leommxj / **pacs_vuln_report.md** Secret

Created 2 years ago

pacs_vuln_report.md

PACS Server vulns

info

- vendor page: https://pacsone.net/
- patched version: 7.1.1
- Credits: Xinjie Ma from Chaitin Research Lab

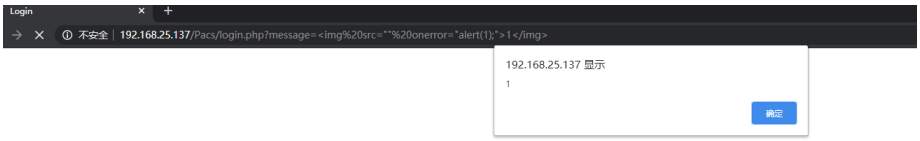
Timeline

- 2020.07.19 send report to a vendor's partner
- 2020.07.20 they inform the real vendor
- 2020.08.18 vendor design a fix plan
- 2020.11.10 vendor's partner inform me all vuln has been fixed and offer a bounty

Details

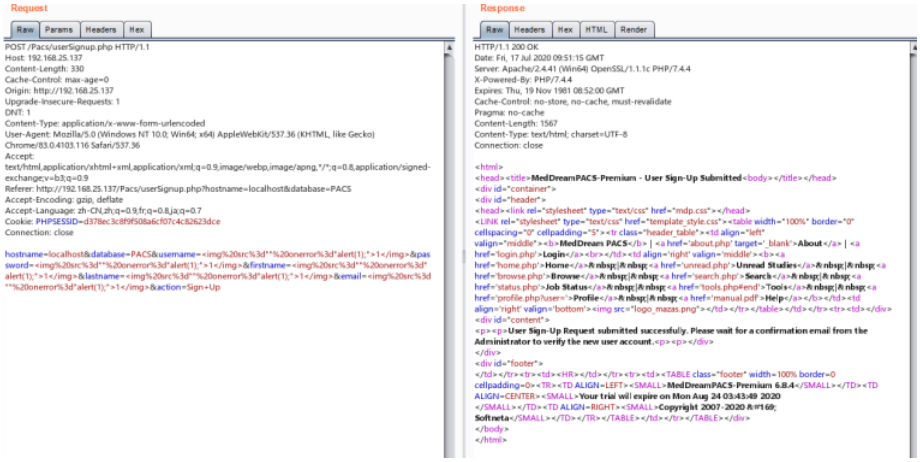
many Reflected XSS(Cross-site scripting)

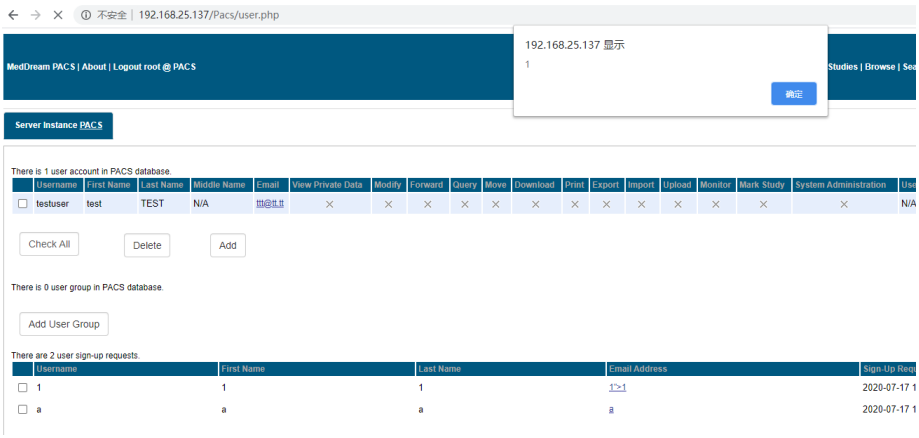
many user input concat or format to response html without any sanitization or check, some filter `<script` tag, for example in `login.php`, but a payload like `[http://192.168.25.137/Pacs/login.php?message=%3Cimg%20src=%22%22%20onerror=%22alert(1);%22%3E1%3C/img%3E](http://192.168.25.137/Pacs/login.php?message=1)` will bypass the check.



Stored XSS(Cross-site scripting)

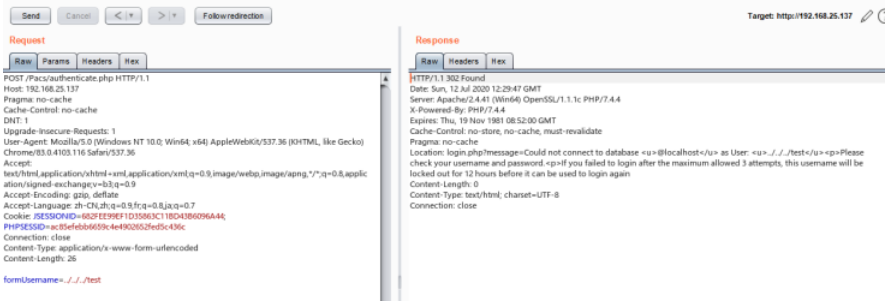
- `Pacs/userSignup.php` when a user sign up, administrator need to review the user. due to no proper sanitization, attacker can insert a xss payload, when admin login to review user sign up requests, will trigger this sotred xss vuln.





arbitrary file creation/override in `authenticate.php`

- `Pacs/authenticate.php`
- `$_POST['formUsername']` will flow into `fopen($file, "w")` as part of $file, intended to create or append a file with username as filename in `MDPACS/PACS/FailedLogin` to count how many failed login tries
- this poc will create a file named test in `c:\` , file content will be 1.

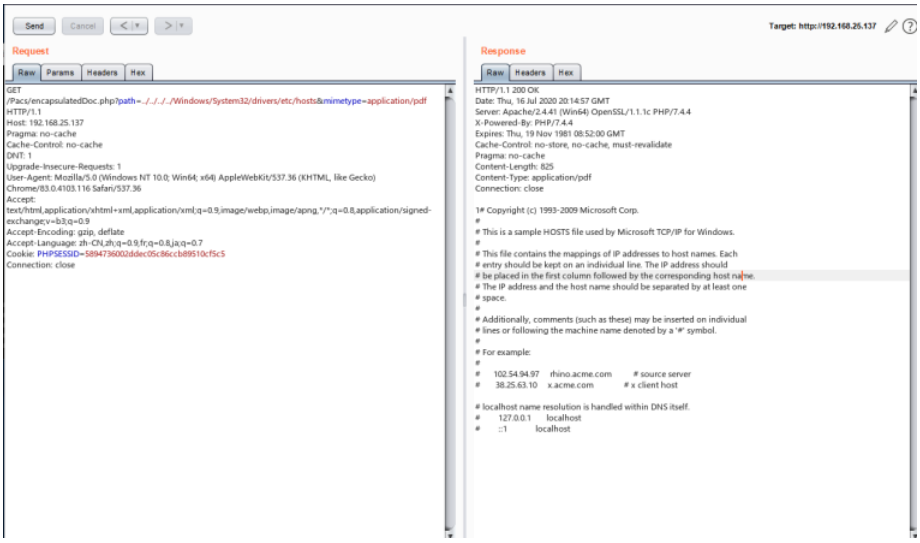


)

- this could be used to break the login mechanism by provide `formUsername=../php/security.php` to overwrite `security.php` , this will make other after-auth vuln more dangerous. or overwrite some important config file to cause a denial of service

arbitrary file read/SSRF in `encapsulatedDoc.php` and others

- `MDPACS/PACS/php/encapsulatedDoc.php`
- will not check wether path is legit, can read any file on the server.
- need login first, previously mentioned vulnerablity could bypass the login.

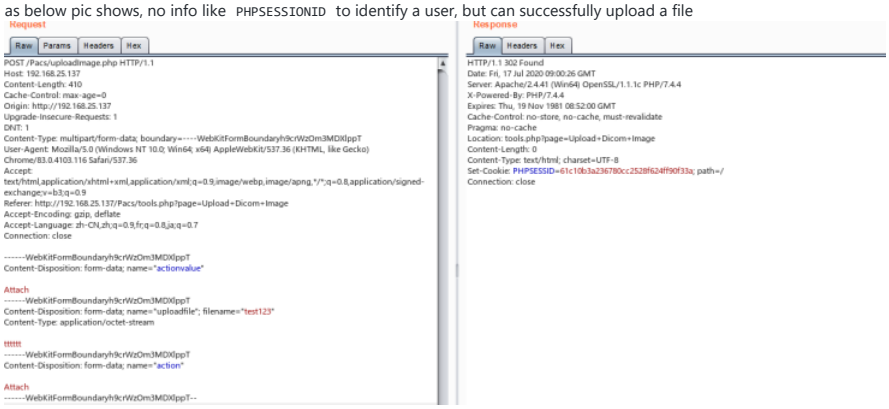


- there are similar behivor in `nocache.php` 、 `tempimage.php`

Broken Authentication

- `MDPACS/PACS/php/importWorklist.php` / `MDPACS/PACS/php/uploadImage.php` and missing authentication in `originalImage.php`
- those page should only let authenicated user to upload file, but due to broken auth, anyone can upload file.

- as below pic shows, no info like `PHPSESSIONID` to identify a user, but can successfully upload a file



multiple SQL Injection

- because the lack of sanitization or check, there are many after authenticated sql injection , for example in `studyNotes.php`
-