Acunetix by Invicti

Compliance Report

2023 CWE Top 25 Most Dangerous Software Weaknesses

Description

The 2023 CWE Top 25 Most Dangerous Software Weaknesses is a list of the most widespread and critical weaknesses that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry, by identifying and avoiding all-too-common mistakes that occur before software is even shipped. Software customers can use the same list to help them to ask for more secure software. Researchers in software security can use the Top 25 to focus on a narrow but important subset of all known security weaknesses. Finally, software managers and CIOs can use the Top 25 list as a measuring stick of progress in their efforts to secure their software.

To create the list, the CWE Team leverages Common Vulnerabilities and Exposures (CVE) data found within the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) scores associated with each CVE Record, including a focus on CVE Records from the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog. A formula is applied to the data to score each weakness based on prevalence and severity. The dataset used to calculate the 2023 Top 25 contains a total of 37,899 CVE records from the previous two calendar years.

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.

This document was generated using information provided in "2023 CWE Top 25 Most Dangerous Software Weaknesses", that can be found at https://cwe.mitre.org/top25/.

Compliance at a Glance

CATEGORY

0 1 Out-of-bounds Write

0 2 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

0 3 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

0 4 Use After Free

0 5 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

0 6 Improper Input Validation

0 7 Out-of-bounds Read

0 8 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

0 9 Cross-Site Request Forgery (CSRF)

0 10 Unrestricted Upload of File with Dangerous Type

0 11 Missing Authorization

0 12 NULL Pointer Dereference

0 13 Improper Authentication

0 14 Integer Overflow or Wraparound

0 15 Deserialization of Untrusted Data

0 16 Improper Neutralization of Special Elements used in a Command ('Command Injection')

0 17 Improper Restriction of Operations within the Bounds of a Memory Buffer

0 18 Use of Hard-coded Credentials

0 19 Server-Side Request Forgery (SSRF)

0 20 Missing Authentication for Critical Function

CATEGORY

0 21 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

0 22 Improper Privilege Management

0 23 Improper Control of Generation of Code ('Code Injection')

18 24 Incorrect Authorization

Detailed Compliance Report by Category

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

1 Out-of-bounds Write

The software writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or code execution. The software may modify an index or perform pointer arithmetic that references a memory location that is outside the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results. The generic term "memory corruption" is often used to describe the consequences of writing to memory outside the bounds of a buffer, or to memory that is invalid, when the root cause is something other than a sequential copy of excessive data from a fixed starting location. This may include issues such as incorrect pointer arithmetic, accessing invalid pointers due to incomplete initialization or memory release.

No alerts in this category

2 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

"XSS" is a common abbreviation for Cross-Site Scripting.

No alerts in this category

3 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands. SQL injection has become a common issue with database-driven websites. The flaw is easily detected, and easily exploited, and as such, any site or software

package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

No alerts in this category

4 Use After Free

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code. The use of previously-freed memory can have any number of adverse consequences, ranging from the corruption of valid data to the execution of arbitrary code, depending on the instantiation and timing of the flaw. The simplest way data corruption may occur involves the system's reuse of the freed memory. Use-after-free errors have two common and sometimes overlapping causes, namely: i) error conditions and other exceptional circumstances, and ii) confusion over which part of the program is responsible for freeing the memory.

No alerts in this category

5 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This could allow attackers to execute unexpected, dangerous commands directly on the operating system. This weakness can lead to a vulnerability in environments in which the attacker does not have direct access to the operating system, such as in web applications. Alternately, if the weakness occurs in a privileged program, it could allow the attacker to specify commands that normally would not be accessible, or to call alternate commands with privileges that the attacker does not have. The problem is exacerbated if the compromised process does not follow the principle of least privileges, because the attacker-controlled commands may run with special system privileges that increases the amount of damage.

No alerts in this category

6 Improper Input Validation

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. Input validation is a frequently-used

technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

No alerts in this category

7 Out-of-bounds Read

The software reads data past the end, or before the beginning, of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. A crash can occur when the code reads a variable amount of data and assumes that a sentinel exists to stop the read operation, such as a NUL in a string. The expected sentinel might not be located in the out-of-bounds memory, causing excessive data to be read, leading to a segmentation fault or a buffer overflow. The software may modify an index or perform pointer arithmetic that references a memory location that is outside the boundaries of the buffer. A subsequent read operation then produces undefined or unexpected results.

No alerts in this category

8 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Many file operations are intended to take place within a restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system.

No alerts in this category

9 Cross-Site Request Forgery (CSRF)

The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. When a web server is designed

to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and can result in exposure of data or unintended code execution.

No alerts in this category

10 Unrestricted Upload of File with Dangerous Type

The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.

No alerts in this category

11 Missing Authorization

Alternate Terms: AuthZ

No alerts in this category

12 NULL Pointer Dereference

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. NULL pointer dereference issues can occur through a number of flaws, including race conditions, and simple programming omissions.

No alerts in this category

13 Improper Authentication

Alternate Terms: authentification, AuthN, AuthC

No alerts in this category

14 Integer Overflow or Wraparound

The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control. An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior in circumstances that rely on wrapping, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs. This becomes security-critical when the result is used to control looping, make a security decision, or determine the offset or size in behaviors such as memory allocation, copying or concatenation.

No alerts in this category

15 Deserialization of Untrusted Data

Alternate Terms: Marshalling/unmarshaling, Pickling/unpickling, PHP Object Injection

No alerts in this category

16 Improper Neutralization of Special Elements used in a Command ('Command Injection')

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. Many protocols and products have their own custom command language. While OS or shell command strings are frequently discovered and targeted, developers may not realize that these other command languages might also be vulnerable to attacks. Command injection is a common problem with wrapper programs.

No alerts in this category

17 Improper Restriction of Operations within the Bounds of a Memory Buffer

Alternate Terms: Buffer overlow, buffer overrun, memory safety

No alerts in this category

18 Use of Hard-coded Credentials

The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This hole might be difficult for the system administrator to detect. Even if detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely.

No alerts in this category

19 Server-Side Request Forgery (SSRF)

Alternate Terms: XPSA (Cross Site Port Attack)

No alerts in this category

20 Missing Authentication for Critical Function

The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

No alerts in this category

21 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

The program contains a code sequence that can run concurrently with other code, and the code sequence requires temporary, exclusive access to a shared resource, but a timing window exists in which the shared resource can be modified by another code sequence that is operating concurrently. This can have security implications when the expected synchronization is in security-critical code, such as recording whether a

user is authenticated or modifying important state information that should not be influenced by an outsider. A race condition occurs within concurrent environments, and is effectively a property of a code sequence.

No alerts in this category

22 Improper Privilege Management

The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.

No alerts in this category

23 Improper Control of Generation of Code ('Code Injection')

The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. When software allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended control flow of the software. Such an alteration could lead to arbitrary code execution.

No alerts in this category

24 Incorrect Authorization

The product performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.

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://10.10.236.31/

Application error messages:

- http://10.10.236.31/openemr/interface/main/main_screen.php
  Unknown column 'Array' in 'where clause'

- http://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/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://10.10.236.31/openemr/interface/main/calendar/index.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/calendar/index.php on line 5137
**

- http://10.10.236.31/openemr/interface/main/calendar/index.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/calendar/index.php on line 5137
**

- http://10.10.236.31/openemr/interface/main/calendar/index.php
  Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

- http://10.10.236.31/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://10.10.236.31/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://10.10.236.31/openemr/interface/login/login.php
  Failed opening '/var/www/html/openemr/vendor/adodb/adodb-php/drivers/adodb-mysqli_log.inc.php' for inclusion

- http://10.10.236.31/openemr/interface/main/tabs/main.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/tabs/main.php on line 5137
**

- http://10.10.236.31/openemr/interface/main/tabs/main.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/tabs/main.php on line 5137
**

Request

```
POST /openemr/interface/main/main_screen.php?auth=login&site=default HTTP/1.1
Content-Type: application/x-www-form-urlencoded
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
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
Content-Length: 72
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: 10.10.236.31
Connection: Keep-alive

authUser[]=1&clearPass=1&languageChoice=1&new_login_session_management=1
```

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 /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: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://192.168.145.128/openemr
Cookie: OpenEMR=fLVw-dnCSUl23MMDJ4XDEmokIFfZN%2CUphA0oNxhYRlFnqazp
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://10.10.236.31/

Development configuration files:

- http://10.10.236.31/openemr/**package.json**

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

- http://10.10.236.31/openemr/**composer.json**

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

- http://10.10.236.31/openemr/**composer.lock**

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

- http://10.10.236.31/openemr/**package-lock.json**

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

- http://10.10.236.31/openemr/public/assets/knockout/**package.json**

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

Request

```
GET /openemr/package.json HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
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: 10.10.236.31
Connection: Keep-alive
```

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 acessible 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://10.10.236.31/ Verified

Folders with directory listing enabled:

- http://10.10.236.31/openemr/interface/
- http://10.10.236.31/openemr/interface/login/
- http://10.10.236.31/openemr/public/assets/moment/min/
- http://10.10.236.31/openemr/public/assets/knockout/build/output/
- http://10.10.236.31/openemr/public/
- http://10.10.236.31/openemr/interface/main/
- http://10.10.236.31/openemr/public/assets/i18next/dist/umd/
- http://10.10.236.31/openemr/public/assets/knockout/
- http://10.10.236.31/openemr/public/assets/knockout/build/
- http://10.10.236.31/openemr/library/js/
- http://10.10.236.31/openemr/Documentation/
- http://10.10.236.31/openemr/Documentation/help_files/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/
- http://10.10.236.31/openemr/public/assets/hotkeys-js/dist/
- http://10.10.236.31/openemr/library/js/vendors/
- http://10.10.236.31/openemr/library/js/vendors/validate/
- http://10.10.236.31/openemr/public/assets/jquery-datetimepicker/build/
- http://10.10.236.31/openemr/interface/main/messages/css/
- http://10.10.236.31/openemr/public/assets/jquery/
- http://10.10.236.31/openemr/interface/main/dated_reminders/
- http://10.10.236.31/openemr/interface/product_registration/

Request

```
GET /openemr/interface/ HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
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: 10.10.236.31
Connection: Keep-alive
```

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://10.10.236.31/

Documentation files:

- http://10.10.236.31/openemr/**README.md**
  File contents (first 100 characters):

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

- http://10.10.236.31/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://10.10.236.31/openemr/public/assets/knockout/**README.md**
  File contents (first 100 characters):

  ```
  # Knockout

  **Knockout** is a JavaScript [MVVM]
  (http://en.wikipedia.org/wiki/Model_View_ViewModel) ...
  ```

Request

```
GET /openemr/README.md HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
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: 10.10.236.31
Connection: Keep-alive
```

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 acessible 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

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

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

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

http://10.10.236.31/

Possible sensitive directories:

- http://10.10.236.31/openemr/**bin**
- http://10.10.236.31/openemr/**sql**
- http://10.10.236.31/openemr/**config**
- http://10.10.236.31/openemr/**tests**
- http://10.10.236.31/openemr/**src**

Request

```
GET /openemr/bin/ HTTP/1.1
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
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: 10.10.236.31
Connection: Keep-alive
```

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

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://10.10.236.31/

Possible sensitive files:

- http://10.10.236.31/openemr/**admin.php**

Request

```
GET /openemr/admin.php HTTP/1.1
Accept: ydabcrvp/kkoy
Cookie: OpenEMR=bbs8OgzIFbvo7hR%2Cj5ZvMq%2C3QTQmauASLmo3p3YX9WgoZJp2
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: 10.10.236.31
Connection: Keep-alive
```

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://10.10.236.31/

Emails found:

- http://10.10.236.31/openemr/acknowledge_license_cert.html **ajabour@iupui.edu**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **andres@paglayan.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **superarnab@gmail.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **drbowen@bowenmd.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **bss@iguanasuicide.net**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **brady.g.miller@gmail.com**

- http://10.10.236.31/openemr/acknowledge_license_cert.html **pandi.param@capminds.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **stephen.waite@cmsvt.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **amit@comlinkinc.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **sbhayani@communitybehavioralhealth.net**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **ramesh@ensoftek.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **george.tye@gmail.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **stone@annashaegrp.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **fndtn357@gmail.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **sherwin@affordablecustomehr.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **julia.longtin@gmail.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **ptspohnpei@gmail.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **kevin.y@integralemr.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **openemr@lillysystems.com**
- http://10.10.236.31/openemr/acknowledge_license_cert.html **mscltd@earthlink.net**
- http://10.10.236.31/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: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/interface/login/login.php
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: 10.10.236.31
Connection: Keep-alive
```

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: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/interface/login/login.php
Cookie: OpenEMR=F-6X1PVslYyH8tuel82CU%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

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://10.10.236.31/

Request

```
GET /KnNz3PhQmq 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: 10.10.236.31
Connection: Keep-alive
```

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://10.10.236.31/

Pages with paths being disclosed:

- http://10.10.236.31/openemr/interface/main/main_screen.php **(/var/www/html/openemr/vendor/adodb/adodb**
- http://10.10.236.31/openemr/interface/main/messages/messages.php **(/var/www/html/openemr/vendor/adodb/adodb**
- http://10.10.236.31/openemr/library/ajax/dated_reminders_counter.php **(/var/www/html/openemr/vendor/adodb/adodb**
- http://10.10.236.31/openemr/library/ajax/i18n_generator.php **(/var/www/html/openemr/vendor/adodb/adodb**

- http://10.10.236.31/
  >/var/www/html/index.html
- http://10.10.236.31/openemr/interface/main/calendar/index.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/interface/login/login.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/interface/main/tabs/main.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/interface/main/dated_reminders/dated_reminders.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/portal/
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/Readme_edihistory.html
  /var/www/htdocs/openemr/sites/
- http://10.10.236.31/openemr/portal/messaging/secure_chat.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/help_files/adminacl_help.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/README-Log-Backup.txt
  /var/www/openemr
- http://10.10.236.31/openemr/Documentation/help_files/cms_1500_help.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/help_files/configure_orders_help.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/library/ajax/imm_autocomplete/search.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/help_files/mfa_help.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/library/ajax/document_helpers.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/interface/login_screen.php
  (/var/www/html/openemr/vendor/adodb/adodb
- http://10.10.236.31/openemr/Documentation/help_files/openemr_installation_help.php
  /var/www/html/openemr

Request

```
GET /openemr/interface/main/main_screen.php HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr
Cookie: OpenEMR=Dj68HNoGw-vYWT2k81NHDiqIHhLtRgfoVY0Tqo%2Cj6JeJm5aU
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: 10.10.236.31
Connection: Keep-alive
```

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-dnCSUl23MMDJ4XDEmokIFfZN%2CUphA0oNxhYRlFnqazp
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

25 Incorrect Default Permissions

During installation, installed file permissions are set to allow anyone to modify those files.

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://10.10.236.31/ Verified

- **Missing object-src in CSP Declaration**
  - **First observed on:** http://10.10.236.31/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: 10.10.236.31
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
```

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,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

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

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

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

None

http://10.10.236.31/ Verified

Pages where the content-type header is not specified:

- http://10.10.236.31/openemr/composer.lock
- http://10.10.236.31/openemr/LICENSE
- http://10.10.236.31/openemr/Documentation/README.phpgacl
- http://10.10.236.31/openemr/Documentation/INSTALL
- http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/COPYING
- http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/README
- http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/default.conf
- http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/lang.eng
- http://10.10.236.31/openemr/interface/main/calendar/modules/PostCalendar/pntemplates/default/config/navigation.conf

Request

```
GET /openemr/composer.lock HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 8595e182db21cbbc10c83c2c4cf193d3
Acunetix-Aspect-ScanID: 816589585389164376
Acunetix-Aspect-Queries: packages;aspectalerts;routes
Referer: http://10.10.236.31/openemr/
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: 10.10.236.31
Connection: Keep-alive
```

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: d4d608fef00a58adee3950d33ced68a7
Acunetix-Aspect-ScanID: 1655702786608078775
Acunetix-Aspect-Queries: aspectalerts;routes
Referer: http://192.168.145.128/openemr/
Cookie: OpenEMR=F-6X1PVslYyH8tuel82CU%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).

No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

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: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

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://10.10.236.31/

Request

```
GET / 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: 10.10.236.31
Connection: Keep-alive
```

http://192.168.145.128/

Request

```
GET / 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

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

Coverage

- http://192.168.145.128/
- http://192.168.145.128/openemr/
- http://192.168.145.128/openemr/public/assets/checklist-model/
- http://192.168.145.128/openemr/vendor/
- http://10.10.236.31/
- http://10.10.236.31/openemr/
- http://10.10.236.31/openemr/vendor/