

Compliance Report

DISA (DoD) Application Security and Development (ASD) Security Technical Implementation Guide (STIG) V5R2

Description

The Application Security and Development (ASD) Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. This STIG provides security guidance for use throughout the application development lifecycle, to promote the development, integration, and updating of secure applications. Subjects covered in this document are: development, design, testing, conversions and upgrades for existing applications, maintenance, software configuration management, education, and training.

The Application Security and Development STIG is a requirement for all DoD developed, architected, and administered enterprise applications and systems connected to DoD networks. The Application Security and Development STIG is designed to be applied to all enterprise applications connected via the network.

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in the DISA STIG is assigned a Severity Category Code of CAT I, II, or III, with CAT I being the most severe.

CAT I: Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.

CAT II: Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.

CAT III: Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

Version: 5, Release: 2

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore, no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of the information in this report is taken from Security Technical Implementation Guide, developed by Defense Information Systems Agency for the Department of Defence and can be found at https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_ASD_V5R2_STIG.zip.

Scan Detail

Target	http://192.168.145.128/openemr
Scan Type	Full Scan
Start Time	Apr 11, 2023, 6:43:26 PM GMT-5
Scan Duration	30 minutes
Requests	655652
Average Response Time	117ms
Maximum Response Time	15582ms
Application Build	v15.5.230326230

Compliance at a Glance

CATEGORY

- 0** The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.
- 0** The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- 0** The application must enforce organization-defined discretionary access control policies over defined subjects and objects.
- 0** The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.
- 0** The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.
- 0** The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
- 0** The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.
- 10** The application must not write sensitive data into the application logs.
- 9** The application must protect audit information from any type of unauthorized read access.
- 0** The application must protect audit information from unauthorized modification.
- 0** The application must protect audit information from unauthorized deletion.
- 0** The application must protect audit tools from unauthorized access.
- 0** The application must protect audit tools from unauthorized modification.
- 0** The application must protect audit tools from unauthorized deletion.
- 1** The application must use cryptographic mechanisms to protect the integrity of audit information.

CATEGORY

- 10** Application audit tools must be cryptographically hashed.
- 10** The application must enforce access restrictions associated with changes to application configuration.
- 10** The application must audit who makes configuration changes to the application.
- 10** The application must be configured to disable non-essential capabilities.
- 10** The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.
- 10** The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.
- 0** The application must authenticate all network connected endpoint devices before establishing any connection.
- 2** Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.
- 0** The application must enforce a minimum 15-character password length.
- 0** The application must enforce password complexity by requiring that at least one upper-case character be used.
- 0** The application must enforce password complexity by requiring that at least one lower-case character be used.
- 0** The application must enforce password complexity by requiring that at least one numeric character be used.
- 0** The application must enforce password complexity by requiring that at least one special character be used.
- 0** The application must require the change of at least 8 of the total number of characters when passwords are changed.
- 0** The application must only store cryptographic representations of passwords.
- 1** The application must transmit only cryptographically-protected passwords.
- 6** The application must not display passwords/PINs as clear text.
- 1** The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for

authentication to a cryptographic module.

1 Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.

1 Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.

0 The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.

1 The application must utilize FIPS-validated cryptographic modules when signing application components.

1 The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.

1 The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.

1 The application must set the **HTTPOnly** flag on session cookies.

0 The application must set the **secure** flag on session cookies.

0 The application must not expose session IDs.

0 The application must destroy the session ID value and/or cookie on logoff or browser close.

0 Applications must use system-generated session identifiers that protect against session fixation.

0 Applications must validate session identifiers.

6 Applications must not use URL embedded session IDs.

0 The application must not re-use or recycle session IDs.

1 The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.

1 The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-

defined information system components.

- 1** The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.
- 0** XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.
- 0** The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.
- 2** The application must protect the confidentiality and integrity of transmitted information.
 - 1** The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).
 - 1** The application must maintain the confidentiality and integrity of information during preparation for transmission.
 - 1** The application must maintain the confidentiality and integrity of information during reception.
- 9** The application must not disclose unnecessary information to users.
- 6** The application must not store sensitive information in hidden fields.
- 0** The application must protect from Cross-Site Scripting (XSS) vulnerabilities.
- 0** The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.
- 0** The application must protect from command injection.
- 0** The application must protect from canonical representation vulnerabilities.
- 0** The application must validate all input.
- 0** The application must not be vulnerable to SQL Injection.
- 0** The application must not be vulnerable to XML-oriented attacks.
- 0** The application must not be subject to input handling vulnerabilities.
- 2** The application must generate error messages that provide information necessary for

CATEGORY

corrective actions without revealing information that could be exploited by adversaries.

- 0 The application must not be vulnerable to overflow attacks.
 - 26 Security-relevant software updates and patches must be kept up to date.
 - 1 The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.
 - 9 The application must not contain embedded authentication data.
 - 1 Application files must be cryptographically hashed prior to deploying to DoD operational networks.
 - 2 An application code review must be performed on the application.
 - 2 The application must not be subject to error handling vulnerabilities.
-

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.

STIG-ID: APSC-DV-000160

Severity: CAT II

No alerts in this category

The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

STIG-ID: APSC-DV-000460

Severity: CAT I

No alerts in this category

The application must enforce organization-defined discretionary access control policies over defined subjects and objects.

STIG-ID: APSC-DV-000470

Severity: CAT II

No alerts in this category

The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.

STIG-ID: APSC-DV-000480

Severity: CAT II

No alerts in this category

The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.

STIG-ID: APSC-DV-000490

Severity: CAT II

No alerts in this category

The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

STIG-ID: APSC-DV-000500

Severity: CAT II

No alerts in this category

The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.

Severity: CAT I

No alerts in this category

The application must not write sensitive data into the application logs.

STIG-ID: APSC-DV-000650

Severity: CAT II

Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/openemr/vendor/>

Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztagfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

<https://www.acunetix.com/websitemanagement/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```

GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36

```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
 >/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
 (/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEMokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

https://www.owasp.org/index.php/Full_Path_Disclosure

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception.

Consult the 'Attack details' section for more information about the affected page(s).

CWE

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/messages/messages.php on line 5137
**

- http://192.168.145.128/openemr/interface/main/messages/messages.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
 /var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
 /var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
<Warning>: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**
/var/www/html/openemr/library/ajax/i18n_generator.php** on line **5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
<Warning>: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**
/var/www/html/openemr/library/ajax/i18n_generator.php** on line **5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php
<Warning>: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**
/var/www/html/openemr/interface/login_screen.php** on line **5137
**
- http://192.168.145.128/openemr/interface/login_screen.php
<Warning>: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**
/var/www/html/openemr/interface/login_screen.php** on line **5137
**
- http://192.168.145.128/openemr/interface/login_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
<Warning>: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**
/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php** on line **5137
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
<Warning>: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-

```
minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
<b>/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php</b> on line <b>5137</b>
<br />
```

- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

References

PHP Runtime Configuration

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

Improper Error Handling

https://www_OWASP.org/index.php/Improper_Error_Handling

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files accessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Host: 192.168.145.128
Connection: Keep-alive

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

Availability Impact	None
----------------------------	------

Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstrap ...
...
```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
```

```
[ ! [B ...
```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

The application must protect audit information from any type of unauthorized read access.

STIG-ID: APSC-DV-001280

Severity: CAT II

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files accessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/

- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/>

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

http://192.168.145.128/

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr ...
...
```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
```

```
[ ! [B ...
```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/openemr/vendor/>

Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztagfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

<https://www.acunetix.com/websitemanagement/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```

GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36

```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
 >/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
 (/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEMokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

https://www.owasp.org/index.php/Full_Path_Disclosure

The application must protect audit information from unauthorized modification.

STIG-ID: APSC-DV-001290

Severity: CAT II

No alerts in this category

The application must protect audit information from unauthorized deletion.

STIG-ID: APSC-DV-001300

Severity: CAT II

No alerts in this category

The application must protect audit tools from unauthorized access.

STIG-ID: APSC-DV-001310

Severity: CAT II

No alerts in this category

The application must protect audit tools from unauthorized modification.

STIG-ID: APSC-DV-001320

Severity: CAT II

No alerts in this category

The application must protect audit tools from unauthorized deletion.

STIG-ID: APSC-DV-001330

Severity: CAT II

The application must use cryptographic mechanisms to protect the integrity of audit information.

STIG-ID: APSC-DV-001350

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
```

Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Application audit tools must be cryptographically hashed.

STIG-ID: APSC-DV-001360

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low

Availability Impact	None
---------------------	------

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

CWE

CWE-209

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/messages/messages.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-

minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/i18n_generator.php on line 5137

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**/var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEMokIFFZN%2CUpmA0oNxhYRlFnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files accessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...  
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None

Availability Impact	None
---------------------	------

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...
```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
[! [B ...
```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None

Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
>/var/www/html/index.html

- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```

GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure

https://www.owasp.org/index.php/Full_Path_Disclosure

The application must enforce access restrictions associated with changes to application configuration.

STIG-ID: APSC-DV-001410

Severity: CAT II

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

CWE

CWE-829

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote file inclusion.

<http://192.168.145.128/>



Verified

Current setting is : **allow_url_fopen = on**

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini

allow_url_fopen = 'off'

.htaccess

php_flag allow_url_fopen off

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

CWE

CWE-664

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote code inclusion.

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir`=

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can set `open_basedir` from `php.ini`

php.ini

`open_basedir = your_application_directory`

Cookies without HttpOnly flag set

One or more cookies don't have the `HttpOnly` flag set. When a cookie is set with the `HttpOnly` flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None

Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LoKuij2mG5Yq0pHL59ThbnUpzb;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/interface/main/main_screen.php

Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZHx; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/dicom_frame.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

```
Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L;  
path=/openemr/; SameSite=Strict
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1  
Host: 192.168.145.128  
Pragma: no-cache  
Cache-Control: no-cache  
accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app  
lication/signed-exchange;v=b3;q=0.9  
accept-language: en-US  
upgrade-insecure-requests: 1  
Accept-Encoding: gzip, deflate, br  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:  
default-src 'self';  
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/
- <http://192.168.145.128/openemr/public/assets/i18next/>
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
- <http://192.168.145.128/openemr/library/ajax/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
```

Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

CWE

CWE-16

Impact

Consult References for more information.

<http://192.168.145.128/>

Verified

- Missing object-src in CSP Declaration

- First observed on: <http://192.168.145.128/openemr/interface/login/login.php>
- CSP Value: frame-ancestors 'none'
- CSP Source: header

- **Summary:** Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
- **Impact:** N/A
- **Remediation:** Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
- **References:**
 - N/A

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

None

<http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- <http://192.168.145.128/openemr/composer.lock>
- <http://192.168.145.128/openemr/LICENSE>
- <http://192.168.145.128/openemr/Documentation/INSTALL>
- <http://192.168.145.128/openemr/Documentation/README.phpacl>
- <http://192.168.145.128/openemr/library/api.inc>
- <http://192.168.145.128/openemr/library/auth.inc>
- <http://192.168.145.128/openemr/library/calendar.inc>
- http://192.168.145.128/openemr/library/direct_message_check.inc
- <http://192.168.145.128/openemr/library/encounter.inc>
- <http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss>
- <http://192.168.145.128/openemr/library/forms.inc>
- <http://192.168.145.128/openemr/library/group.inc>
- <http://192.168.145.128/openemr/library/lab.inc>
- <http://192.168.145.128/openemr/library/lists.inc>
- http://192.168.145.128/openemr/library/options_listadd.inc
- <http://192.168.145.128/openemr/library/patient.inc>
- <http://192.168.145.128/openemr/library/pid.inc>
- <http://192.168.145.128/openemr/library/pnotes.inc>
- <http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss>
- <http://192.168.145.128/openemr/library/registry.inc>
- <http://192.168.145.128/openemr/library/report.inc>

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low

Confidentiality	None
Integrity Impact	None
Availability Impact	None

Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

<http://192.168.145.128/>

Locations without Permissions-Policy header:

- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/library/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/
- http://192.168.145.128/openemr/interface/main/tabs/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/main/main_screen.php
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/main/messages/messages.php
- http://192.168.145.128/openemr/public/assets/jquery/dist/
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
- http://192.168.145.128/openemr/public/assets/select2/
- http://192.168.145.128/openemr/library/js/vendors/
- http://192.168.145.128/openemr/interface/login/login.php
- http://192.168.145.128/openemr/interface/main/calendar/
- http://192.168.145.128/openemr/public/assets/jquery/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/Documentation/help_files/
- http://192.168.145.128/openemr/public/assets/i18next/

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed

Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- <http://192.168.145.128/openemr/public/assets/checklist-model/>
Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- <http://192.168.145.128/openemr/public/assets/checklist-model/>
Script SRC: https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js

Request

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the <https://example.com/example-framework.js> script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js">
```

integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous">></script>

References

Subresource Integrity

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator

<https://www.srihash.org/>

The application must audit who makes configuration changes to the application.

STIG-ID: APSC-DV-001420

Severity: CAT II

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

CWE

CWE-829

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None

Availability Impact	None
---------------------	------

Impact

Application dependant - possible remote file inclusion.

<http://192.168.145.128/>



Verified

Current setting is : **allow_url_fopen = on**

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini

allow_url_fopen = 'off'

.htaccess

php_flag allow_url_fopen off

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

CWE

CWE-664

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low

Base Score	0.0
Attack Vector	Network

Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote code inclusion.

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir=`

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can set `open_basedir` from `php.ini`

php.ini

`open_basedir = your_application_directory`

Cookies without HttpOnly flag set

One or more cookies don't have the `HttpOnly` flag set. When a cookie is set with the `HttpOnly` flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required

Availability Impact	None
----------------------------	------

Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- http://192.168.145.128/openemr/interface/login/login.php

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LOkuij2mG5Yq0pHL59ThbnUpzb;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/calendar/index.php

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/calendar/index.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
```

```
path=/openemr/; SameSite=Strict  
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;  
path=/openemr/; SameSite=Strict  
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/main_screen.php

```
Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J;  
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

```
Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZHx;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/dicom_frame.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

```
Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L;
path=/openemr/; SameSite=Strict
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:  
default-src 'self';  
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/
- <http://192.168.145.128/openemr/public/assets/i18next/>
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
- <http://192.168.145.128/openemr/library/ajax/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

CWE

CWE-16

Impact

Consult References for more information.

<http://192.168.145.128/>

Verified

- Missing object-src in CSP Declaration
 - First observed on: <http://192.168.145.128/openemr/interface/login/login.php>
 - CSP Value: frame-ancestors 'none'
 - CSP Source: header
 - Summary: Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
 - Impact: N/A
 - Remediation: Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
 - References:
 - N/A

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

None

<http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- http://192.168.145.128/openemr/composer.lock
- http://192.168.145.128/openemr/LICENSE
- http://192.168.145.128/openemr/Documentation/INSTALL
- http://192.168.145.128/openemr/Documentation/README.phpgacl
- http://192.168.145.128/openemr/library/api.inc
- http://192.168.145.128/openemr/library/auth.inc
- http://192.168.145.128/openemr/library/calendar.inc
- http://192.168.145.128/openemr/library/direct_message_check.inc
- http://192.168.145.128/openemr/library/encounter.inc
- http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss
- http://192.168.145.128/openemr/library/forms.inc
- http://192.168.145.128/openemr/library/group.inc
- http://192.168.145.128/openemr/library/lab.inc
- http://192.168.145.128/openemr/library/lists.inc
- http://192.168.145.128/openemr/library/options_listadd.inc
- http://192.168.145.128/openemr/library/patient.inc
- http://192.168.145.128/openemr/library/pid.inc
- http://192.168.145.128/openemr/library/pnotes.inc
- http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss

- <http://192.168.145.128/openemr/library/registry.inc>
- <http://192.168.145.128/openemr/library/report.inc>

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None

Availability Impact	None
---------------------	------

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

http://192.168.145.128/

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Access Vector	Network
---------------	---------

Base Score	0.0
------------	-----

Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

<http://192.168.145.128/>

Locations without Permissions-Policy header:

- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/library/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/
- http://192.168.145.128/openemr/interface/main/tabs/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/main/main_screen.php
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/main/messages/messages.php
- http://192.168.145.128/openemr/public/assets/jquery/dist/
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
- http://192.168.145.128/openemr/public/assets/select2/
- http://192.168.145.128/openemr/library/js/vendors/
- http://192.168.145.128/openemr/interface/login/login.php
- http://192.168.145.128/openemr/interface/main/calendar/
- http://192.168.145.128/openemr/public/assets/jquery/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/Documentation/help_files/
- http://192.168.145.128/openemr/public/assets/i18next/

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
```

```
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- <http://192.168.145.128/openemr/public/assets/checklist-model/>
Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- <http://192.168.145.128/openemr/public/assets/checklist-model/>
Script SRC: https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js

Request

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFTvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the <https://example.com/example-framework.js> script, the browser must first compare the script to the

expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgccY5uykM6+R9GqQ8K/uxy9rx7HNQ1GY11kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References

[Subresource Integrity](#)

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

[SRI Hash Generator](#)

<https://www.srihash.org/>

The application must be configured to disable non-essential capabilities.

STIG-ID: APSC-DV-001500

Severity: CAT II

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

CWE

CWE-829

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed

Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote file inclusion.

<http://192.168.145.128/>



Verified

Current setting is : **allow_url_fopen = on**

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini

```
allow_url_fopen = 'off'
```

.htaccess

```
php_flag allow_url_fopen off
```

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

CWE

CWE-664

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote code inclusion.

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir=`

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can set `open_basedir` from `php.ini`

`php.ini`

`open_basedir = your_application_directory`

Cookies without HttpOnly flag set

One or more cookies don't have the `HttpOnly` flag set. When a cookie is set with the `HttpOnly` flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low

Confidentiality	None
Integrity Impact	None
Availability Impact	None

Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LOkuij2mG5Yq0pHL59ThbnUpzb;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/main_screen.php

```
Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZYx; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/library/dicom_frame.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052I; path=/openemr/; SameSite=Strict

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

`Content-Security-Policy:`

```
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/
- <http://192.168.145.128/openemr/public/assets/i18next/>

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
- <http://192.168.145.128/openemr/library/ajax/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

CWE

CWE-16

Impact

Consult References for more information.

- Missing object-src in CSP Declaration

- First observed on: <http://192.168.145.128/openemr/interface/login/login.php>
- CSP Value: frame-ancestors 'none'
- CSP Source: header
- Summary: Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
- Impact: N/A
- Remediation: Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
- References:
 - N/A

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

None

<http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- <http://192.168.145.128/openemr/composer.lock>
- <http://192.168.145.128/openemr/LICENSE>
- <http://192.168.145.128/openemr/Documentation/INSTALL>
- <http://192.168.145.128/openemr/Documentation/README.phpacl>
- <http://192.168.145.128/openemr/library/api.inc>
- <http://192.168.145.128/openemr/library/auth.inc>
- <http://192.168.145.128/openemr/library/calendar.inc>
- http://192.168.145.128/openemr/library/direct_message_check.inc
- <http://192.168.145.128/openemr/library/encounter.inc>
- <http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss>
- <http://192.168.145.128/openemr/library/forms.inc>
- <http://192.168.145.128/openemr/library/group.inc>
- <http://192.168.145.128/openemr/library/lab.inc>
- <http://192.168.145.128/openemr/library/lists.inc>
- http://192.168.145.128/openemr/library/options_listadd.inc

- http://192.168.145.128/openemr/library/patient.inc
- http://192.168.145.128/openemr/library/pid.inc
- http://192.168.145.128/openemr/library/pnotes.inc
- http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss
- http://192.168.145.128/openemr/library/registry.inc
- http://192.168.145.128/openemr/library/report.inc

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

Availability Impact	None
---------------------	------

Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

<http://192.168.145.128/>

Locations without Permissions-Policy header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/login/login.php>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/
- <http://192.168.145.128/openemr/public/assets/i18next/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js

Request

```

GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References

[Subresource Integrity](#)

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

[SRI Hash Generator](#)

<https://www.srihash.org/>

The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.

STIG-ID: APSC-DV-001620

Severity: CAT II

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

CWE

CWE-829

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low

Base Score	0.0
Attack Vector	Network

Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote file inclusion.

<http://192.168.145.128/>



Verified

Current setting is : **allow_url_fopen = on**

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini

allow_url_fopen = 'off'

.htaccess

php_flag allow_url_fopen off

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it.

open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

CWE

CWE-664

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote code inclusion.

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir`=

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can set `open_basedir` from `php.ini`

php.ini

`open_basedir = your_application_directory`

Cookies without HttpOnly flag set

One or more cookies don't have the `HttpOnly` flag set. When a cookie is set with the `HttpOnly` flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/> Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LOkuij2mG5Yq0pHL59ThbnUpzb;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/main_screen.php

```
Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZYx; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/dicom_frame.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

```
Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L;
path=/openemr/; SameSite=Strict
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:  
default-src 'self';  
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/

- <http://192.168.145.128/openemr/public/assets/i18next/>
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
- <http://192.168.145.128/openemr/library/ajax/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqggkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

CWE

CWE-16

Impact

Consult References for more information.

<http://192.168.145.128/>

Verified

- Missing object-src in CSP Declaration

- First observed on: <http://192.168.145.128/openemr/interface/login/login.php>
- CSP Value: frame-ancestors 'none'
- CSP Source: header
- Summary: Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
- Impact: N/A
- Remediation: Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
- References:
 - N/A

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

None

<http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- <http://192.168.145.128/openemr/composer.lock>
- <http://192.168.145.128/openemr/LICENSE>
- <http://192.168.145.128/openemr/Documentation/INSTALL>
- <http://192.168.145.128/openemr/Documentation/README.phpacl>
- <http://192.168.145.128/openemr/library/api.inc>
- <http://192.168.145.128/openemr/library/auth.inc>
- <http://192.168.145.128/openemr/library/calendar.inc>
- http://192.168.145.128/openemr/library/direct_message_check.inc
- <http://192.168.145.128/openemr/library/encounter.inc>
- <http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss>
- <http://192.168.145.128/openemr/library/forms.inc>
- <http://192.168.145.128/openemr/library/group.inc>
- <http://192.168.145.128/openemr/library/lab.inc>

- http://192.168.145.128/openemr/library/lists.inc
- http://192.168.145.128/openemr/library/options_listadd.inc
- http://192.168.145.128/openemr/library/patient.inc
- http://192.168.145.128/openemr/library/pid.inc
- http://192.168.145.128/openemr/library/pnotes.inc
- http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss
- http://192.168.145.128/openemr/library/registry.inc
- http://192.168.145.128/openemr/library/report.inc

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact**<http://192.168.145.128/>**

Locations without Permissions-Policy header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/login/login.php>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/
- <http://192.168.145.128/openemr/public/assets/i18next/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js

Request

```

GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References

[Subresource Integrity](#)

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

[SRI Hash Generator](#)

<https://www.srihash.org/>

The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.

STIG-ID: APSC-DV-001630

Severity: CAT II

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

CWE

CWE-829

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low

Base Score	0.0
Attack Vector	Network

Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote file inclusion.

<http://192.168.145.128/>



Verified

Current setting is : **allow_url_fopen = on**

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini

allow_url_fopen = 'off'

.htaccess

php_flag allow_url_fopen off

References

[Runtime Configuration](#)

<https://www.php.net/manual/en/filesystem.configuration.php>

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it.

open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

CWE

CWE-664

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Application dependant - possible remote code inclusion.

<http://192.168.145.128/>



Verified

Current setting is : `open_basedir`=

Observed on /openemr/interface/main/main_screen.php

Recommendation

You can set `open_basedir` from `php.ini`

php.ini

`open_basedir = your_application_directory`

Cookies without HttpOnly flag set

One or more cookies don't have the `HttpOnly` flag set. When a cookie is set with the `HttpOnly` flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LOkuij2mG5Yq0pHL59ThbnUpzb;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp;
path=/openemr/; SameSite=Strict
```

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpA0oNxhYRlFnqazp;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/main_screen.php

```
Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZYx; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/dicom_frame.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

```
Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L;
path=/openemr/; SameSite=Strict
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:  
default-src 'self';  
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.145.128/>

Paths without CSP header:

- <http://192.168.145.128/openemr/public/assets/>
- <http://192.168.145.128/openemr/library/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/>
- <http://192.168.145.128/openemr/interface/main/tabs/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/interface/>
- http://192.168.145.128/openemr/interface/main/main_screen.php
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- <http://192.168.145.128/openemr/interface/main/messages/messages.php>
- <http://192.168.145.128/openemr/public/assets/jquery/dist/>
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- <http://192.168.145.128/openemr/public/assets/select2/>
- <http://192.168.145.128/openemr/library/js/vendors/>
- <http://192.168.145.128/openemr/interface/main/calendar/>
- <http://192.168.145.128/openemr/public/assets/jquery/>
- <http://192.168.145.128/openemr/Documentation/>
- http://192.168.145.128/openemr/Documentation/help_files/

- <http://192.168.145.128/openemr/public/assets/i18next/>
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
- <http://192.168.145.128/openemr/library/ajax/>

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqggkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

CWE

CWE-16

Impact

<http://192.168.145.128/>

Verified

- Missing object-src in CSP Declaration
 - First observed on: http://192.168.145.128/openemr/interface/login/login.php
 - CSP Value: frame-ancestors 'none'
 - CSP Source: header
 - Summary: Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
 - Impact: N/A
 - Remediation: Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
 - References:
 - N/A

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](#)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](#)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](#)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

None

<http://192.168.145.128/>

Verified

Pages where the content-type header is not specified:

- <http://192.168.145.128/openemr/composer.lock>
- <http://192.168.145.128/openemr/LICENSE>
- <http://192.168.145.128/openemr/Documentation/INSTALL>
- <http://192.168.145.128/openemr/Documentation/README.phpacl>
- <http://192.168.145.128/openemr/library/api.inc>
- <http://192.168.145.128/openemr/library/auth.inc>
- <http://192.168.145.128/openemr/library/calendar.inc>
- http://192.168.145.128/openemr/library/direct_message_check.inc
- <http://192.168.145.128/openemr/library/encounter.inc>
- <http://192.168.145.128/openemr/interface/themes/colors/utilities/batch-payments.scss>
- <http://192.168.145.128/openemr/library/forms.inc>
- <http://192.168.145.128/openemr/library/group.inc>
- <http://192.168.145.128/openemr/library/lab.inc>

- http://192.168.145.128/openemr/library/lists.inc
- http://192.168.145.128/openemr/library/options_listadd.inc
- http://192.168.145.128/openemr/library/patient.inc
- http://192.168.145.128/openemr/library/pid.inc
- http://192.168.145.128/openemr/library/pnotes.inc
- http://192.168.145.128/openemr/interface/themes/core/patient/demographics.scss
- http://192.168.145.128/openemr/library/registry.inc
- http://192.168.145.128/openemr/library/report.inc

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact**http://192.168.145.128/**

Locations without Permissions-Policy header:

- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/library/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/
- http://192.168.145.128/openemr/interface/main/tabs/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/main/main_screen.php
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/main/messages/messages.php
- http://192.168.145.128/openemr/public/assets/jquery/dist/
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
- http://192.168.145.128/openemr/public/assets/select2/
- http://192.168.145.128/openemr/library/js/vendors/
- http://192.168.145.128/openemr/interface/login/login.php
- http://192.168.145.128/openemr/interface/main/calendar/
- http://192.168.145.128/openemr/public/assets/jquery/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/Documentation/help_files/
- http://192.168.145.128/openemr/public/assets/i18next/

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://192.168.145.128/openemr/public/assets/checklist-model/>

Pages where SRI is not implemented:

- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- http://192.168.145.128/openemr/public/assets/checklist-model/

Script SRC: https://cdn.rawgit.com/google/code-prettify/master/loader/run_prettify.js

Request

```

GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFtvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"
crossorigin="anonymous"></script>
```

References

[Subresource Integrity](#)

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

[SRI Hash Generator](#)

<https://www.srihash.org/>

The application must authenticate all network connected endpoint devices before establishing any connection.

STIG-ID: APSC-DV-001650

Severity: CAT II

No alerts in this category

Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.

STIG-ID: APSC-DV-001660

Severity: CAT II

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

http://192.168.145.128/

Forms with credentials sent in clear text:

- http://192.168.145.128/openemr/interface/login/login.php

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad0e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must enforce a minimum 15-character password length.

STIG-ID: APSC-DV-001680

Severity: CAT I

No alerts in this category

The application must enforce password complexity by requiring that at least one upper-case character be used.

STIG-ID: APSC-DV-001690

Severity: CAT II

No alerts in this category

The application must enforce password complexity by requiring that at least one lower-case character be used.

STIG-ID: APSC-DV-001700

Severity: CAT II

No alerts in this category

The application must enforce password complexity by requiring that at least one numeric character be used.

STIG-ID: APSC-DV-001710

Severity: CAT II

No alerts in this category

The application must enforce password complexity by requiring that at least one special character be used.

STIG-ID: APSC-DV-001720

Severity: CAT II

No alerts in this category

The application must require the change of at least 8 of the total number of characters when passwords are changed.

STIG-ID: APSC-DV-001730

Severity: CAT II

No alerts in this category

The application must only store cryptographic representations of passwords.

STIG-ID: APSC-DV-001740

Severity: CAT I

No alerts in this category

The application must transmit only cryptographically-protected passwords.

STIG-ID: APSC-DV-001750

Severity: CAT I

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CWE

CWE-523

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://192.168.145.128/>

Forms with credentials sent in clear text:

- http://192.168.145.128/openemr/interface/login/login.php

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

The application must not display passwords/PINs as clear text.

STIG-ID: APSC-DV-001850

Severity: CAT I

Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/openemr/vendor/>

Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low

Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
 >/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)

- http://192.168.145.128/openemr/portal/
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

STIG-ID: APSC-DV-001860

Severity: CAT I

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.

STIG-ID: APSC-DV-001940

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	Partial
Availability Impact	None

User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.

STIG-ID: APSC-DV-001950

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.

STIG-ID: APSC-DV-001970

Severity: CAT II

No alerts in this category

The application must utilize FIPS-validated cryptographic modules when signing application components.

STIG-ID: APSC-DV-002020

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged

Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.

STIG-ID: APSC-DV-002030

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.

STIG-ID: APSC-DV-002040

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must set the **HTTPOnly** flag on session cookies.

STIG-ID: APSC-DV-002210

Severity: CAT II

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

CWE

CWE-1004

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Cookies can be accessed by client-side scripts.

<http://192.168.145.128/>

Verified

Cookies without HttpOnly flag set:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Set-Cookie: OpenEMR=PrCCihxJI%2CqG1CX0p7oP16LOkuij2mG5Yq0pHL59ThbnUpzb; path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFfZN%2CUpmA0oNxhYRlFnqazp; path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=ShqPYxekgSvnztaqfRyq0J2b-9njDrQM43HnaYAqgkzuKU15; path=/openemr/; SameSite=Strict
```

- <http://192.168.145.128/openemr/interface/main/calendar/index.php>

```
Set-Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFfZN%2CUpmA0oNxhYRlFnqazp; path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/interface/main/main_screen.php

Set-Cookie: OpenEMR=9Y8ac4csy6RvRyifO9Yg1001but4qLPoxBtXKUc8Kxsv0A5J; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/interface/main/tabs/main.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/portal/messaging/messages.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/portal/messaging/secure_chat.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/library/ajax/execute_background_services.php

Set-Cookie: OpenEMR=W75Ms9wo0idBaU3cwZ3komU0jWJ6XL2Pyzz3muoDQyhZHx; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheet.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/common_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- <http://192.168.145.128/openemr/library/FeeSheetHtml.class.php>

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/cqm_amc_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/fee_sheet_help.php

Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/openemr/; SameSite=Strict

- http://192.168.145.128/openemr/Documentation/help_files/procedure_provider_help.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/library/dicom_frame.php

```
Set-Cookie: OpenEMR=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;  
path=/openemr/; SameSite=Strict
```

- http://192.168.145.128/openemr/Documentation/help_files/report_dashboard_help.php

```
Set-Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFTvIbo%2CVxmCKL9iQGY052L;  
path=/openemr/; SameSite=Strict
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1  
Host: 192.168.145.128  
Pragma: no-cache  
Cache-Control: no-cache  
accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
accept-language: en-US  
upgrade-insecure-requests: 1  
Accept-Encoding: gzip, deflate, br  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

The application must set the secure flag on session cookies.

Severity: CAT II

No alerts in this category

The application must not expose session IDs.

STIG-ID: APSC-DV-002230

Severity: CAT I

No alerts in this category

The application must destroy the session ID value and/or cookie on logoff or browser close.

STIG-ID: APSC-DV-002240

Severity: CAT I

No alerts in this category

Applications must use system-generated session identifiers that protect against session fixation.

STIG-ID: APSC-DV-002250

Severity: CAT II

No alerts in this category

Applications must validate session identifiers.

STIG-ID: APSC-DV-002260

Severity: CAT II

Applications must not use URL embedded session IDs.

STIG-ID: APSC-DV-002270

Severity: CAT II

Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/openemr/vendor/>

Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- http://192.168.145.128/openemr/bin
- http://192.168.145.128/openemr/sql
- http://192.168.145.128/openemr/config
- http://192.168.145.128/openemr/tests
- http://192.168.145.128/openemr/src

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
jabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
 >/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
 (/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)

- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

https://www.owasp.org/index.php/Full_Path_Disclosure

The application must not re-use or recycle session IDs.

STIG-ID: APSC-DV-002280

Severity: CAT II

No alerts in this category

The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption,

key exchange, digital signature, and hash functionality.

STIG-ID: APSC-DV-002290

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3e3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.

STIG-ID: APSC-DV-002340

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.

STIG-ID: APSC-DV-002350

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.

Severity: CAT II

No alerts in this category

The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.

STIG-ID: APSC-DV-002400

Severity: CAT II

No alerts in this category

The application must protect the confidentiality and integrity of transmitted information.

STIG-ID: APSC-DV-002440

Severity: CAT I

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CWE

CWE-523

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low

Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://192.168.145.128/>

Forms with credentials sent in clear text:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must implement cryptographic mechanisms to prevent unauthorized disclosure of

information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).

STIG-ID: APSC-DV-002450

Severity: CAT II

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CWE

CWE-523

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://192.168.145.128/>

Forms with credentials sent in clear text:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Form name: login_form
```

```
Form action: ../main/main_screen.php?auth=login&site=default
```

Form method: POST

Password input: clearPass

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

The application must maintain the confidentiality and integrity of information during preparation for transmission.

STIG-ID: APSC-DV-002460

Severity: CAT II

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CWE

CWE-523

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://192.168.145.128/>

Forms with credentials sent in clear text:

- <http://192.168.145.128/openemr/interface/login/login.php>

```

Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass

```

Request

```

GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36

```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

The application must maintain the confidentiality and integrity of information during reception.

STIG-ID: APSC-DV-002470

Severity: CAT II

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

CWE

CWE-523

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://192.168.145.128/>

Forms with credentials sent in clear text:

- <http://192.168.145.128/openemr/interface/login/login.php>

```
Form name: login_form
Form action: ../main/main_screen.php?auth=login&site=default
Form method: POST
Password input: clearPass
```

Request

```
GET /openemr/interface/login/login.php?site=default HTTP/1.1
Host: 192.168.145.128
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

The application must not disclose unnecessary information to users.

STIG-ID: APSC-DV-002480

Severity: CAT II

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

CWE

CWE-209

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low

Base Score	5.3
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/messages/messages.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-

minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/i18n_generator.php on line 5137

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**/var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
**/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
**/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEMokIFFZN%2CUpmA0oNxhYRlFnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files accessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low

Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/
- http://192.168.145.128/openemr/library/ajax/
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- http://192.168.145.128/openemr/public/assets/select2/dist/css/
- http://192.168.145.128/openemr/public/assets/moment/min/
- http://192.168.145.128/openemr/interface/product_registration/
- http://192.168.145.128/openemr/Documentation/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/
- http://192.168.145.128/openemr/interface/main/tabs/js/
- http://192.168.145.128/openemr/public/assets/i18next/dist/
- http://192.168.145.128/openemr/public/assets/i18next/dist/umd/
- http://192.168.145.128/openemr/public/
- http://192.168.145.128/openemr/public/assets/i18next/
- http://192.168.145.128/openemr/public/assets/knockout/
- http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...  
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

[CWE-548: Exposure of Information Through Directory Listing](#)

<https://cwe.mitre.org/data/definitions/548.html>

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None

Availability Impact	None
---------------------	------

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface
```

```
The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstr
...
```

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md>

File contents (first 100 characters):

```
# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)
[! [B ...
```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None

Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
>/var/www/html/index.html

- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr
- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```

GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure

https://www.owasp.org/index.php/Full_Path_Disclosure

The application must not store sensitive information in hidden fields.

STIG-ID: APSC-DV-002485

Severity: CAT I

Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/openemr/vendor/>

Request

```
GET /openemr/vendor/composer/installed.json HTTP/1.1
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzXjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to vendors directory

References

[Composer Basic usage](#)

<https://getcomposer.org/doc/01-basic-usage.md>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

Availability Impact	None
---------------------	------

Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqqkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics

data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

<https://www.acunetix.com/websitemanagement/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzxjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
>/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

https://www.owasp.org/index.php/Full_Path_Disclosure

The application must protect from Cross-Site Scripting (XSS) vulnerabilities.

STIG-ID: APSC-DV-002490

Severity: CAT I

No alerts in this category

The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.

STIG-ID: APSC-DV-002500

Severity: CAT II

No alerts in this category

The application must protect from command injection.

STIG-ID: APSC-DV-002510

Severity: CAT I

No alerts in this category

The application must protect from canonical representation vulnerabilities.

STIG-ID: APSC-DV-002520

Severity: CAT II

No alerts in this category

The application must validate all input.

STIG-ID: APSC-DV-002530

Severity: CAT II

No alerts in this category

The application must not be vulnerable to SQL Injection.

STIG-ID: APSC-DV-002540

Severity: CAT I

No alerts in this category

The application must not be vulnerable to XML-oriented attacks.

STIG-ID: APSC-DV-002550

Severity: CAT I

No alerts in this category

The application must not be subject to input handling vulnerabilities.

STIG-ID: APSC-DV-002560

Severity: CAT I

No alerts in this category

The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

STIG-ID: APSC-DV-002570

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

These messages may also contain the location of the file that produced an unhandled exception.

Consult the 'Attack details' section for more information about the affected page(s).

CWE

CWE-209

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cons

ole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/main_screen.php on line 5137

- http://192.168.145.128/openemr/interface/main/main_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/interface/login/login.php on line 5137

- http://192.168.145.128/openemr/interface/login/login.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
 /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137

- http://192.168.145.128/openemr/library/ajax/i18n_generator.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
 /var/www/html/openemr/interface/login_screen.php on line 5137

- http://192.168.145.128/openemr/interface/login_screen.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
 (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
 /var/www/html/openemr/interface/login_screen.php on line 5137

- http://192.168.145.128/openemr/interface/login_screen.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
**
**
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYRlFnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

Internal IP addresses

Secrets (passwords, keys, tokens...)
Operating system distributions
Software version numbers
Missing security patches
Application stack traces
SQL statements
Location of sensitive files (backups, temporary files...)
Location of sensitive resources (databases, caches, code repositories...)

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

The application must not be vulnerable to overflow attacks.

STIG-ID: APSC-DV-002590

Severity: CAT I

No alerts in this category

Security-relevant software updates and patches must be kept up to date.

Severity: CAT II

Vulnerable package dependencies [high]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

CWE

CWE-1104

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-41343

Title: Files or Directories Accessible to External Parties

Description: registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-552

References:

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2023-23924

Title: Incorrect Authorization

Description: Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-863

References:

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2023-24813

Title: Interpretation Conflict

Description: Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-436

References:

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

Package: guzzlehttp/guzzle

Version: 7.4.4

CVE: CVE-2022-31091

Title:

Description: Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: NVD-CWE-noinfo

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

Package: guzzlehttp/guzzle

Version: 7.4.4

CVE: CVE-2022-31090

Title: Exposure of Sensitive Information to an Unauthorized Actor

Description: Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: CWE-200

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

Package: knplabs/knp-snappy

Version: 1.4.1

CVE: CVE-2023-28115

Title: Deserialization of Untrusted Data

Description: Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-502

References:

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>
- <https://github.com/KnpLabs/snappy/pull/469>

Package: phpseclib/phpseclib

Version: 2.0.37

CVE: CVE-2023-27560

Title: Loop with Unreachable Exit Condition ('Infinite Loop')

Description: Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE: CWE-835

References:

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-26119

Title:

Description: Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template_object can be accessed in sandbox mode.

CVSS V2: AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CWE: NVD-CWE-noinfo

References:

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-26120

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2017-1000480

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS V3: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- https://github.com/smarty-php/smarty/blob/master/change_log.txt
- <https://www.debian.org/security/2018/dsa-4094>
- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-13982

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Smarty_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>

- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-21408

Title: Improper Input Validation

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-20

References:

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-29454

Title: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-74

References:

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>

- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2022-29221

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdb5c9874262b702ccddd>
- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: twig/twig

Version: 3.4.1

CVE: CVE-2022-39261

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQ0763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYVJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAZZIPV2GUD/>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

CWE

CWE-937

CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Consult References for more information.

http://192.168.145.128/

Confidence: 95%

- AngularJS 1.4.8

- URL: <https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.4.8/angular.js>
- Detection method: The library's name and version were determined based on the file's CDN URI.
- CVE-ID: CVE-2020-7676
- Description: Prototype pollution / Cross-Site Scripting.
- References:
 - <https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cf5e2e592841db743a>
 - <https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>
 - <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

Request

```
GET /openemr/public/assets/checklist-model/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=g3GhfkD5xIsb3Ge5m8KYxfe43LFTvIbo%2CVxmCKL9iQGY052L
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

http://192.168.145.128/

Verified

- jQuery UI 1.12.1

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique

syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1Sl%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.12.1**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1Sl%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Chrome/109.0.0.0 Safari/537.36

Host: 192.168.145.128

Connection: Keep-alive

http://192.168.145.128/

Verified

- **jQuery 1.12.4**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/external/jquery/jquery.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
 - <https://github.com/jquery/jquery/issues/2432>
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jQuery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/public/assets/jquery-ui/external/jquery/jquery.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/jquery-ui/
Cookie: OpenEMR=6WeVd6ZCNQZ1gcdzS-0v%2CJShmKVZumFVDGJv2At8hAWUVeJ3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.10.2**

- URL: <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/jquery.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jQuery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/public/assets/jquery-datetimepicker/jquery.js HTTP/1.1
Host: 192.168.145.128
accept: */*
accept-language: en-US
cookie: OpenEMR=SMoagLf26TS1Vx2PDvSGHTEJwG3t9eYeCWJyUPD7WNEu5a8X
Referer: http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>

- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

Request

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.8.10**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2010-5312, CVE-2016-7103
- Description: Title cross-site scripting vulnerability / XSS in dialog closeText
- References:
 - <http://bugs.jqueryui.com/ticket/6016>
 - <https://nodesecurity.io/advisories/127>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
 - <https://www.cvedetails.com/cve/CVE-2016-7103/>

Request

```
GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
```

Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

<http://192.168.145.128/>

Verified

- **jQuery 1.5.1**

- URL: <http://192.168.145.128/openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
 - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
 - <http://research.insecurelabs.org/jquery/test/>
 - <http://bugs.jquery.com/ticket/11290>
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jQuery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

GET /openemr/interface/super/rules/www/js/cdr-multiselect/jquery.min.js HTTP/1.1
Acunetix-Aspect: enabled

Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

<http://192.168.145.128/> Verified

- **jQuery 1.4.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
 - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
 - <http://research.insecurelabs.org/jquery/test/>
 - <http://bugs.jquery.com/ticket/11290>
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.lo.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jQuery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery.treeview-1.4.1/lib/jquery.js
HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

http://192.168.145.128/

Verified

- **jQuery UI 1.11.4**

- URL: http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.11.4**

- URL: http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
 - <https://nodesecurity.io/advisories/127>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
 - <https://www.cvedetails.com/cve/CVE-2016-7103/>

Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.8.0**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js
- Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources -

even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <http://bugs.jquery.com/ticket/11290>
- <http://research.insecurelabs.org/jquery/test/>
- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.0.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.8.2**

- o URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.2.min.js
- o Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- o Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources -

even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <http://bugs.jquery.com/ticket/11290>
- <http://research.insecurelabs.org/jquery/test/>
- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.2.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery 1.8.3**

- o URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js
- o Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- o Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources -

even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- o References:

- <http://bugs.jquery.com/ticket/11290>
- <http://research.insecurelabs.org/jquery/test/>
- <https://github.com/jquery/jquery/issues/2432>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-1.8.3.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 80%

- **jQuery UI 1.9.2**

- o URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js
- o Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
- o CVE-ID: [CVE-2021-41184](#)
- o Description: XSS in the 'of' option of the '.position()' util
- o References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.9.2**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwcc>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.custom.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2021-41184
- Description: XSS in the 'of' option of the '.position()' util
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Dialog 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
 - <https://nodesecurity.io/advisories/127>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
 - <https://www.cvedetails.com/cve/CVE-2016-7103/>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Confidence: 95%

- **jQuery UI Datepicker 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58ad3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKwzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

CWE

CWE-1104

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-0085

Title: Server-Side Request Forgery (SSRF)

Description: Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

CVSS V2: AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CWE: CWE-918

References:

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-2400

Title: External Control of File Name or Path

Description: External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE: CWE-73

References:

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aec1efec9213e87098d42eb09439e7ee0bb6a>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-16831

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted_dir protection mechanism via a file:../../ substring in an include statement.

CVSS V2: AV:N/AC:M/Au:N/C:C/I:N/A:N

CVSS V3: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/smarty-php/smarty/issues/486>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-25047

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty_function_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE: CWE-79

References:

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2023-28447

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CWE: CWE-79

References:

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

CWE

CWE-937

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Consult References for more information.

<http://192.168.145.128/>

Verified

- jQuery UI Dialog 1.12.1

- URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

- o References:

- <https://jqueryui.com/download/>

Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.12.1**

- o URL: <http://192.168.145.128/openemr/public/assets/jquery-ui/jquery-ui.js>
- o Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- o References:
 - <https://jqueryui.com/download/>

Request

```
GET /openemr/public/assets/jquery-ui/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/Documentation/help_files/openemr_installation_help.php
Cookie: OpenEMR=d40D5DeYlSqGsuSImcMvd1XbnUvSB1S1%2CNItgLcdHnpIKp4G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.11.4**

- URL: http://192.168.145.128/openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
 - <https://jqueryui.com/download/>

Request

```
GET /openemr/interface/forms/eye_mag/js/jquery-ui-1-11-4/jquery-ui.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

<http://192.168.145.128/>

Verified

- **jQuery UI Tooltip 1.10.3**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- References:
 - <https://jqueryui.com/download/>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/jquery-ui.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
```

Host: 192.168.145.128
Connection: Keep-alive

<http://192.168.145.128/>

Confidence: 95%

- **Modernizr 2.6.2**

- URL: http://192.168.145.128/openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js
- Detection method: The library's name and version were determined based on the file's name.
- References:
 - <https://github.com/Modernizr/Modernizr/releases>

Request

```
GET /openemr/interface/modules/zend_modules/public/js/lib/modernizr-2.6.2.min.js HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login_screen.php
Cookie: OpenEMR=2biStMm-fnsHdYMyYHQGKWzilsysHJvKUerLZszaOGdltFQQ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.

STIG-ID: APSC-DV-003100

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

The application must not contain embedded authentication data.

STIG-ID: APSC-DV-003110

Severity: CAT I

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

CWE

CWE-209

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in

**/var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in

**/var/www/html/openemr/interface/main/main_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/main_screen.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in

**/var/www/html/openemr/interface/main/messages/messages.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/messages/messages.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in

**/var/www/html/openemr/interface/main/messages/messages.php on line 5137
**
- http://192.168.145.128/openemr/interface/main/messages/messages.php

Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in

**/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php

Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in

**/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137
**

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/login/login.php on line 5137
**
- http://192.168.145.128/openemr/interface/login/login.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/interface/login/login.php on line 5137
**
- http://192.168.145.128/openemr/interface/login/login.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-

```
php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
<b>/var/www/html/openemr/interface/login_screen.php</b> on line <b>5137</b><br />
```

- http://192.168.145.128/openemr/interface/login_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137

- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137

- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Base Score	3.1
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged

Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Development configuration files:

- <http://192.168.145.128/openemr/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/composer.json>

composer.json => Composer configuration file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/composer.lock>

composer.lock => Composer lock file. Composer is a dependency manager for PHP.

- <http://192.168.145.128/openemr/package-lock.json>

package-lock.json => npm file. This file keeps track of the exact version of every package that is installed.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/package.json>

package.json => Grunt configuration file. Grunt is a JavaScript task runner.

- <http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/bower.json>

bower.json => Bower manifest file. Bower is a package manager for the web.

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
```

Recommendation

Remove or restrict access to all configuration files accessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://192.168.145.128/>

Verified

Folders with directory listing enabled:

- http://192.168.145.128/openemr/interface/
- http://192.168.145.128/openemr/interface/login/
- http://192.168.145.128/openemr/interface/main/messages/css/
- http://192.168.145.128/openemr/public/assets/
- http://192.168.145.128/openemr/public/assets/bootstrap/dist/js/
- http://192.168.145.128/openemr/interface/main/messages/js/
- http://192.168.145.128/openemr/public/assets/moment/

- <http://192.168.145.128/openemr/library/ajax/>
- http://192.168.145.128/openemr/interface/main/dated_reminders/
- <http://192.168.145.128/openemr/public/assets/select2/dist/css/>
- <http://192.168.145.128/openemr/public/assets/moment/min/>
- http://192.168.145.128/openemr/interface/product_registration/
- <http://192.168.145.128/openemr/Documentation/>
- <http://192.168.145.128/openemr/public/assets/bootstrap/dist/>
- <http://192.168.145.128/openemr/interface/main/tabs/js/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/>
- <http://192.168.145.128/openemr/public/assets/i18next/dist/umd/>
- <http://192.168.145.128/openemr/public/>
- <http://192.168.145.128/openemr/public/assets/i18next/>
- <http://192.168.145.128/openemr/public/assets/knockout/>
- <http://192.168.145.128/openemr/public/assets/hotkeys-js/dist/>

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.

On IIS directory listings are disabled by default.

For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like

```
<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ...
</Directory>
```

To disable directory listing for that directory you need to remove the 'Indexes' option.

References

Documentation files

One or more documentation files (e.g. `readme.txt`, `changelog.txt`, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

CWE

CWE-538

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

<http://192.168.145.128/>

Documentation files:

- <http://192.168.145.128/openemr/README.md>

File contents (first 100 characters):

```
! [Syntax Status] (https://github.com/openemr/openemr/workflows/Syntax/badge.svg?branch=rel-700)
! [Sty ...
```

- <http://192.168.145.128/openemr/interface/README.md>

File contents (first 100 characters):

```
# OpenEMR-interface

The OpenEMR UI is built with [SASS] (https://sass-lang.com/) on top of a bootstrap
...
• http://192.168.145.128/openemr/public/assets/jquery-datetimepicker/README.md
File contents (first 100 characters):

# jQuery DateTimePicker
[Demo and Documentation] (https://xdsoft.net/jqplugins/datetimepicker/)

[! [B ...
```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file accessible from internet.

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

Availability Impact	None
---------------------	------

Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive directories:

- <http://192.168.145.128/openemr/bin>
- <http://192.168.145.128/openemr/sql>
- <http://192.168.145.128/openemr/config>
- <http://192.168.145.128/openemr/tests>
- <http://192.168.145.128/openemr/src>

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqqkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitetecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics

data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<http://192.168.145.128/>

Possible sensitive files:

- <http://192.168.145.128/openemr/admin.php>

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: shxrinco/hemy
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

<https://www.acunetix.com/websitemanagement/webserver-security/>

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Impact

Email addresses posted on Web sites may attract spam.

<http://192.168.145.128/>

Emails found:

- http://192.168.145.128/openemr/acknowledge_license_cert.html
ajabour@iupui.edu
- http://192.168.145.128/openemr/acknowledge_license_cert.html
andres@paglayan.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
superarnab@gmail.com

- http://192.168.145.128/openemr/acknowledge_license_cert.html
drbowen@bowenmd.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
bss@iguanasuicide.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
brady.g.miller@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
pandi.param@capminds.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stephen.waite@cmsvt.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
amit@comlinkinc.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sbhayani@communitybehavioralhealth.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ramesh@ensoftek.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
george.tye@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
stone@annashaegrp.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
fndtn357@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
sherwin@affordablecustomehr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
julia.longtin@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
ptspohnpei@gmail.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
kevin.y@integralemr.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
openemr@lillysystems.com
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mscltd@earthlink.net
- http://192.168.145.128/openemr/acknowledge_license_cert.html
mdsupport@users.sf.net

Request

```
GET /openemr/acknowledge_license_cert.html HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVs1YyH8tuel82CU%2CjzxjI%2C2Xj1wHpg%2CMTJEHOAPWa5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)

https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

<http://192.168.145.128/>

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Possible sensitive information disclosure.

<http://192.168.145.128/>

Pages with paths being disclosed:

- http://192.168.145.128/openemr/interface/main/main_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/messages/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/login/login.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/
>/var/www/html/index.html
- http://192.168.145.128/openemr/interface/login_screen.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/interface/main/tabs/main.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/messages.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/portal/messaging/secure_chat.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/Readme_edihistory.html
/var/www/htdocs/openemr/sites/
- http://192.168.145.128/openemr/Documentation/help_files/add_edit_transactions_dashboard_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/README-Log-Backup.txt
/var/www/openemr

- http://192.168.145.128/openemr/Documentation/help_files/adminacl_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/cms_1500_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheet.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/common_help.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/library/FeeSheetHtml.class.php
(/var/www/html/openemr/vendor/adodb/adodb)
- http://192.168.145.128/openemr/Documentation/help_files/configure_orders_help.php
(/var/www/html/openemr/vendor/adodb/adodb)

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure](#)

https://www.owasp.org/index.php/Full_Path_Disclosure

Application files must be cryptographically hashed prior to deploying to DoD operational networks.

STIG-ID: APSC-DV-003140

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

An application code review must be performed on the application.

STIG-ID: APSC-DV-003170

Severity: CAT II

Vulnerable package dependencies [high]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

CWE

CWE-1104

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-41343

Title: Files or Directories Accessible to External Parties

Description: registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-552

References:

- <https://github.com/dompdf/dompdf/releases/tag/v2.0.1>
- <https://github.com/dompdf/dompdf/issues/2994>
- <https://github.com/dompdf/dompdf/pull/2995>
- <https://tantosec.com/blog/cve-2022-41343/>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2023-23924

Title: Incorrect Authorization

Description: Dompdf is an HTML to PDF converter. The URI validation on dompdf 2.0.1 can be bypassed on SVG parsing by passing `<image>` tags with uppercase letters. This may lead to arbitrary object unserialize on PHP < 8, through the `phar` URL wrapper. An attacker can exploit the vulnerability to call arbitrary URL with arbitrary protocols, if they can provide a SVG file to dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, that will lead to the very least to an arbitrary file deletion and even remote code execution, depending on classes that are available.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-863

References:

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-3cw5-7cxw-v5qg>
- <https://github.com/dompdf/dompdf/releases/tag/v2.0.2>
- <https://github.com/dompdf/dompdf/commit/7558f07f693b2ac3266089f21051e6b78c6a0c85>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2023-24813

Title: Interpretation Conflict

Description: Dompdf is an HTML to PDF converter written in php. Due to the difference in the attribute parser of Dompdf and php-svg-lib, an attacker can still call arbitrary URLs with arbitrary protocols. Dompdf parses the href attribute of `image` tags and respects `xlink:href` even if `href` is specified. However, php-svg-lib, which is later used to parse the svg file, parses the href attribute. Since `href` is respected if both `xlink:href` and `href` is specified, it's possible to bypass the protection on the Dompdf side by providing an empty `xlink:href` attribute. An attacker can exploit the vulnerability to call arbitrary URLs with arbitrary protocols if they provide an SVG file to the Dompdf. In PHP versions before 8.0.0, it leads to arbitrary unserialize, which will lead, at the very least, to arbitrary file deletion and might lead to remote code execution, depending on available classes. This vulnerability has been addressed in commit `95009ea98` which has been included in release version 2.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-436

References:

- <https://github.com/dompdf/dompdf/security/advisories/GHSA-56gj-mvh6-rp75>
- <https://github.com/dompdf/dompdf/commit/95009ea98230f9b084b040c34e3869ef3dccc9aa>

Package: guzzlehttp/guzzle

Version: 7.4.4

CVE: CVE-2022-31091

Title:

Description: Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: NVD-CWE-noinfo

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699>
- <https://www.debian.org/security/2022/dsa-5246>

Package: guzzlehttp/guzzle

Version: 7.4.4

CVE: CVE-2022-31090

Title: Exposure of Sensitive Information to an Unauthorized Actor

Description: Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT_HTTPAUTH` option to specify an `Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE: CWE-200

References:

- <https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fdb82>
- <https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r>
- <https://www.debian.org/security/2022/dsa-5246>

Package: knplabs/knp-snappy

Version: 1.4.1

CVE: CVE-2023-28115

Title: Deserialization of Untrusted Data

Description: Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to

version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-502

References:

- <https://github.com/KnpLabs/snappy/releases/tag/v1.4.2>
- <https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc>
- <https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c244427963fa2d92980b5d3>
- <https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6>
- <https://github.com/KnpLabs/snappy/blob/5126fb5b335ec929a226314d40cd8dad497c3d67/src/Knp/Snappy/AbstractGenerator.php#L670>

- <https://github.com/KnpLabs/snappy/pull/469>

Package: phpseclib/phpseclib

Version: 2.0.37

CVE: CVE-2023-27560

Title: Loop with Unreachable Exit Condition ('Infinite Loop')

Description: Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE: CWE-835

References:

- <https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440>
- <https://github.com/phpseclib/phpseclib/releases/tag/3.0.19>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-26119

Title:

Description: Smarty before 3.1.39 allows a Sandbox Escape because \$smarty.template_object can be accessed in sandbox mode.

CVSS V2: AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CWE: NVD-CWE-noinfo

References:

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>

- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-26120

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- <https://github.com/smarty-php/smarty/blob/master/CHANGELOG.md>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://security.gentoo.org/glsa/202105-06>
- <https://www.debian.org/security/2022/dsa-5151>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2017-1000480

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty 3 before 3.1.32 is vulnerable to a PHP code injection when calling fetch() or display() functions on custom resources that does not sanitize template name.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS V3: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- https://github.com/smarty-php/smarty/blob/master/change_log.txt
- <https://www.debian.org/security/2018/dsa-4094>
- <https://lists.debian.org/debian-lts-announce/2018/02/msg00000.html>
- <https://lists.debian.org/debian-lts-announce/2018/01/msg00023.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-13982

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Smarty_Security::isTrustedResourceDir() in Smarty before 3.1.33 is prone to a path traversal vulnerability due to insufficient template code sanitization. This allows attackers controlling the executed template code to bypass the trusted directory security restriction and read arbitrary files.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/smarty-php/smarty/commit/f9ca3c63d1250bb56b2bda609dcc9dd81f0065f8>
- <https://github.com/smarty-php/smarty/commit/c9dbe1d08c081912d02bd851d1d1b6388f6133d1>
- <https://github.com/smarty-php/smarty/commit/bcedfd6b58bed4a7366336979ebaa5a240581531>
- <https://github.com/smarty-php/smarty/commit/8d21f38dc35c4cd6b31c2f23fc9b8e5adbc56dfe>
- <https://github.com/smarty-php/smarty/commit/2e081a51b1effddb23f87952959139ac62654d50>
- https://github.com/sbaresearch/advisories/tree/public/2018/SBA-ADV-20180420-01_Smarty_Path_Traversal
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00004.html>
- <https://lists.debian.org/debian-lts-announce/2021/04/msg00014.html>
- <https://lists.debian.org/debian-lts-announce/2021/10/msg00015.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-21408

Title: Improper Input Validation

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-20

References:

- <https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.43>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.3>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2021-29454

Title: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-74

References:

- <https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m>
- <https://packagist.org/packages/smarty/smarty>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.42>
- <https://www.smarty.net/docs/en/language.function.math.tpl>
- <https://github.com/smarty-php/smarty/releases/tag/v4.0.2>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2022-29221

Title: Improper Control of Generation of Code ('Code Injection')

Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.

CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE: CWE-94

References:

- <https://github.com/smarty-php/smarty/releases/tag/v3.1.45>
- <https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c>
- <https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdb5c9874262b702ccddd>
- <https://github.com/smarty-php/smarty/releases/tag/v4.1.1>
- <https://www.debian.org/security/2022/dsa-5151>
- <https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/>

Package: twig/twig

Version: 3.4.1

CVE: CVE-2022-39261

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/..some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b>
- <https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33>
- <https://www.drupal.org/sa-core-2022-016>
- <https://www.debian.org/security/2022/dsa-5248>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/2OKRUHPVLIQVFPPJ2UWC3WV3WQO763NR/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AUVTXMNPSZAHS3DWZEM56V5W4NPVR6L7/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWRFPZSR74SYJKBTKTMYUK36IJ3SQJP/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/YU4ZYX62H2NUAKKGUES4RZIM4KMTKZ7F/>
- <https://lists.debian.org/debian-lts-announce/2022/10/msg00016.html>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TW53TFJ6WWNXMUHOFACKATJTS7NIHVQE/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WV5TNNJLGG536TJH6DLCIAAZZIPV2GUD/>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

CWE

CWE-1104

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

<http://192.168.145.128/openemr/>

List of vulnerable **composer** packages:

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-0085

Title: Server-Side Request Forgery (SSRF)

Description: Server-Side Request Forgery (SSRF) in GitHub repository dompdf/dompdf prior to 2.0.0.

CVSS V2: AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CWE: CWE-918

References:

- <https://github.com/dompdf/dompdf/commit/bb1ef65011a14730b7cfbe73506b4bb8a03704bd>
- <https://huntr.dev/bounties/73dbcc78-5ba9-492f-9133-13bbc9f31236>

Package: dompdf/dompdf

Version: 1.2.2

CVE: CVE-2022-2400

Title: External Control of File Name or Path

Description: External Control of File Name or Path in GitHub repository dompdf/dompdf prior to 2.0.0.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE: CWE-73

References:

- <https://huntr.dev/bounties/a6da5e5e-86be-499a-a3c3-2950f749202a>
- <https://github.com/dompdf/dompdf/commit/99aec1efec9213e87098d42eb09439e7ee0bb6a>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-16831

Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: Smarty before 3.1.33-dev-4 allows attackers to bypass the trusted_dir protection mechanism via a file:../../ substring in an include statement.

CVSS V2: AV:N/AC:M/Au:N/C:C/I:N/A:N

CVSS V3: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE: CWE-22

References:

- <https://github.com/smarty-php/smarty/issues/486>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2018-25047

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty_function_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE: CWE-79

References:

- <https://github.com/smarty-php/smarty/releases/tag/v4.2.1>
- <https://github.com/smarty-php/smarty/releases/tag/v3.1.47>
- <https://bugs.gentoo.org/870100>
- <https://github.com/smarty-php/smarty/issues/454>
- <https://security.gentoo.org/glsa/202209-09>
- <https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html>

Package: smarty/smarty

Version: 2.6.33

CVE: CVE-2023-28447

Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description: Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CWE: CWE-79

References:

- <https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj>
- <https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d>

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

The application must not be subject to error handling vulnerabilities.

STIG-ID: APSC-DV-003235

Severity: CAT II

Application error messages

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).

CWE

CWE-209

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

<http://192.168.145.128/>

Application error messages:

- http://192.168.145.128/openemr/interface/main/main_screen.php
< b > Warning < /b >: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-

mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/main/main_screen.php on line 5137

- http://192.168.145.128/openemr/interface/main/main_screen.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/main_screen.php on line 5137

- http://192.168.145.128/openemr/interface/main/main_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/messages/messages.php on line 5137

- http://192.168.145.128/openemr/interface/main/messages/messages.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/library/ajax/dated_reminders_counter.php on line 5137

- http://192.168.145.128/openemr/library/ajax/dated_reminders_counter.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login/login.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/login/login.php on line 5137
**
- http://192.168.145.128/openemr/interface/login/login.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/interface/login/login.php on line 5137
**
- http://192.168.145.128/openemr/interface/login/login.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
**Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion (include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/cole_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in /var/www/html/openemr/library/ajax/i18n_generator.php on line 5137
**
- http://192.168.145.128/openemr/library/ajax/i18n_generator.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/login_screen.php
**Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/login_screen.php on line 5137
**
- http://192.168.145.128/openemr/interface/login_screen.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

```
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in  
<b>/var/www/html/openemr/interface/login_screen.php</b> on line <b>5137</b><br />
```

- http://192.168.145.128/openemr/interface/login_screen.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php): failed to open stream: No such file or directory in /var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137

- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Warning: include_once(): Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion
(include_path='/var/www/html/openemr/vendor/pear/archive_tar:/var/www/html/openemr/vendor/pear/console_getopt:/var/www/html/openemr/vendor/pear/pear-core-minimal/src:/var/www/html/openemr/vendor/pear/pear_exception:::/usr/share/php') in
/var/www/html/openemr/interface/main/dated_reminders/dated_reminders.php on line 5137
- http://192.168.145.128/openemr/interface/main/dated_reminders/dated_reminders.php
Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSU123MMDJ4XDEmokIFFZN%2CUpmA0oNxhYR1Fnqazp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

Description

While information disclosure vulnerabilities are not directly exploitable by an attacker, they may help an attacker to learn about system specific information. The following is a list of **some** of the information an attacker may be able to obtain from application error disclosure.

- Internal IP addresses
- Secrets (passwords, keys, tokens...)
- Operating system distributions
- Software version numbers
- Missing security patches
- Application stack traces
- SQL statements
- Location of sensitive files (backups, temporary files...)
- Location of sensitive resources (databases, caches, code repositories...)

References

[PHP Runtime Configuration](#)

<https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

[Improper Error Handling](#)

https://www.owasp.org/index.php/Improper_Error_Handling

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None

Integrity Impact	None
Availability Impact	None

User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

http://192.168.145.128/

Request

```
GET /OSEbyESLkq HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

[Custom Error Responses \(Apache HTTP Server\)](#)

<https://httpd.apache.org/docs/current/custom-error.html>

[server_tokens \(Nginx\)](#)

http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

[Remove Unwanted HTTP Response Headers \(Microsoft IIS\)](#)

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

Unnecessary built-in application accounts must be disabled.

Severity: CAT II

No alerts in this category

Default passwords must be changed.

STIG-ID: APSC-DV-003280

Severity: CAT I

No alerts in this category

Protections against DoS attacks must be implemented.

STIG-ID: APSC-DV-003320

Severity: CAT II

No alerts in this category

The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

STIG-ID: APSC-DV-002010

Severity: CAT II

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Impact

Possible information disclosure.

<http://192.168.145.128/>

Verified

Request

```
GET /openemr/public/assets/ HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: d4d608fef00a58addee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/public/assets/
Cookie: OpenEMR=ShqPYxekgSvnztaqfRyqOJ2b-9njDrQM43HnaYAqgkzuKU15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Host: 192.168.145.128
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Coverage

http://192.168.145.128
1
interface
product_registration
product_registration_controller.php
icons
interface
forms
fee_sheet
contraception_products
css
contraception_products.css
js
view_model.js
questionnaire_assessments
lforms
fhir
R4
lformsFHIR.min.js
webcomponent
assets
lib
zone.min.js
main-es2015.js
polyfills-es2015.js
runtime-es2015.js
scripts.js
styles.css
product_registration
product_registration_controller.php
Inputs

POST , email

library

ajax

 user_settings.php

 Inputs

POST , csrf_token_form, setting, target

openemr

bin

config

Documentation

 help_files

 add_edit_transactions_dashboard_help.php

 Inputs

GET site

 adminacl_help.php

 Inputs

GET site

 cms_1500_help.php

 common_help.php

 Inputs

GET site

 configure_orders_help.php

 Inputs

GET site

 cqm_amc_help.php

 Inputs

GET site

 fee_sheet_help.php

 history_dashboard_help.php

 issues_dashboard_help.php

 ledger_dashboard_help.php

 medical_dashboard_help.php

 message_center_help.php

	#fragments
	medex_communication_service
	messages
	recalls
	reminders
	mfa_help.php
	openemr_installation_help.php
	#fragments
	main-list
	section1
	section10
	section11
	section12
	section2
	section3
	section4
	section5
	section6
	section7
	section8
	section9
	openemr_multisite_admin_help.php
	procedure_provider_help.php
	Inputs
	GET site
	report_dashboard_help.php
	sl_eob_help.php
	template_maintenance_help.php
	transactions_dashboard_help.php
	IPPF_Guides
	privileged_db
	de_identification_readme.txt
	Direct_Messaging_README.txt

Emergency_User_README.txt
 INSTALL
 Readme_edihistory.html
 README-Log-Backup.txt
 README.phpgacl
 SystemArchitecture.txt

interface

batchcom
 batchcom.inc.php

billing
 billing_process.php
 billing_report.php
 billing_tracker.php
 clear_log.php
 customize_log.php
 Inputs
 GET site

edi_270.php
 Inputs
 GET site

edi_271.php
 edih_main.php
 Inputs
 GET site

edih_view.php
 Inputs
 GET site

edit_payment.php
 era_payments.php
 Inputs
 GET site

get_claim_file.php
 indigent_patients_report.php

- new_payment.php
- payment_master.inc.php
- print_billing_report.php
- print_daysheet_report_num1.php
- print_daysheet_report_num2.php
- print_daysheet_report_num3.php
- search_payments.php
- sl_eob_invoice.php
- sl_eob_patient_note.php
- sl_eob_process.php
- sl_eob_search.php
- sl_receipts_report.php
- ub04_codes.inc.php
- ub04_dispose.php
- ub04_form.php
- ub04_helpers.php
- ub04_submit.php

clickmap

template

{\$form-%3Etemplate_dir}

css

clickmap.css

css

clickmap.css

{\$form-%3Eimage}

{\$form-%3EsaveAction}

Inputs

POST data, id, pid, process

{php}echo%20\$GLOBALS['webroot']

Inputs

GET

general_new.html

AbstractClickmapModel.php



Inputs

GET site



C_AbstractClickmap.php



couchdb



couchdb_log.php



de_identification_forms



de_identification_procedure.sh



re_identification_procedure.sh



drugs



add_edit_drug.php



add_edit_lot.php



destroy_lot.php



dispense_drug.php



drug_inventory.php



Inputs

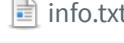
GET site



forms



aftercare_plan



info.txt



new.php



Inputs

GET site



report.php



Inputs

GET site



save.php



Inputs

GET site



table.sql



view.php



Inputs

GET site



ankleinjury

 info.txt	
 new.php	 Inputs  site
 report.php	 Inputs  site
 save.php	
 table.sql	
 view.php	 Inputs  site
 bronchitis	
 info.txt	
 new.php	 Inputs  site
 report.php	 Inputs  site
 save.php	 Inputs  site
 table.sql	
 view.php	 Inputs  site
 CAMOS	
 admin.php	
 ajax_save.php	 Inputs  site
 CAMOS.css	

 help.html
 #fragments
 admin
 advanced
 basic
 intro
 rx
 top
 troubleshooting
 info.txt
 new.php
 Inputs
 site
 notegen.php
 Inputs
 site
 print.php
 Inputs
 site
 README.txt
 report.php
 Inputs
 site
 rx_print.php
 Inputs
 site
 rx.css
 save.php
 Inputs
 site
 table_no_data.sql
 table.sql
 view.php

	 Inputs	
	 site	
	 care_plan	
	 careplan.js	
	 info.txt	
	 new.php	
	 Inputs	
	 site	
	 save.php	
	 Inputs	
	 site	
	 table.sql	
	 view.php	
	 clinic_note	
	 info.txt	
	 new.php	
	 Inputs	
	 site	
	 report.php	
	 Inputs	
	 site	
	 table.sql	
	 view.php	
	 Inputs	
	 site	
	 clinical_instructions	
	 info.txt	
	 new.php	
	 Inputs	
	 site	
	 report.php	
	 Inputs	
	 site	

 save.php	
 Inputs	
	 site
<hr/>	
 table.sql	
 view.php	
 Inputs	
	 site
<hr/>	
 clinical_notes	
 info.txt	
 new.php	
 report.php	
 Inputs	
	 site
<hr/>	
 save.php	
 Inputs	
	 site
<hr/>	
 table.sql	
 view.php	
 Inputs	
	 site
<hr/>	
 dictation	
 info.txt	
 new.php	
 Inputs	
	 site
<hr/>	
 report.php	
<hr/>	
 save.php	
 Inputs	
	 site
<hr/>	
 view.php	
 Inputs	
	 site
<hr/>	
 eye_mag	

 css
 images
 report.css
 style.css
 images
 js
 jquery-1-10-2
 jquery.min.js
 jquery-panelslider
 jquery.panelslider.min.js
 jquery-ui-1-11-4
 jquery-ui.min.js
 shortcut.js-2-01-B
 shortcut.js
 canvasdraw.js
 eye_base.php
 Inputs
 site
 shorthand_eye.js
 login
 login.php
 Inputs
 site
 a_issue.php
 Inputs
 site
 help.php
 Inputs
 site
 info.txt
 new.php
 Inputs
 site

 report.php	
 Inputs	
	 site
<hr/>	
 save.php	
 Inputs	
	 site
<hr/>	
 SpectacleRx.php	
 taskman.php	
 Inputs	
	 site
<hr/>	
 view.php	
 Inputs	
	 site
<hr/>	
 fee_sheet	
 code_choice	
 css	
 code_choices.css	
 js	
 view_model.js	
<hr/>	
 contraception_products	
 ajax	
 find_contraception_products.php	
 Inputs	
	 site
<hr/>	
 css	
 contraception_products.css	
 js	
 view_model.js	
<hr/>	
 login	
 login.php	
 Inputs	
	 site
<hr/>	
 templates	
 contraception_products.php	

	 initialize_contraception_products.php
 login	 login.php
	 Inputs
	 site
 review	
	 js
	 fee_sheet_core.js
 views	
	 procedure_select.php
	 review.css
	 code_check.php
	 fee_sheet_ajax.php
	 Inputs
	 site
	 fee_sheet_justify_view_model.js
	 fee_sheet_justify.php
	 Inputs
	 site
	 fee_sheet_options_ajax.php
	 Inputs
	 site
	 fee_sheet_options_queries.php
	 fee_sheet_review_view_model.js
	 fee_sheet_search_ajax.php
	 Inputs
	 site
	 initialize_review.js
	 codes.php
	 fee_sheet_customization.ods
	 info.txt
	 new.php
	 Inputs

	 site
 report.php	
 Inputs	
	 site
 table.sql	
 view.php	
 Inputs	
	 site
 forms	
 eye_mag	
 images	
 functional_cognitive_status	
 info.txt	
 new.php	
 Inputs	
	 site
 report.php	
 Inputs	
	 site
 save.php	
 Inputs	
	 site
 table.sql	
 view.php	
 Inputs	
	 site
 gad7	
 gad7_javasrc.js	
 gad7.inc.php	
 Inputs	
	 site
 info.txt	
 new.php	

 Inputs	
	 site
 report.php	
 Inputs	
	 site
 save.php	
 Inputs	
	 site
 table.sql	
 view.php	
 Inputs	
	 site
 group_attendance	
 info.txt	
 new.php	
 Inputs	
	 site
 report.php	
 Inputs	
	 site
 save.php	
 table.sql	
 view.php	
 Inputs	
	 site
 LBF	
 new.php	
 printable.php	
 report.php	
 Inputs	
	 site
 view.php	
 Inputs	
	 site

 login
 login.php
 Inputs
 site

 misc_billing_options
 info.txt
 new.php
 Inputs
 site

 report.php
 Inputs
 site

 save.php
 Inputs
 site

 table.sql
 view.php
 Inputs
 site

 newGroupEncounter
 info.txt
 new.php
 Inputs
 site

 report.php
 Inputs
 site

 save.php
 Inputs
 site

 view.php
 Inputs
 site

 newpatient

 info.txt

 new.php

 Inputs

 site

 report.php

 Inputs

 site

 save.php

 Inputs

 site

 view.php

 note

 info.txt

 new.php

 Inputs

 site

 print.php

 report.php

 Inputs

 site

 save.php

 Inputs

 site

 table.sql

 view.php

 Inputs

 site

 observation

 info.txt

 new.php

 Inputs

 site

 observation.js

 report.php
 Inputs
 site

 save.php
 Inputs
 site

 table.sql
 view.php
 Inputs
 site

 painmap
 templates
 README.TXT
 info.txt
 new.php
 Inputs
 site

 report.php
 Inputs
 site

 save.php
 Inputs
 site

 table.sql
 view.php
 Inputs
 site

 physical_exam
 edit_diagnoses.php
 info.txt
 new.php
 Inputs
 site

 report.php	
 Inputs	 site
<hr/>	
 table.sql	
 view.php	
 Inputs	
	 site
<hr/>	
 prior_auth	
 templates	
 prior_auth	
 {\$FORM_ACTION}	
 interface	
 forms	
 prior_auth	
 save.php	
 Inputs	
	 Submit, activity, comments, csrf_token_form, date_from, date_to, id, pid, prior_auth_number, process
<hr/>	
	 csrf_token_form, prior_auth_number, date_from, date_to, comments, id, activity, pid, process
<hr/>	
 general_new.html	
<hr/>	
 info.txt	
 new.php	
 Inputs	
	 site
<hr/>	
 report.php	
 Inputs	
	 site
<hr/>	
 save.php	
 Inputs	
	 site
<hr/>	
 table.sql	
<hr/>	
 view.php	
 Inputs	

GET site

procedure_order

common.php

delete.php

info.txt

new.php

Inputs

GET site

report.php

Inputs

GET site

table.sql

view.php

Inputs

GET site

questionnaire_assessments

lforms

fhir

R4

lformsFHIR.min.js

STU3

lformsFHIR.min.js

lformsFHIRAll.min.js

webcomponent

assets

lib

zone.min.js

lh-forms.es2015.js

lh-forms.es5.js

main-es2015.js

main-es5.js

polyfills-es2015.js

polyfills-es5.js

 runtime-es2015.js
 runtime-es5.js
 scripts.js
 styles.css
 LICENSE.md
 README.md
 info.txt
 lform_webcomponents.php
 new.php
 Inputs
 site
 patient_portal.php
 Inputs
 site
 questionnaire_assessments.php
 Inputs
 site
 save.php
 Inputs
 site
 view.php
 Inputs
 site
 requisition
 barcode.php
 info.txt
 new.php
 Inputs
 site
 table.sql
 view.php
 Inputs
 site

 reviewofs	
 info.txt	
 new.php	
 Inputs	
	 site
 report.php	
 Inputs	
	 site
 save.php	
 Inputs	
	 site
 table.sql	
 view.php	
 Inputs	
	 site
 ros	
 templates	
 ros	
 {\$FORM_ACTION}	
 interface	
 forms	
 ros	
 save.php	
 Inputs	
	 Submit, csrf_token_form, id, pid, process
	 csrf_token_form, id, pid, process
 general_new.html	
 info.txt	
 new.php	
 Inputs	
	 site
 report.php	
 save.php	
 Inputs	

	<code>GET</code>	site
		table.sql
		view.php
		Inputs
	<code>GET</code>	site
		sdoh
		info.txt
		new.php
		Inputs
	<code>GET</code>	site
		patient_portal.php
		report.php
		save.php
		Inputs
	<code>GET</code>	site
		table.sql
		view.php
		Inputs
	<code>GET</code>	site
		soap
		templates
		{\$FORM_ACTION}
		interface
		forms
		soap
		save.php
		Inputs
	<code>POST</code>	Submit, activity, assessment, csrf_token_form, id, objective, pid, plan, process, subjective
	<code>POST</code>	csrf_token_form, subjective, objective, assessment, plan, id, activity, pid, process
		general_new.html
		info.txt
		new.php

 Inputs	
	 site
 report.php	
 Inputs	
	 site
 save.php	
 Inputs	
	 site
 table.sql	
 view.php	
 Inputs	
	 site
 trackAnything	
 create.php	
 history.php	
 Inputs	
	 site
 info.txt	
 new.php	
 Inputs	
	 site
 readme.txt	
 report.js	
 report.php	
 Inputs	
	 site
 style.css	
 table.sql	
 view.php	
 Inputs	
	 site
 transferSummary	
 info.txt	

 new.php		
 Inputs		
	 GET	site
<hr/>		
 report.php		
 Inputs		
	 GET	site
<hr/>		
 save.php		
 Inputs		
	 GET	site
<hr/>		
 table.sql		
<hr/>		
 view.php		
 Inputs		
	 GET	site
<hr/>		
 treatment_plan		
 info.txt		
<hr/>		
 new.php		
 Inputs		
	 GET	site
<hr/>		
 report.php		
 Inputs		
	 GET	site
<hr/>		
 save.php		
 Inputs		
	 GET	site
<hr/>		
 table.sql		
<hr/>		
 view.php		
 Inputs		
	 GET	site
<hr/>		
 vitals		
 growthchart		
 chart.php		
 Inputs		
	 GET	site
<hr/>		
 page1.css		

	page2.css
login	
	login.php
	Inputs
	site
templates	
	summary
	demographics.php
vitals	
	{%20FORM_ACTION attr%20}
	interface
	forms
	vitals
	save.php
	Inputs
	POST Submit, activity, csrf_token_form, date, id, pid, process, uuid
	POST csrf_token_form, date, id, uuid, activity, pid, process
	vitals.css
	vitals.js
	vitals_actions.html.twig
	vitals_bmi_status.html.twig
	vitals_bmi.html.twig
	vitals_growthchart_actions.html.twig
	vitals_historical_values_complete.html.twig
	#fragments
	# vitals-screen-top
	vitals_historical_values.html.twig
	vitals_interpretation_selector.html.twig
	vitals_notes.html.twig
	vitals_reason_row.html.twig
	vitals_temp_method.html.twig
	vitals_textbox_conversion.html.twig
	vitals_textbox.html.twig

	vitals.html.twig
	#fragments
	# patient-vitals-history
	info.txt
	new.php
	Inputs
	GET site
	report.php
	Inputs
	GET site
	save.php
	Inputs
	GET site
	table.sql
	view.php
	Inputs
	GET site
	vitals.css
	vitals.js
img	
language	
csv	
	load_csv_file.php
	translation_utilities.php
	validate_csv.php
	lang_constant.php
	lang_definition.php
	lang_language.php
	lang_manage.php
	lang.info.html
	language.inc.php
login	
	login.php



Inputs

GET site

logview

erx_logview.php

logview.php

main

calendar

includes

pnAPI.php

pnHTML.php

pnMod.php

modules

PostCalendar

plugins

function.pc_date_select.php

function.pc_filter.php

function.pc_form_nav_close.php

function.pc_form_nav_open.php

function.pc_popup.php

function.pc_sort_events.php

function.pc_url.php

function.pc_view_select.php

pnincludes

Date

Calc.php

AnchorPosition.js

ColorPicker2.js

index.htm

overlib_mini.js

PopupWindow.js

pnlang

eng

index.htm

 index.htm

 pntemplates

 default

 admin

 modules

 [-\$pcDir-]

 pnincludes

 AnchorPosition.js

 ColorPicker2.js

 PopupWindow.js

 [-\$action-]

 Inputs

 [-\$InputACO|attr-]], [-\$InputAllDay|attr-][-literal-][[-/literal-]
[-\$cat.id|attr-][-literal-]][-/literal-], [-\$InputCatType|attr-]],
[-\$InputDurationHour|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]][-/literal-],
[-\$InputDurationMin|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]][-/literal-],
active[-literal-][[-/literal-][\$cat.id|attr-][-literal-]][-/literal-], color[], constantid[],
del[], desc[], id[], name[], new[-\$InputACO|attr-], new[-\$InputAllDay|attr-],
new[-\$InputCatType|attr-], new[-\$InputDurationHour|attr-],
new[-\$InputDurationMin|attr-], new[-\$InputEndDateFreqType|attr-],
new[-\$InputEndDateFreq|attr-], new[-\$InputEndOn|attr-],
new[-\$InputNoRepeat|attr-], new[-\$InputRepeatFreqType|attr-],
new[-\$InputRepeatFreq|attr-], new[-\$InputRepeatOnDay|attr-],
new[-\$InputRepeatOnFreq|attr-], new[-\$InputRepeatOnNum|attr-],
new[-\$InputRepeatOn|attr-], new[-\$InputRepeat|attr-], newactive, newcolor,
newconstantid, newdesc, newid, newname, newsequence, sequence[],
[-\$InputEndDateFreqType|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputEndDateFreq|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputEndOn|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputNoRepeat|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatFreqType|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatFreq|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatOnDay|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatOnFreq|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatOnNum|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeatOn|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], [-\$InputRepeat|attr-][-literal-][[-/literal-][\$cat.id|attr-][-literal-]]
[-/literal-], pc_html_or_text

 index.html

 submit_category.html

 config
 default.conf
 index.html
 lang.eng
 navigation.conf
 images
 index.html
 style
 day.css
 index.html
 week.css
 user
 [-php-]echo%20\$GLOBALS['assets_static_relative']%-20[-
 php-]
 jquery-datetimepicker
 build
 jquery.datetimepicker.full.min.js
 jquery.datetimepicker.min.css
 ".\$GLOBALS[
 [-\$FORM_ACTION-]
 Inputs
 pc_keywords, pc_keywords_andor, pc_category, pc_topic, start, end
 end, pc_category, pc_facility, pc_keywords, pc_keywords_andor,
pc_topic, provider_id, start, submit
 ajax_search.html
 index.html
 views
 [-php-]echo%20\$GLOBALS['webroot']%-20[-
 php-]
 library
 js
 calendarDirectSelect.js
 day_print
 outlook_ajax_template.html

day

\$NEXT_DAY_URL

\$PREV_DAY_URL

ajax_template.html

default.html

index.html

index.php

Inputs

func, module, pc_category, pc_topic, tplview

jumpdate, pc_facility, pc_username[], viewtype

month_print

outlook_ajax_template.html

month

".\$gotoURL."

\$NEXT_MONTH_URL

\$PREV_MONTH_URL

ajax_template.html

default.html

index.html

index.php

Inputs

func, module, pc_category, pc_topic, tplview

jumpdate, pc_facility, pc_username[], viewtype

week_print

outlook_ajax_template.html

week

\$gotoURL

\$NEXT_WEEK_URL

\$PREV_WEEK_URL

ajax_template.html

default.html

index.html

index.php

Inputs

POST func, module, pc_category, pc_topic, tplview

POST jumpdate, pc_facility, pc_username[], viewtype

\$cssSrc

\$script

footer.html

header.html

index.html

index.html

COPYING

pntables.php

pnversion.php

README

undefined

public

assets

interactjs

dist

interact.js

add_edit_event.php

Inputs

GET catid, date, startampm, starttimeh, starttimem, userid

index.php

Inputs

POST func, module, pc_category, pc_topic, tplview

POST jumpdate, pc_username[], viewtype

GET Date, func, module, pc_category, pc_topic, pc_username, print, tplview, viewtype

pntables.php

dated_reminders

dated_reminders_add.php

Inputs

GET mID

	dated_reminders_log.php	
	Inputs	
		site
	dated_reminders.php	
	Inputs	
		csrf_token_form, drR, skip_timeout_reset,
	finder	
	dynamic_finder.php	
	Inputs	
		search_any
	holidays	
	Holidays_Controller.php	
	Holidays_Storage.php	
	login	
	login.php	
	Inputs	
		site
	messages	
	css	
	reminder_style.css	
	js	
	reminder_appts.js	
	trusted-messages.js	
	undefined	
	public	
	assets	
	interactjs	
	dist	
	interact.js	
	messages.php	
	Inputs	
		form_active, , show_all, form_inactive, sortby, sortorder, begin, showall, task, go
		, begin, showall, sortby, sortorder, form_active

POST task

 print_postcards.php

 Inputs

GET site

 save.php

 Inputs

POST, action, pid

GET site

 trusted-messages-ajax.php

 Inputs

GET site

 trusted-messages.php

 Inputs

GET site

 onotes

 office_comments_full.php

 Inputs

GET site

 office_comments.php

 Inputs

GET site

 tabs

 js

 application_view_model.js

 custom_bindings.js

 dialog_utils.js

 frame_proxies.js

 include_opener.js

 menu_analysis.js

 patient_data_view_model.js

 shortcuts.js

 tabs_view_model.js

 therapy_group_data_view_model.js

	user_data_view_model.js
menu	
menus	
patient_menus	
standard.json	
	answering_service.json
	front_office.json
	standard.json
templates	
menu_template.php	
webroot_url	
library	
ajax	
unset_session_ajax.php	
Inputs	
, csrf_token_form, func	
main.php	
Inputs	
token_main, anySearchBox	
backuplog.php	
backuplog.sh	
main_info.php	
main_screen.php	
Inputs	
auth, site	
authUser, clearPass, languageChoice, new_login_session_management	
new_login_session_management, languageChoice, authUser, clearPass	
modules	
custom_modules	
oe-module-comlink-telehealth	
public	
assets	
css	
telehealth.css	

js
cvb.min.js
telehealth-appointment.js
telehealth-calendar.js
telehealth-patient.js
telehealth-provider.js
telehealth.js
sql
table.sql
src
Controller
Admin
TeleHealthPatientAdminController.php
TeleHealthUserAdminController.php
TeleconferenceRoomController.php
TeleHealthCalendarController.php
TeleHealthFrontendSettingsController.php
TeleHealthPatientPortalController.php
TeleHealthVideoRegistrationController.php
Exception
TelehealthProviderNotEnrolledException.php
TeleHealthProviderSuspendedException.php
Models
TeleHealthPersonSettings.php
TeleHealthUser.php
UserVideoRegistrationRequest.php
Repository
CalendarEventCategoryRepository.php
TeleHealthPersonSettingsRepository.php
TeleHealthProviderRepository.php
TeleHealthSessionRepository.php
Services
TelehealthRegistrationCodeService.php

TeleHealthRemoteRegistrationService.php

Util

CalendarUtils.php

Bootstrap.php

TelehealthGlobalConfig.php

templates

comlink

 {{%20assetPath%20}}..

 {{}}

 {{%20assetPath%20}}css

 {{}}

 {{%20assetPath%20}}js

 {{}}

admin

 user_admin-extension.html.twig

appointment

 add_edit_event.js.twig

 conference-room.twig

 patient-portal.twig

 telehealth-frontend-settings.js.twig

 video-control-bar.twig

 waiting-room-patient.twig

 waiting-room-provider.twig

 waiting-room.twig

 #fragments

 waitingRoomProfile

emails

partials

patient

 {{%20fhir_address|attr%20}}

 {{%20fhir_requirements_address|attr%20}}

 email-message-fhir-access.html.twig

 email-message-fhir-access.text.twig

	patient
	partials
	registration-code.html.twig
	portal
	appointment-item.html.twig
	tests
	bootstrap.php
	CHANGELOG.md
	cleanup.sql
	info.txt
	phpunit.xml
	Readme.md
	README
	zend_modules
	config
	autoload
	global.php
	module
	Acl
	config
	module.config.php
	autoload_classmap.php
	Module.php
	Application
	config
	module.config.php
	view
	application
	index
	index.phtml
	Module.php
	Carecoordination
	config

	module.config.php
src	
Carecoordination	
Model	
CcdaDocumentTemplateOids.php	
CcdaGenerator.php	
CcdaGlobalsConfiguration.php	
CcdaServiceConnectionException.php	
CcdaServiceDocumentRequestor.php	
CcdaServiceRequestModelGenerator.php	
CcdaUserPreferencesTransformer.php	
GeneratedCcdaResult.php	
view	
carecoordination	
carecoordination	
index.phtml	
encountermanager	
download.phtml	
autoload_classmap.php	
autoload_function.php	
autoload_register.php	
LICENSE.txt	
Module.php	
Ccr	
config	
module.config.php	
autoload_classmap.php	
Module.php	
CodeTypes	
config	
module.config.php	
Module.php	
Documents	

	config
	module.config.php
	autoload_classmap.php
	info.txt
	FHIR
	config
	module.config.php
	Module.php
	Immunization
	config
	module.config.php
	autoload_classmap.php
	Module.php
	Installer
	config
	module.config.php
	src
	Installer
	Model
	InstModuleTable.php
	autoload_classmap.php
	info.txt
	Module.php
	Multipledb
	config
	module.config.php
	src
	Multipledb
	Controller
	ModuleconfigController.php
	Model
	MultipledbTable.php
	autoload_classmap.php

	Module.php
	Readme.md
	PatientFlowBoard
	config
	module.config.php
	Module.php
	Patientvalidation
	config
	module.config.php
	src
	Patientvalidation
	Model
	PatientDataTable.php
	autoload_classmap.php
	Module.php
	Readme.md
	PrescriptionTemplates
	config
	module.config.php
	view
	prescription-templates
	default.phtml
	autoload_classmap.php
	Module.php
	Syndromicsurveillance
	config
	module.config.php
	autoload_classmap.php
	Module.php
	public
	css
	autosuggest
	autosuggest.css

 icons
 images
 jquery.treeview-1.4.1
 images
 rtl-treeview
 jquery.treeview.rtl.css
 jquery.treeview.css
 multipledb
 multipledb.css
 slider
 CSS
 slide.css
 images
 acl.css
 bootstrap-responsive.min.css
 bootstrap.min.css
 bubbles.css
 bubbletip-IE.css
 bubbletip.css
 carecoordination_style.css
 ccda.css
 CDA.xsl
 demo.css
 drag_and_drop_uploader.css
 easyui.css
 emr.css
 encounter.css
 icon.css
 immunization.css
 jquery-ui.css
 jquery.contextMenu.css
 jquery.custom-scrollbar.css
 jquery.treeview.css

 mockjax.css
 responsive-tables.css
 sendTo.css
 style.css
 suggestion.css
 images
 img
 js
 acl
 acl.js
 application
 common.js
 sendTo.js
 autosuggest
 autosuggest.js
 carecoordination
 demo.js
 encounterManager.js
 responsive-tables.js
 installer
 action.js
 lib
 jquery.treeview-1.4.1
 lib
 jquery.cookie.js
 jquery.js
 jquery.treeview.async.js
 jquery.treeview.edit.js
 jquery.treeview.js
 jquery.treeview.sortable.js
 README.md
 bootstrap.min.js
 jquery-1.10.2.min.js

	jquery-1.4.3.js
	jquery-1.8.0.min.js
	jquery-1.8.2.min.js
	jquery-1.8.3.js
	jquery-ui.custom.js
	jquery-ui.js
	jquery.custom-scrollbar.js
	jquery.easyui.min.js
	jquery.easyui.override.js
	jquery.ui.core.js
	jquery.ui.datepicker.js
	jquery.ui.mouse.js
	jquery.ui.sortable.js
	jquery.ui.tabs.js
	jquery.ui.widget.js
	modernizr-2.6.2.min.js
	virtualpaginate.js
scripts	
	cancercare.js
	file_uploader.js
	fixdate.js
	immunization.js
	syndromicsurveillance.js
xsd	
	Schema
	CDA2
	infrastructure
	cda
	CDA_SDTC.xsd
	POCD_MT000040_SDTC.xsd
	SDTC.xsd
	processable
	coreschemas

	 datatypes-base_SDTC.xsd
	 datatypes.xsd
	 infrastructureRoot.xsd
	 NarrativeBlock.xsd
	 voc.xsd
	 xsl
	 ccd.xsl
	 ccr.xsl
	 cda.xsl
	 qrda.xsl
	 .htaccess
	 orders
	 configure_orders_worksheet.ods
	 qoe.inc.php
	 patient_file
	 report
	 custom_report.js
	 summary
	 add_edit_issue_medication_fragment.php
	 addr_appt_label.php
	 addr_label.php
	 barcode_label.php
	 deleter.php
	 download_template.php
	 education.php
	 Inputs
	 site
	 front_payment_cc.php
	 Inputs
	 site
	 front_payment_terminal.php
	 Inputs
	 site

 front_payment.php

 Inputs

 GET site

 label.php

 manage_dup_patients.php

 merge_patients.php

 pos_checkout_normal.php

 pos_checkout.php

 printed_fee_sheet.php

 problem_encounter.php

 void_dialog.php

 patient_tracker

 patient_tracker_status.php

 patient_tracker.php

 Inputs

 GET skip_timeout_reset

 pic

 practice

 address_verify.php

 ins_list.php

 ins_search.php

 product_registration

 exceptions

 generic_product_registration_exception.php

 product_registration_controller.js

 product_registration_controller.php

 product_registration_service.js

 reports

 report.script.php

 smart

 admin-client.php

 register-app.php

 super

 login
 login.php
 Inputs
GET site
<hr/>
 rules
 base
 library
 ActionRouter.php
 BaseController.php
 ControllerRouter.php
 template
 redirect.php
 undecorated.php
<hr/>
 controllers
 edit
 helper
 common.php
<hr/>
 include
 common.php
<hr/>
 library
 CdrHelper.class.php
 Code.php
 CodeManager.php
 Option.php
 ReminderIntervalDetail.php
 ReminderIntervalRange.php
 ReminderIntervals.php
 ReminderIntervalType.php
 Rule.php
 RuleAction.php
 RuleActions.php
 RuleCriteria.php
 RuleCriteriaBuilder.php

	RuleCriteriaDbView.php
	RuleCriteriaFactory.php
	RuleCriteriaType.php
	RuleFilters.php
	RulesPlanMappingEventHandlers_ajax.php
	 Inputs
	 site
	RulesPlanMappingEventHandlers.php
	RuleTargetActionGroup.php
	RuleTargets.php
	RuleType.php
	TimeUnit.php
 login	
	login.php
	 Inputs
	 site
 www	
	 css
	 cdr-multiselect
	 common.css
	 plans_config.css
	 ui.multiselect.css
 js	
	 cdr-multiselect
	 locale
	 ui-multiselect-cdr.js
	 plugins
	 localisation
	 jquery.localisation-min.js
	 jquery.localisation-pack.js
	 jquery.localisation.js
	 scrollTo
	 jquery.scrollTo-min.js
	 jquery.scrollTo.js

 jquery-ui.min.js
 jquery.min.js
 jquery.switchButton.js
 ui.multiselect.js
 bucket.js
 custom.js
 detail.js
 edit.js
 jQuery.autocomplete.js
 jQuery.fn.sortElements.js
 list.js
 typeahead.js
 index.php
 Inputs
 GET site
 edit_globals.js
 edit_globals.php
 Inputs
 GET site
 edit_layout_props.php
 edit_layout.php
 Inputs
 GET site
 edit_list.php
 Inputs
 GET site
 layout_listitems_ajax.php
 layout_service_codes.php
 load_codes.php
 manage_document_templates.php
 manage_site_files.php
 themes

 colors

 utilities

 batch-payments

 batch-payments.scss

 bootstrap

 bootstrap-nav-menu

 bootstrap-nav-menu.scss

 bootstrap.scss

 codes

 codes.scss

 default_variables.scss

 edit_globals_colors

 edit_globals_colors.scss

 external-data

 external-data.scss

 fee-sheet

 fee-sheet.scss

 help-files

 help-files.scss

 login

 login.scss

 recall-flow-board

 recall-flow-board.scss

 ros

 ros.scss

 tabs-full

 tabs-full.scss

 style_ash_blue.scss

 style_burgundy.scss

 style_cadmium_yellow.scss

 style_chocolate.scss

 style_cobalt_blue.scss

 style_coral.scss

 style_deep_purple.scss
 style_dune.scss
 style_emerald.scss
 style_forest_green.scss
 style_mauve.scss
 style.mustard_green.scss
 style_olive.scss
 style_pink.scss
 style_powder_blue.scss
 style_red.scss
 style_sienna.scss
 style_tangerine.scss
 core
 patient
 demographics.scss
 history.scss
 notes.scss
 past_encounters.scss
 report_custom.scss
 reports.scss
 stats_summary.scss
 stats.scss
 addressbook.scss
 closeDlglframe.scss
 cursor.scss
 documents.scss
 edit_globals.scss
 FontAwesome.scss
 forms.scss
 links.scss
 list-table.scss
 navmenu.scss
 oe-mobile.scss

-  reports.scss
-  sddm.scss
-  tabs.scss
-  text.scss
-  therapy-groups.scss

misc

-  bootstrap-navbar.scss
-  edi_history_v2.scss
-  encounters.scss
-  labdata.scss
-  rules.scss

navigation-slide

-  _color.scss
-  _future-bootstrap.scss
-  _manilla.scss
-  color
-  future-bootstrap
-  manilla

oe-common

-  acl-common.scss
-  help-files-common.scss
-  main-common.scss
-  messages-common.scss
-  oe-sidebar
-  oe-sidebar.scss
-  procedures-common.scss

oe-styles

-  style_dark.scss
-  style_light.scss
-  style_manila.scss
-  style_solar.scss

-  ajax_calendar_ie.css
-  ajax_calendar_sass.scss

-  color_base.scss
-  compact-theme-defaults.scss
-  core
-  core.css
-  core.scss
-  default-variables
-  default-variables.scss
-  directional
-  directional.scss
-  jquery.autocomplete.css
-  login_page.scss
-  oe-bootstrap
-  oe-bootstrap.scss
-  oemr_compact_imports.scss
-  oemr rtl_compact_imports.scss
-  oemr-rtl.scss
-  patientportal-base.scss
-  patientportal-register.scss
-  patientportal-style.scss
-  rtl_style_pdf.css
-  rtl.scss
-  style_pdf.scss
-  style.scss
-  tabs_style_compact.scss
-  tabs_style_full.scss
-  theme-defaults
-  theme-defaults.scss

-  therapy_groups
 -  therapy_groups_controllers
 -  base_controller.php
 -  therapy_groups_models
 -  group_statuses_model.php
 -  therapy_groups_counselors_model.php

	 therapy_groups_encounters_model.php
	 therapy_groups_events_model.php
	 therapy_groups_model.php
	 therapy_groups_participants_model.php
	 users_model.php
	therapy_groups_views
	 footer.php
	 index.php
	usergroup
	 checkpwd_validation.js
	weno
	 facilities.php
	 indexrx.php
	 rxlogmanager.php
	 weno.js
	 wenoconnected.php
	 eRx.php
	 eRxGlobals.php
	 eRxPage.php
	 eRxSOAP.php
	 eRxStore.php
	 globals.php
	 help_modal.php
	 login_screen.php
	 Inputs
	 error, site
	 logout.php
	 README.md
	library
	 admin
	 ajax
	 drug_autocomplete
	 search.php

imm_autocomplete

search.php

messages

validate_messages_document_ajax.php

Inputs

GET site

addlistitem.php

adminacl_ajax.php

amc_misc_data.php

billing_tracker_ajax.php

code_attributes_ajax.php

collect_new_report_id.php

dated_reminders_counter.php

Inputs

POST skip_timeout_reset, isPortal, csrf_token_form

document_helpers.php

drug_screen_completed.php

easipro_util.php

Inputs

GET site

execute_background_services.php

Inputs

POST skip_timeout_reset, ajax, csrf_token_form

GET site

execute_cdr_report.php

execute_patReminder.php

Inputs

GET site

facility_ajax_code.php

graph_track_anything.php

Inputs

GET site

graphs.php

 i18n_generator.php

 Inputs

 GET csrf_token_form, lang_id

 lists_touch.php

 Inputs

 GET site

 log_print_action_ajax.php

 Inputs

 POST , comments, csrf_token_form

 GET site

 payment_ajax.php

 plan_setting.php

 Inputs

 GET site

 prescription_drugname_lookup.php

 rule_setting.php

 set_pt.php

 Inputs

 GET site

 specialty_form_ajax.php

 sql_server_status.php

 Inputs

 GET site

 status_report.php

 Inputs

 GET site

 template_context_search.php

 Inputs

 GET site

 turnoff_birthday_alert.php

 udi.php

 unset_session_ajax.php

 upload.php



classes

custom_template

edihistory

Esign

fonts

js

vendors

validate



login



Inputs

GET site

MedEx

smarty

templates

validation



%3C

Inputs

GET

\$1

ADODB_mysqli_log.php

allow_cronjobs.php

amc.php

api.inc

appointment_status.inc.php

appointments.inc.php

auth.inc

 billing_sftp_service.php

 calendar.inc

 checkout_receipt_array.inc.php

 clinical_rules.php

 contraception_billing_scan.inc.php

 create_ssl_certificate.php

 csv_like_join.php

 date_functions.php

 dated_reminder_functions.php

 daysheet.inc.php

 deletedrug.php

 dialog.js

 dicom_frame.php



GET site

 direct_message_check.inc

 display_help_icon_inc.php

 documents.php

 dupscore.inc.php

 encounter_events.inc.php

 encounter.inc

 erx_javascript.inc.php

 expand_contract_inc.php

 FeeSheet.class.php



GET site

 FeeSheetHtml.class.php



GET site

 formatting_DateToYYYYMMDD_js.js.php

 formatting.inc.php

 formdata.inc.php

 forms.inc

-  globals.inc.php
-  grelations.inc.php
-  group.inc
-  htmlspecialchars.inc.php
-  immunization_helper.php
-  ippf_issues.inc.php
-  lab.inc
-  layout.inc.php
-  lists.inc
-  maviq_phone_api.php
-  options_listadd.inc
-  options.inc.php
-  options.js.php
-  patient_tracker.inc.php
-  patient.inc
-  patientvalidation.inc.php
-  payment_jav.inc.php
-  payment.inc.php
-  pid.inc
-  pnotes.inc
-  registry.inc
-  reminders.php
-  report_database.inc
-  report.inc
-  restoreSession.php
-  sanitize.inc.php
-  specialty_forms.php
-  spreadsheet.inc.php
-  sql_upgrade_fx.php
-  sql-ccr.inc
-  sql.inc
-  sqlconf.php
-  standard_tables_capture.inc

textformat.js
 tooltip.js
 topdialog.js
 transactions.inc
 translation.inc.php
 user.inc
 uuid.php
 weno_log_sync.php
 xmltoarray_parser_htmlfix.php

login
 login.php
 Inputs
GET site

modules

portal
 images
 login
 login.php
 Inputs
GET site

messaging

messages.php
 Inputs
GET site

secure_chat.php
 Inputs
GET site

public

assets
 @eastdesire
 @fortawesome
 fontawesome-free
 css
 all.min.css

	scss
	brands
	fontawesome
	regular
	solid
	webfonts
	@ttskch
	angular-sanitize
	angular
	backbone
	bootstrap-rtl
	bootstrap
	dist
	css
	bootstrap.min.css
	js
	bootstrap.bundle.js
	bootstrap.bundle.min.js
	bootstrap.js
	bootstrap.min.js
	scss
	vendor
	rfs
	bootswatch
	chart.js
	checklist-model
	docs
	img
	app.js
	main.css
	checklist-model.js
	ckeditor4
	datatables.net-bs4

 datatables.net-colreorder-dt
 datatables.net-colreorder
 datatables.net-dt
 datatables.net-jqui
 datatables.net-scroller-jqui
 datatables.net-scroller
 datatables.net
 dropzone
 dvw
 flot
 hotkeys-js
 dist
 hotkeys.min.js
 i18next-browser-languagedetector
 i18next-xhr-backend
 i18next
 dist
 umd
 i18next.min.js
 interactjs
 jquery-creditcardvalidator
 jquery-datetimepicker
 build
 jquery.datetimepicker.full.min.js
 jquery.datetimepicker.min.css
 node_modules
 jquery-mousewheel
 jquery.mousewheel.js
 php-date-formatter
 js
 php-date-formatter.min.js
 bower.json
 jquery.datetimepicker.css

 jquery.datetimepicker.js
 jquery.js
 package.json
 README.md
<hr/>
 jquery-panelslider
 jquery-ui-themes
 jquery-ui
 #fragments
 tabs-1
 tabs-2
 tabs-3
<hr/>
 Inputs
 GET radio
<hr/>
 "images
 ui-icons_444444_256x240.png"
 ui-icons_555555_256x240.png"
 ui-icons_777620_256x240.png"
 ui-icons_777777_256x240.png"
 ui-icons_cc0000_256x240.png"
 ui-icons_ffffff_256x240.png"
<hr/>
 external
 jquery
 jquery.js
<hr/>
 images
 jquery-ui.css
 jquery-ui.js
<hr/>
 jquery-validation
 jquery
 dist
 jquery.js
 jquery.min.js
 jquery.slim.js
 jquery.slim.min.js

 jspdf
 jszip
 knockout
 build
 output
 knockout-latest.debug.js
 knockout-latest.js
 konva
 literallycanvas
 magic-wand-js
 modified
 moment
 min
 moment.min.js
 moment.js
 numeral
 purecss
 react
 select2
 dist
 css
 select2.min.css
 js
 select2.full.min.js
 sortablejs
 underscore
 validate.js
 ckeditor4
 images
 themes
 style_light.css
 tabs_style_full.css
 sql

 src

 templates

 tests

 vendor
