ODOO

IS IT SAFE AND SECURE?

INVESICS

What is ODOO?

- **Odoo** is an all-in-one management software that offers a range of business applications that form a complete suite of enterprise management applications targeting companies of all sizes. - including CRM, website/e-commerce, billing, accounting, manufacturing, warehouse - and project management, and inventory.
- The prime benefit of Odoo is its extensible architecture. A large number of freelancers and organizations develop Odoo Apps or Modules and place them in the marketplace for sale or to be downloaded for free.
- The main Odoo components are the Open Object framework, about 30 core modules (also called official modules) and more than 5000 community modules. Most Odoo modules are available in Odoo S.A's marketplace where community could buy or download many modules for free.
- As per 9 July 2018, 15759 Apps or modules were found on the marketplace in different categories. Most modules are served in all active versions of 9.0, 10.0 and 11.0.
- Odoo uses Python scripting and PostgreSQL database. The software is accessed via a web browser in a one page app developed in JavaScript. The Community edition repository is on GitHub.

Ref: https://en.wikipedia.org/wiki/Odoo

Odoo Security

Below are the security practices done by Odoo team to ensure security on Odoo cloud:

- **Backup and disaster recovery:** Odoo provides full backups for its instances up to 3 months. Odoo also has effective disaster management practices, with worst case scenario where the users can lose maximum 24 hours of work if data cannot be recovered and restores the last daily backup.
- **Database security:** Customer data is stored in a dedicated database, where data is not shared between clients. Data access control rules implement complete isolation between customer databases.
- **Password security:** Customer passwords are protected with industry standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds).Odoo staff does not have user passwords. If you lose it, you have to reset it.
- **Employee access:** Odoo staff may access user accounts to fix support issues (with use of a staff authorization, not user password).
- **System security:** All Odoo online servers are running hardened Linux distributions. Only a few trusted Odoo engineers have clearance to remotely manage the servers. Firewall and intrusion countermeasures prevent unauthorized access.

Ref: https://www.odoo.com

- **Physical security:** Security cameras are monitoring the physical data centres. Physical access to data centres where Odoo servers are located is restricted to data centre technicians only.
- **Communications:** All web connections to client instances are protected with 256 bit SSL encryption. Odoo servers are always under watch and patched against latest SSL vulnerabilities.

Odoo Software Security

- Odoo being an open source software, the whole codebase is constantly under observation by Odoo users and contributors worldwide. Community bug reports are an important source of feedback regarding security issues and Odoo encourages developers to audit the code and report security issues.

Ref: https://www.odoo.com

Is Odoo really secure? ..still it is not hack proof.

Some recent vulnerabilities in Odoo which got exploited:

- **CVE-2017-10803:**
  In Odoo 8.0, Odoo Community Edition 9.0 and 10.0, and Odoo Enterprise Edition 9.0 and 10.0, insecure handling of anonymization data in the Database Anonymization module allows remote authenticated privileged users to execute arbitrary Python code, because unpickle is used.
- **CVE-2017-10804:**
  In Odoo 8.0, Odoo Community Edition 9.0 and 10.0, and Odoo Enterprise Edition 9.0 and 10.0, remote attackers can bypass authentication under certain circumstances because parameters containing 0x00 characters are truncated before reaching the database layer. This occurs because Psycopg 2.x before 2.6.3 is used.
- **CVE-2017-10805:**
  In Odoo 8.0, Odoo Community Edition 9.0 and 10.0, and Odoo Enterprise Edition 9.0 and 10.0, incorrect access control on OAuth tokens in the OAuth module allows remote authenticated users to hijack OAuth sessions of other users.
- **CVE-2017-9416:**
  Directory traversal vulnerability in tools.file open in Odoo 8.0, 9.0, and 10.0 allows remote authenticated users to read arbitrary local files readable by the Odoo service.

Ref: https://www.cvedetails.com

Our Manual VAPT on Odoo platform

- We have practiced manual vulnerability assessment and panitration testing process on Odoo based systems and found general vulnerabilities that presents in system when there is no extra care is taken while development.

- Every Cyber-attack is a designed attack - where vulnerabilities will be put in a sequence to get the access of the data or the system. Following vulnerabilities can be used as an attack vector to make the designed attack successful.

- It is found that there are more vulnerabilities available in the Odoo platform that is not patched yet. These are based on development standards, server configurations, network and much more. It is better to have a professional Security Test performed to avoid such attacks and future business loss or reputation loss due to them.

Cookie poisoning

Description:

- Cookie poisoning is the act of manipulating or forging a cookie (a small piece of data created and stored in a user's browser that keeps track of important information regarding his or her session information for a particular site) for the purpose of bypassing security measures or sending false information to a server.
- An attacker using cookie poisoning can gain unauthorized access to a user's account on the particular site the cookie was created for, or potentially tricking a server into accepting a new version of the original intercepted cookie with modified values.

Impact:

- Can be used to steal personal and sensitive data like personal information, credit card details, passwords, etc. as it is saved on Odoo cloud.
- It can also be used for session hijacking.

Session Termination

Description:

- Session termination is an important part of the session lifecycle.
- To properly terminate a session some manual or automated functions are needed , for manual termination of a process logout functionality is provided and for automatic termination session timeouts are used.
- Adding to this if the site doesn’t have a proper session timeout then attacker can easily restore sessions if gets hand on the session keys.

Impact:

- Sessions can be restored without user credentials.
- If a Odoo developers session is restored it can be used for stealing confidential data or to add malicious code in the environment.
- Improper session termination can lead to attacks like Cross Site Scripting(XSS) and Cross Site Request Forgery(CSRF) as they mostly rely on a user having an authenticated session present.

Broken Access Control

Description:

- Access control, sometimes called authorization, is how a web application grants access to content and functions to some users and not others. These checks are performed after authentication, and govern what ‘authorized’ users are allowed to do.
- Access control sounds like a simple problem but is insidiously difficult to implement correctly. A web application’s access control model is closely tied to the content and functions that the site provides.
- An example would be /admin, /settings or similar that only an admin should be allowed to visit. If any user can access those, this would be considered a vulnerability.

Impact:

- The potential impact of Broken Access Control greatly depends on what kind of information or features the attacker can gain access to. This can be anything from seemingly useless information to a full system takeover.
- If certain files containing the configuration or source code of any Odoo component are accessed by the hacker it can lead to major attacks depending on the information he gets.

Cross Site Request Forgery

Description:

- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.
- With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
- It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet.

Impact:

- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, purchasing something, changing their email address, and so forth.
- If the victim is an administrative account, CSRF can compromise the entire web application i.e. Odoo software in this case.

Cross Site Scripting(XSS)

Description:

- Cross-site scripting (XSS) is a type of injection security attack in which an attacker injects data, such as a malicious script, into content from otherwise trusted websites.
- Cross-site scripting attacks happen when an untrusted source is allowed to inject its own code into a web application, and that malicious code is included with dynamic content delivered to a victim's browser.

Impact:

- The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account.
- Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirect the user to some other page or site, or modify presentation of content(content spoofing).
- For example a successful attack can change the values of the prices of products in an e-commerce website.

Code Injection

Description:

- Code Injection is the general term for attack types which consist of injecting code that is then interpreted/executed by the application. This type of attack exploits poor handling of untrusted data.
- These types of attacks are usually made possible due to a lack of proper input/output data validation, for example:
  - allowed characters (standard regular expressions classes or custom)
  - data format
  - amount of expected data

Impact:

- If successfully exploited, impact could cover loss of confidentiality, loss of integrity, loss of availability, and/or loss of accountability.
- Many attacks are possible through code injection depending upon the injecting language.
- SSI injection, XML injection, SQL injection, LDAP injection are some related attacks to the code injection.
- Odoo also uses SQL, so a successful SQL Injection may lead in compromising of database or can just extract important data from the database.

Using HTTP Connection

Description:

- HTTP stands for Hyper Text Transfer Protocol. HTTP is designed to permit intermediate network elements to improve or enable communications between clients and servers, but it lacks security.
- All data, which is sent between the browser and the server, can be intercepted. In HTTP the data isn't encrypted with SSL/TSL Certificates.

Impact:

- Any data sent over an http connection is not encrypted i.e. it is in plain text which is the biggest threat as it can disclose every single bit of data and details about the session.
- HTTP is vulnerable to all severe vulnerabilities like SQL Injection, XSS, Broken Authentication and Session Management, Insecure Direct Object Reference, CSRF, etc.
- Moreover google has decided to label all the HTTP sites as not secure in its future update of google chrome.
- If an Odoo client tries to connect with Odoo using HTTP connection anyone in the same network will be able to capture the data and easily extract sensitive information like username and password, credit card details, etc. with help of packet capturing tools like wireshark or burpsuite.

Sensitive Data Exposure

Description:

- Sensitive Data Exposure occurs when an application does not adequately protect sensitive information.
- The data can vary and anything from passwords, session tokens, credit card data to private health data and more can be exposed.

Impact:

- As the finding only applies to sensitive data, the potential impact is always considered high. What the data consists of varies and so does the impact. The danger lies in the data being exposed, and the potential impact reflects the data's sensitivity.
- For example, if credit card data is stolen, the attacker can empty the victim's bank account. If passwords are exposed, the attacker can abuse these credentials. If certificates are stolen, the attacker can pretend to be the target. It all depends on what kind of data is at risk of being exposed.

Clickjacking

Description:

- Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page.
- Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Impact:

- A single click is required to download and install a malware on someone’s device or to open a malicious link which is easily possible by clickjacking.
- Some other attacks possible are likejacking , cursorjacking and password manager attack.
- A user might receive an email with a link to a video about a news item, but another webpage, say a product page on Odoo, can be "hidden" on top or underneath the "PLAY" button of the news video. The user tries to "play" the video but actually "buys" the product from that page. The hacker can only send a single click, so they rely on the fact that the visitor is both logged into that Odoo page and has 1-click ordering enabled.

Cross Frame Scripting(XFS)

Description:

- Cross-Frame Scripting (XFS) is an attack that combines malicious JavaScript with an iframe that loads a legitimate page in an effort to steal data from an unsuspecting user.
- This attack is usually only successful when combined with social engineering.
- An example would consist of an attacker convincing the user to navigate to a web page the attacker controls. The attacker's page then loads malicious JavaScript and an HTML iframe pointing to a legitimate site. Once the user enters credentials into the legitimate site within the iframe, the malicious JavaScript steals the keystrokes.

Impact:

- An attacker might use a hidden frame to carry out a Cross-site Scripting (XSS) attack.
- An attacker might use a hidden frame to carry out a Cross-Site Request Forgery (CSRF) attack.
- An attacker might use a visible frame to carry out a Clickjacking attack.
- An XFS attack exploiting a browser bug which leaks events across frames is a form of a Phishing attack (the attacker lures the user into typing-in sensitive information into a frame containing a legitimate third-party page).

Information Disclosure

Description:

- Information disclosure is when an application fails to properly protect sensitive information from parties that are not supposed to have access to such information in normal circumstances.
- These type of issues are not exploitable in most cases, but are considered as web application security issues because they allows attackers to gather information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn't get access to such information.
- Different types of information disclosure includes Banner Grabbing, Path Traversal, Directory listing, Source code disclosure.

Impact:

- Information disclosure issues can range in the criticality of the information leaked, from disclosing details about the server environment to the leakage of administrative accounts credentials or API secret keys, which may have devastating outcomes on the vulnerable web application i.e. Odoo in our case.

Odoo is not Secure. Does your Odoo App??

info@invesics.com