

[New issue](#)

[Jump to bottom](#)

## Multiple vulnerabilities in LDAP Account Manager #170

✓ Closed

Fumenoid opened this issue on Apr 10 · 1 comment

**Fumenoid** commented on Apr 10

Hello..

I am a security researcher, and with my friend Manthan(@netsectuna), We reviewed the application and discovered multiple vulnerabilities.

## 1. Stored XSS

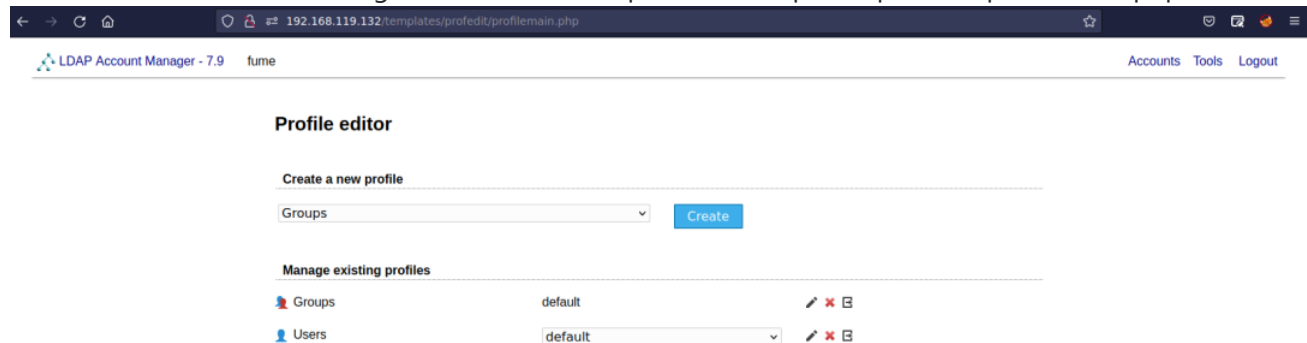
Description - The profile editor tool has an edit profile functionality, the parameters on this page are not properly sanitized and hence leads to stored XSS attacks. An authenticated user can store XSS payloads in the profiles, which gets triggered when any other user try to access the edit profile page.

Impact - Medium/High (depends on how the server profile is configured.. if ldap users and ldap admin both can login to ldap account manager, an ldap user can write save xss payloads to trigger tasks as admin)

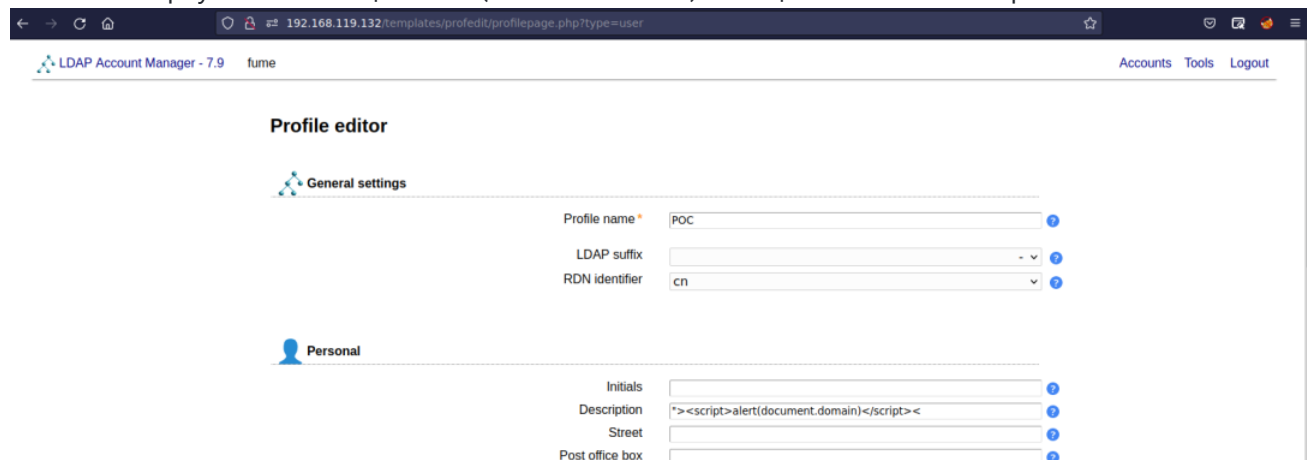
Affected URL - <http://<IP>/templates/profedit/profilepage.php>

POC :

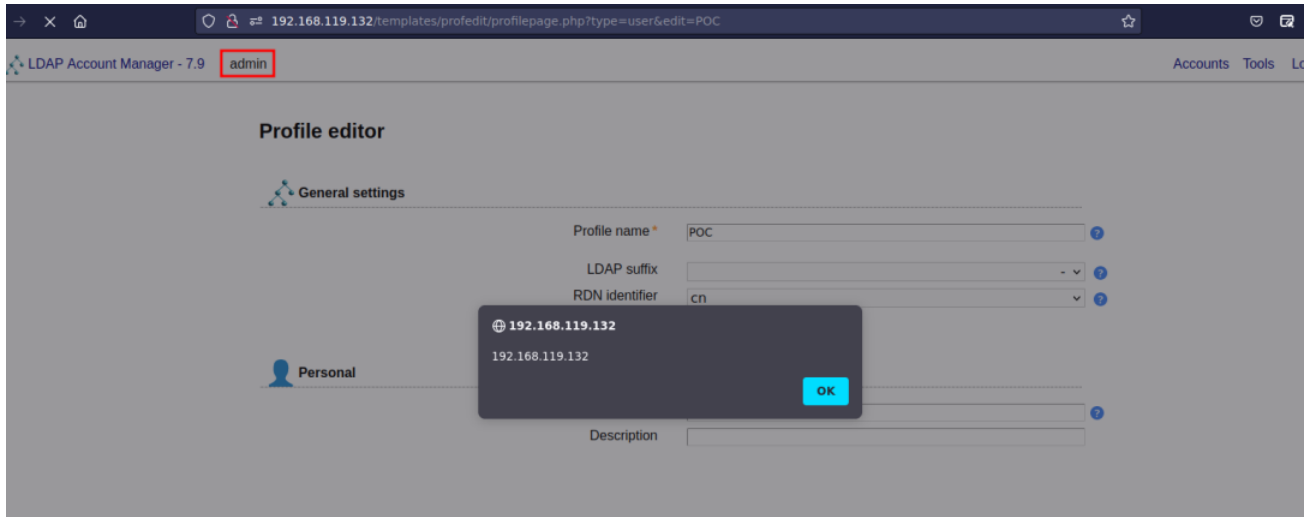
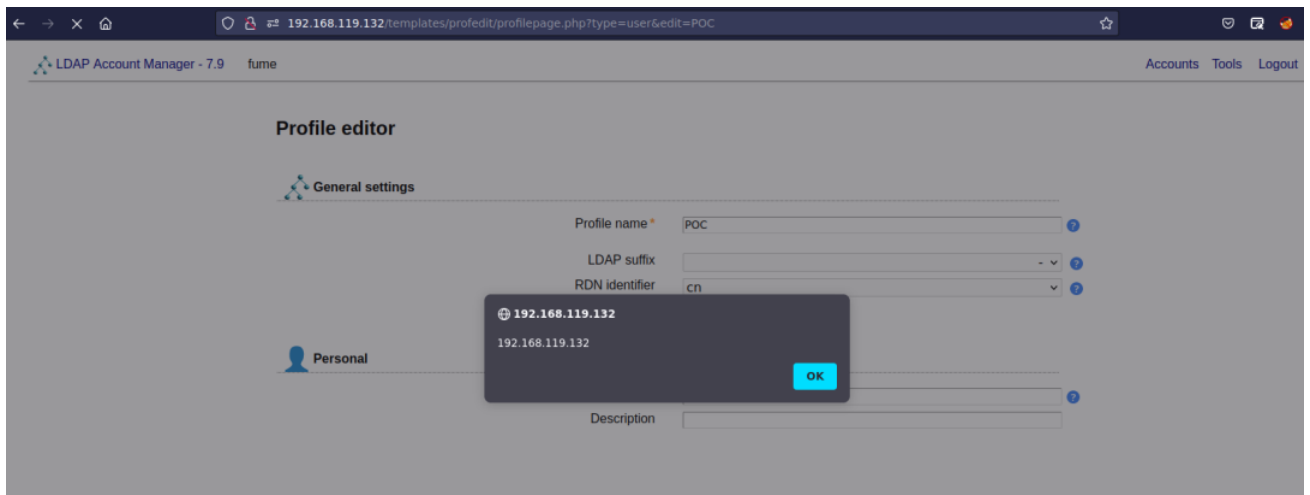
As an authenticated user navigate to the URL - <http://<IP>/templates/profedit/profilemain.php>



Create a new user profile for either user or group (editing profile will also work) and in description field add the XSS payload "><script>alert(document.domain)</script><" and save the profile.



Now whenever any authenticated user will edit this profile page, XSS payload will be triggered.



## 2. Arbitrary jpg/png file read

Description - The pdf editor tool has an edit pdf profile functionality, the `logoFile` parameter in it is not properly sanitized and an user can enter relative paths like

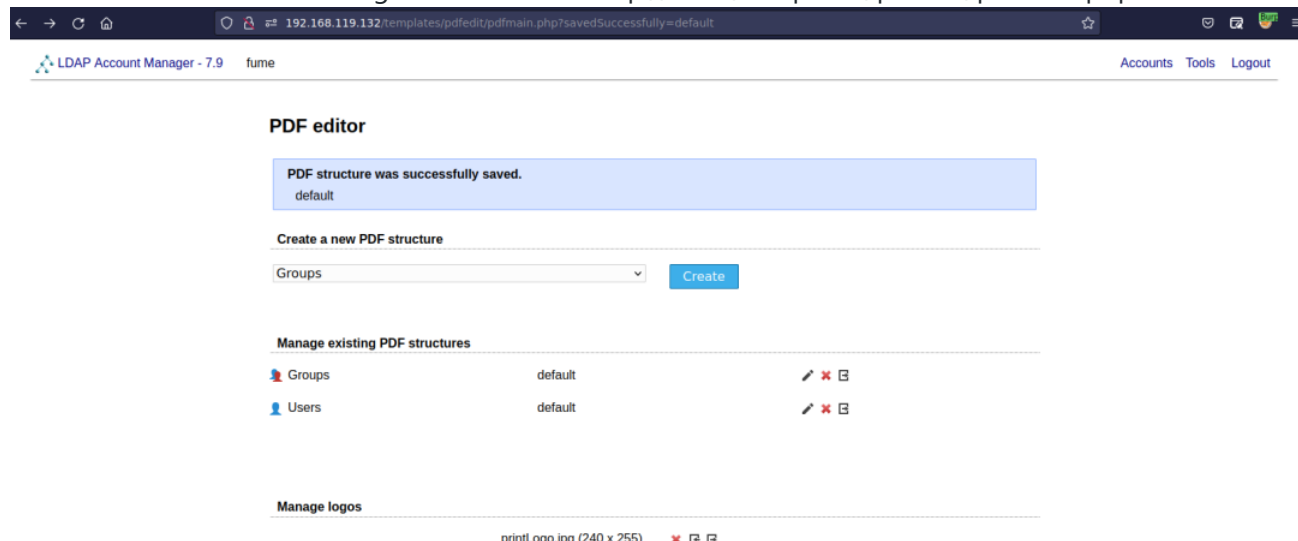
`../../../../../../../../../../../../../../../../usr/share/icons/hicolor/48x48/apps/gvim.png` via tools like burpsuite. Later when a pdf is exported using the edited profile the pdf icon has the image on that path(if image is present).

Impact - Low (Impact is low, due to highly unlikelihood of ldap admin knowing the locations of images having any sensitive/Personal information. One possible attack vector is to enumerate tools/software on the system by checking for icon images.. like in this POC we can verify the server has vim installed)

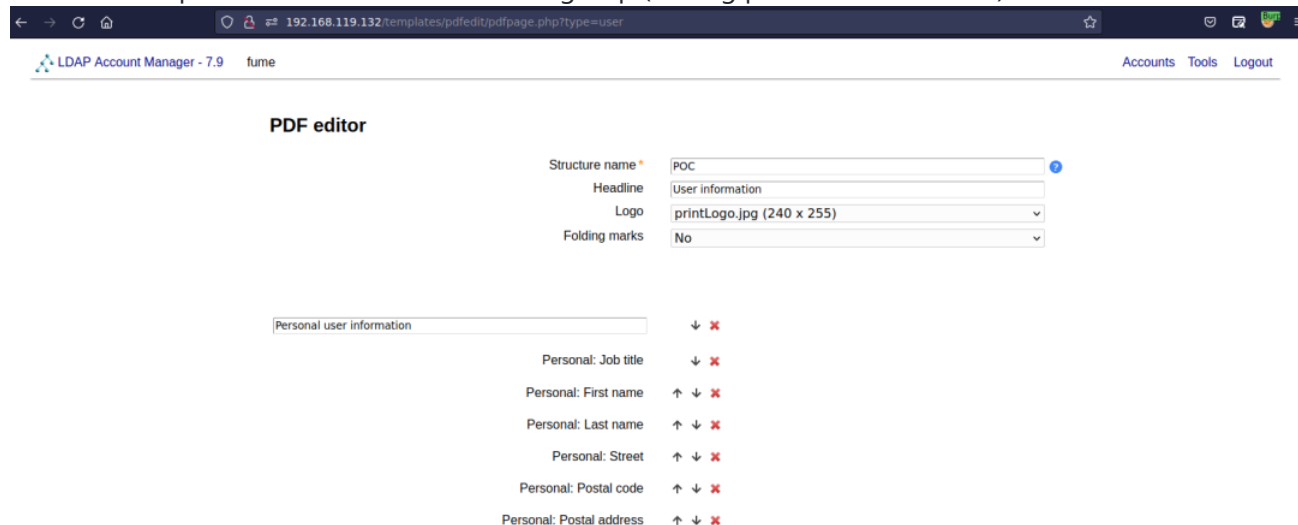
Affected URL - `http://<IP>/templates/pdfedit/pdfpage.php`

POC :

As an authenticated user navigate to the URL - `http://<IP>/templates/pdfedit/pdfmain.php`



Create a new pdf structure for either user or group (editing profile will also work)



With burpsuite proxy on, click on save. In burpsuite, replace the value of `logoFile` parameter to the path of image file, lets say

`../../../../../../../../../../../../../../../../usr/share/icons/hicolor/48x48/apps/gvim.png` for the icon file of vim and forward the request.

```
POST /templates/pdfedit/pdfpage.php HTTP/1.1
Host: 192.168.119.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 514
Origin: http://192.168.119.132
Connection: close
Referer: http://192.168.119.132/templates/pdfedit/pdfpage.php?type=user
Cookie: lam_last_language=en_US.utf8; PHPSESSID=siv51v6obip13u411pp5qctm0; Key=pmWCKY5CsworISsCmm3A5D%2FJ1H%2BdiXwjPQf6u9cABbE%3D; IV=jzgOZew%2F6oy5WcyGgiawur%3D%3D
Upgrade-Insecure-Requests: 1

pdfname=POC&headline=User+information&logoFile=../../../../../../../../usr/share/icons/hicolor/48x48/apps/gvim.png&foldingmarks=no&section_0=Personal+user+information&section_1=
Unix+settings&section_2=Windows+settings&section_3=Quota+Settings&new_field=main_dn&add_field_position=0&new_section_text=add_sectionText_position=0&new_section_item=main_dn&add_section_position=0&
text_text=add_text_position=0&submit=&modules=main%2CinetOrgPerson%2CshadowAccount%2CposixAccount&type=user&form_submit=true&sec_token=1069089487638&scrollTop=1254&scrollPositionLeft=0
```

Now while exporting pdf for a user if that poc profile is selected, the exported pdf will have the vim logo image.

#### Create PDF file

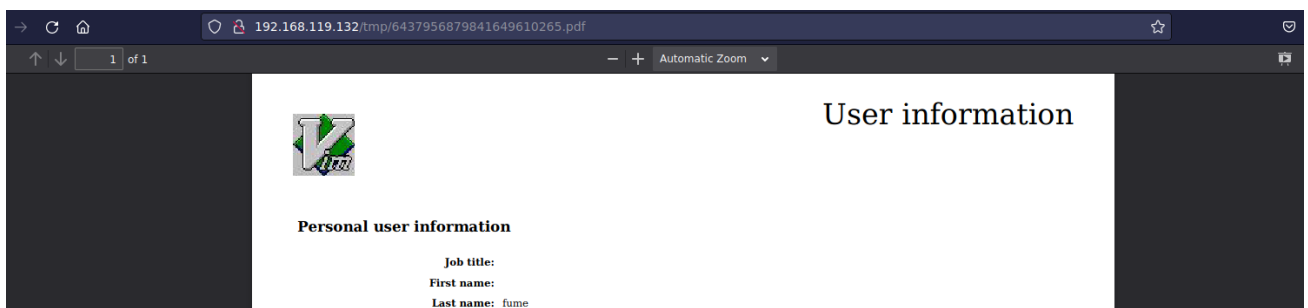
PDF structure  ?

Font  ?

Create for ☒ fume > people > acruxlare > tech


☐ All selected accounts (1)

☐ All accounts (2)



We would have loved to fix these ourselves.... but *cries bcz of bad dev skills*.

 gruberroland added a commit that referenced this issue on Apr 11

 #170 fixed security issues in profile editor and PDF editor

✓ 3c6f09a

gruberroland commented on Apr 11

Contributor

Thank you very much for your detailed report. The issues were fixed in the codebase and be published with 8.0 in June.



1

 gruberroland closed this as completed on Apr 11



**gruberroland** added a commit that referenced this issue on Apr 14



**#170** fixed security issues in profile editor and PDF editor ...

39c4850

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

