165 - Stored XSS in Bacularis 5.4.0 - 6.5.1 - Organization name

@

Summary

Stored XSS affects all users (admin/normal) via the organization name. In the `Security / Organizations`, add an organization and enter the XSS payload in the `Organization name`. The payload gets executed when any user, linked to the created organization, clicks on the logout button.

General information

Description: The organization name within `Security / Organizations / Add organization` is vulnerable to Stored Cross-Site Scripting (XSS).

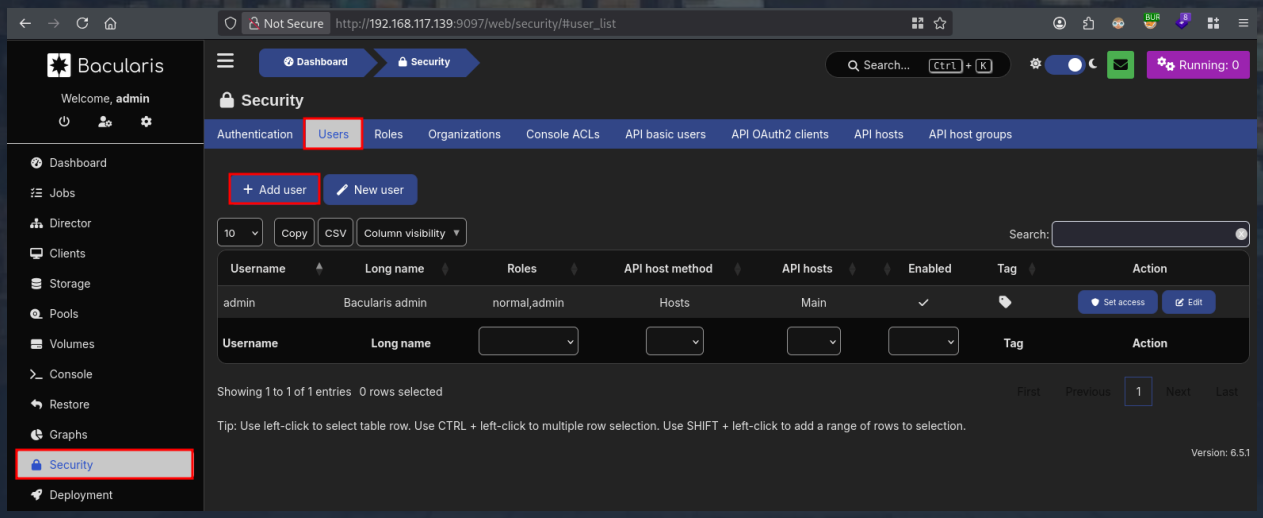
Versions Affected: 5.4.0 through 6.5.1
Version Fixed: 6.5.2
Researcher: HEKK.ONE

Creating a new normal user

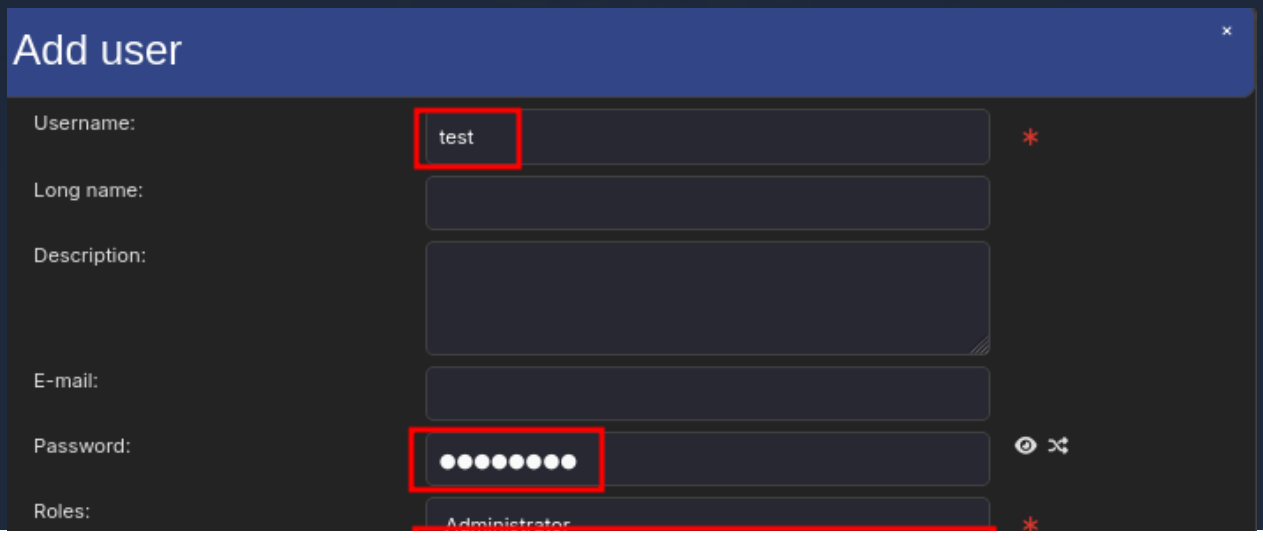
On a fresh install of Bacularis 6.5.1

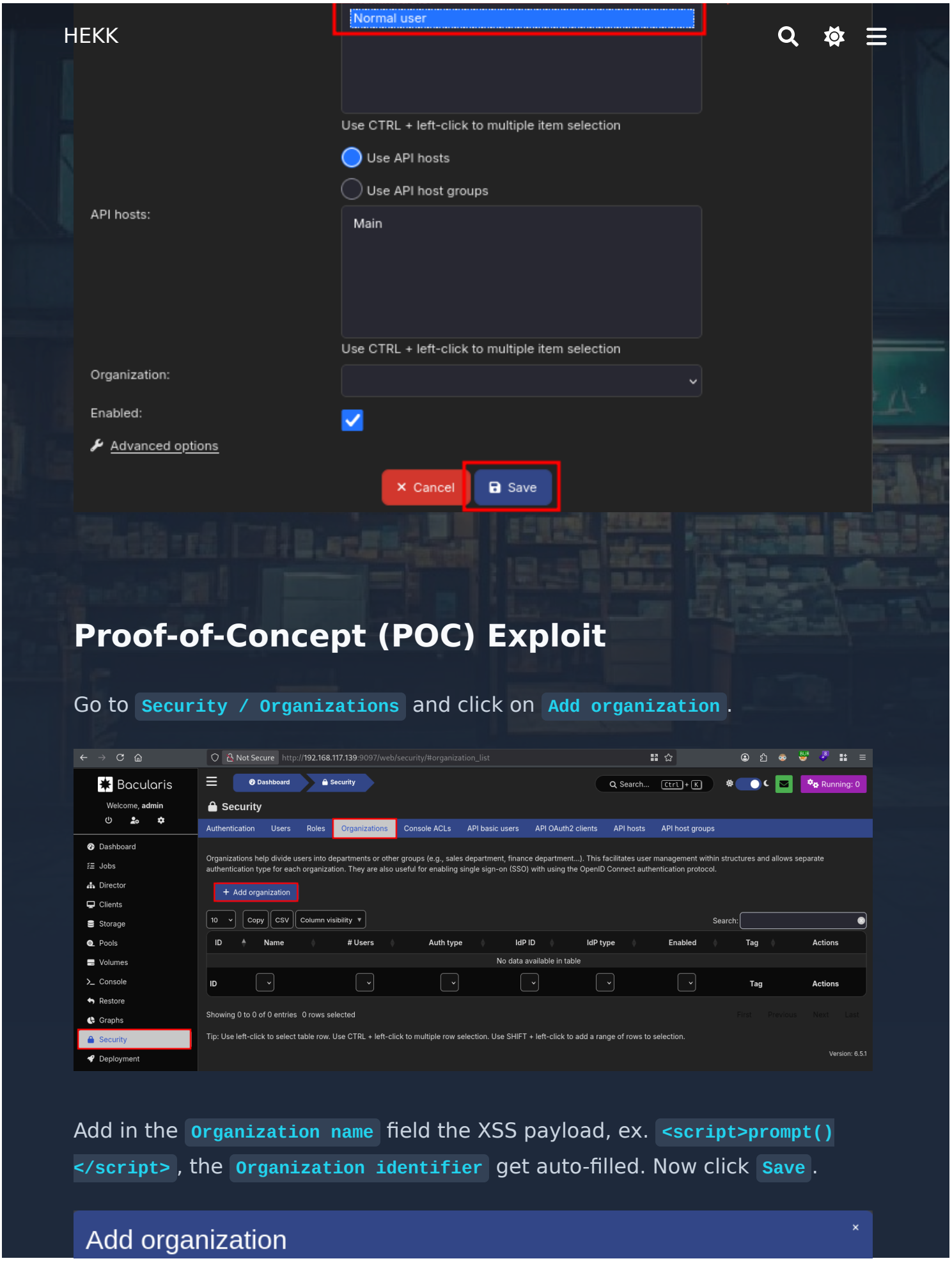
```
docker run -d -p 9097:9097 bacularis/bacularis-standalone:6.5.1-alpine
```

Login with `admin:admin`, go to `Security / Users / Add user`.



We give the new user these values for name and password: `test:password1`, and select `Normal user`. Now click `Save`.

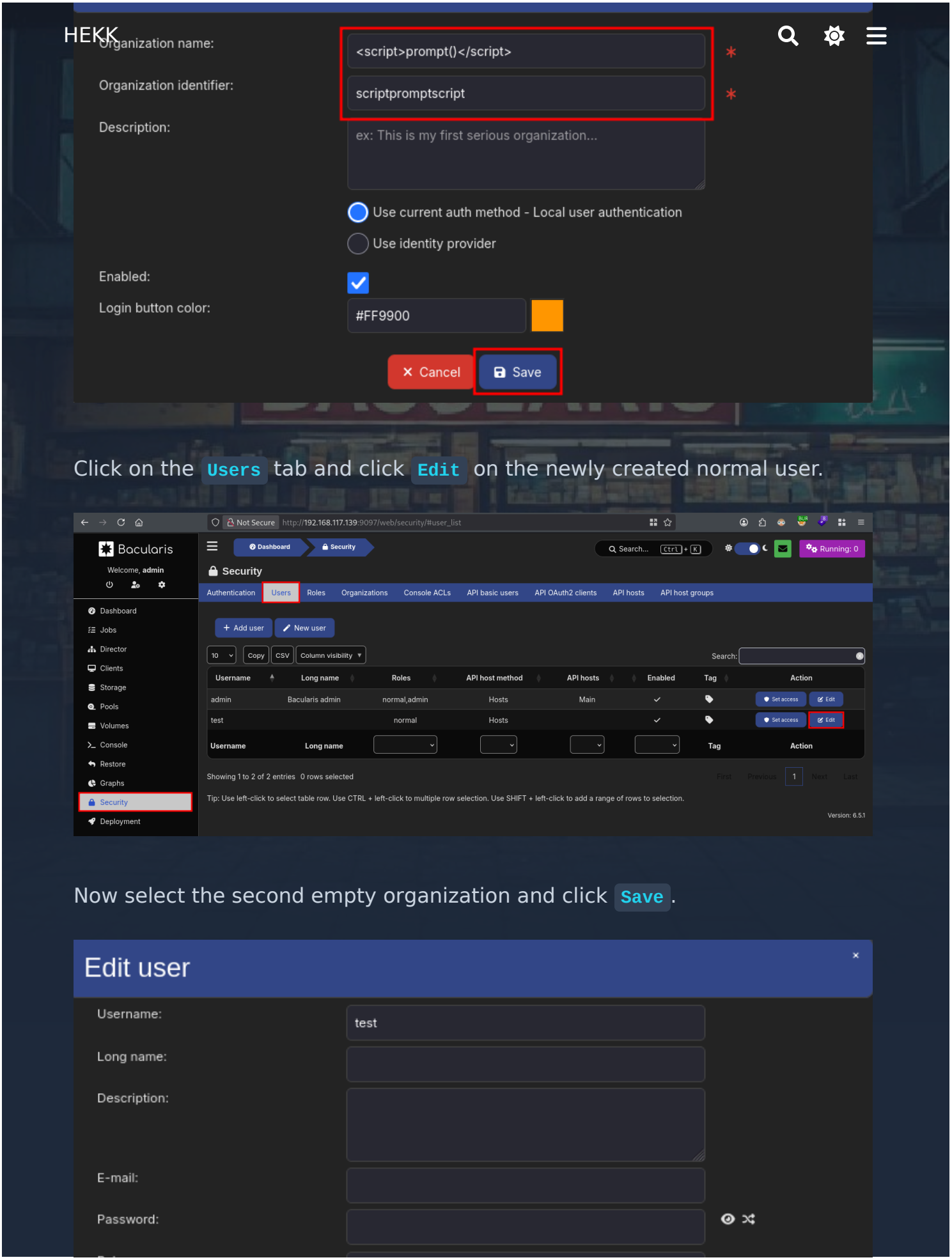




Proof-of-Concept (POC) Exploit

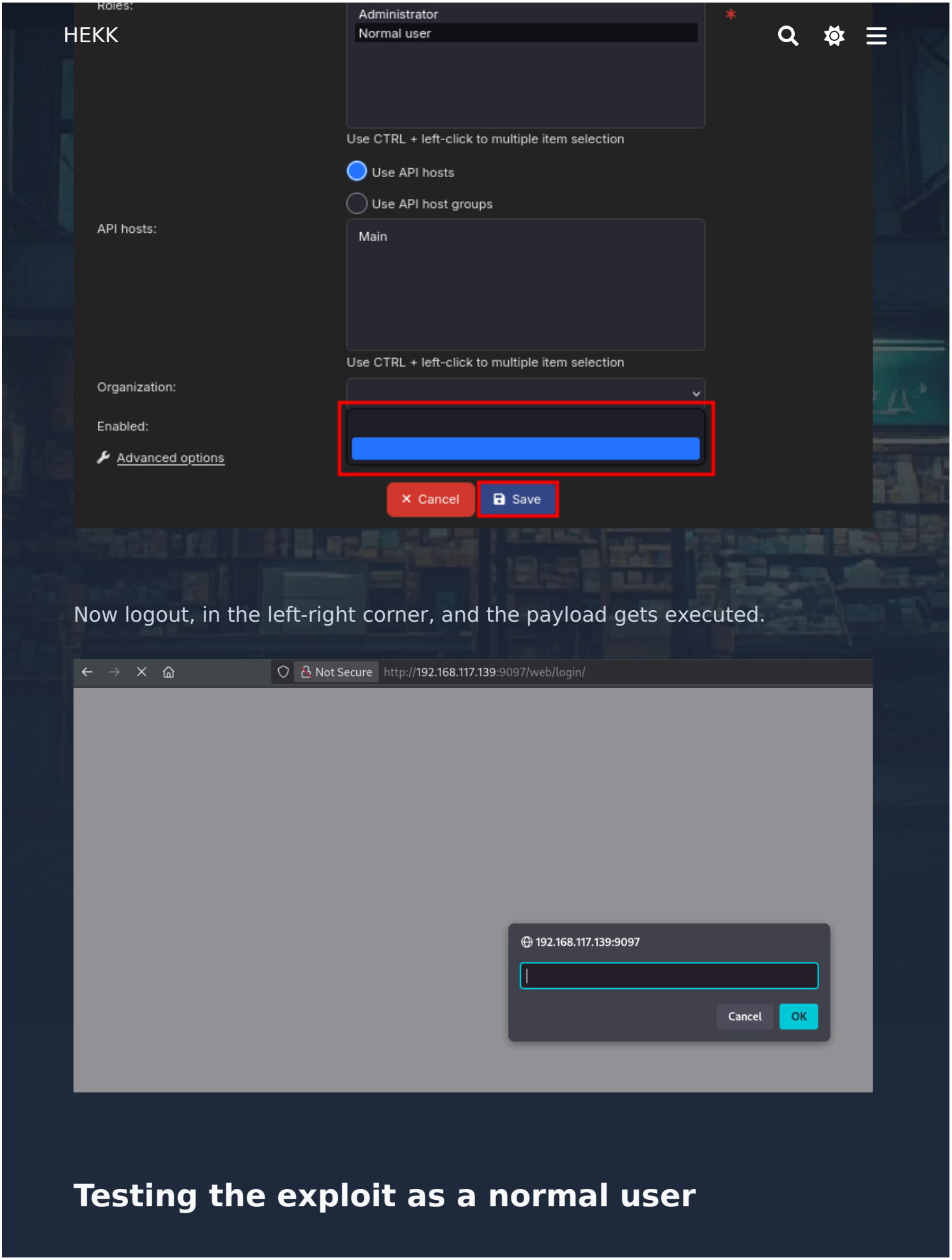
Go to `Security / Organizations` and click on `Add organization`.

Add in the `Organization name` field the XSS payload, ex. `<script>prompt()</script>`, the `Organization identifier` get auto-filled. Now click `Save`.



Click on the `Users` tab and click `Edit` on the newly created normal user.

Now select the second empty organization and click `Save`.



Now logout, in the left-right corner, and the payload gets executed.

Testing the exploit as a normal user

Login as the new user with these credentials: `test:password1`. We get logged in as a normal user. Now, logout and the XSS payload gets executed.

Related



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

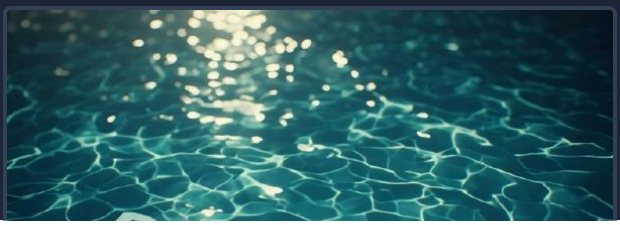


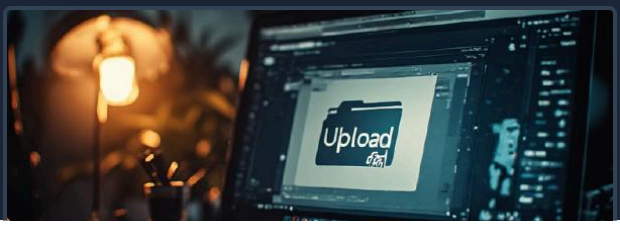
[RESEARCH] - CVE-2026-88743 - Stored XSS in Bacularis 4.7.0 - 6.5.0 - director tags

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-2026-95166 - Stored XSS in Bacularis 1.0.0 - 6.5.1 - Pool LabelFormat field

30 September 2026 · 168 words · 1 min

RESEARCH CVE-2026-95166 BACULARIS

Stored XSS affects admins or users with PoolList/PoolView. Add an XSS payload to labelFormat in Pools / Add pool; it executes when viewing pool details and running Update pool.

[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



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

5 September 2026 · 343 words ·

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.

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.

