ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ПОТИКЕВИЧ Михайло Іванович

Аналіз методів розробки захищених ERP-систем

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2019

Дипломною роботою є рукопис.

Роботу виконано у Тернопільському національному технічному університеті імені Івана Пулюя.

Науковий керівник: кандидат педагогічних наук, доцент
Кареліна Олена Володимирівна,
Тернопільський національний технічний університет імені Івана Пулюя, кафедра кібербезпеки, доцент.

Рецензент: кандидат технічних наук, доцент
Баран Ігор Олегович
Тернопільський національний технічний університет імені Івана Пулюя, декан факультету ФІС

Підпис:_____

Захист відбудеться 24 грудня 2019 р. о __ год. на засіданні Державної екзаменаційної комісії у Тернопільському національному технічному університеті імені Івана Пулюя за адресою:
46001, м. Тернопіль, вул. Руська, 56.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Кожне підприємство прагне зайняти становище на ринку, а для цього необхідно правильно і раціонально управляти своїм виробництвом. У сучасних умовах ефективне управління являє собою цінний ресурс організації

Найбільш очевидним способом підвищення ефективності протікання трудового процесу є його автоматизація.

Значною перевагою ERP-системи є високий коефіцієнт прискорення обробки фінансових обчислень, швидкості виконання всіх замовлень, створення та формування звітів щодо прибутків та зведення фінального балансу.

Ядро кожної компанії - це ERP система, в ній проходять всі основні для бізнесу процеси. Вся інформація, що зберігається в ERP-системах, має найважливіше значення, і будь-який неправомірний доступ до неї може понести за собою величезні втрати включно аж до зупинки бізнесу.

Важливою стадією розробки ERP-системи є вибір методів реалізації, від яких в подальшому буде залежати надійність та захищеність кінцевого продукту.

Мета і завдання дослідження. Метою дипломної роботи є порівняння методів розробки ERP-систем, та вибір найбільш ефективного з них.

Об'єктом дослідження дипломної роботи є ризики несанкціонованого доступу до ERP-системи.

Предметом дослідження є пошук найбільш ефективного методу розробки захищеної ERP-системи.

Методи дослідження. В процесі дослідження нами було порівняно основні методи розробки веб-проектів:

1. Написання проекту без використання зовнішніх бібліотек
2. Реалізація проекту з підключенням зовнішніх бібліотек
3. Використання CMS/фреймворків для реалізації проекту

Опираючись на вихідні дані порівняння методів нами було обрано метод розробки на базі CMS та фреймворків.

Наукова новизна роботи:

Для захисту від несанкціонованого доступу засобами Bitrix Framework було реалізовано функціонал, який унеможливлює доступ сторонніх осіб до ERP-системи у позаробочий час засобами Bitrix Framework.

Практичне значення полягає у тому, що доступ до інформаційних ресурсів унеможливлюється у позаробочий час, фіксуючи при цьому спроби авторизації сторонніх осіб.

Апробація результатів дослідження. Тестування функціоналу проводилось на віртуальній машині. Спроби взаємодії з ERP-системою проводились з різних користувацьких аккаунтів з різними рівнями доступу.

Структура роботи. Дипломна робота складається із вступу, 8-ми розділів, висновків, списку використаних джерел із ... найменувань. Робота містить ... рисунків і ... лістингів. Обсяг основного тексту становить ... сторінок, перелік використаних джерел ... сторінки. Загальний обсяг дипломної роботи складає ... сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано ефективність використання ERP-систем для управління ресурсами та важливість реалізації комплексу систем захисту від несанкціонованого доступу.

У першому розділі — "Аналіз методів розробки захищених ERP - систем" — Оглянуто інуючі ERP-системи та проаналізовано їхні переваги та недоліки

У сучасному бізнесі необхідність автоматизації різних процесів стала вже звичним явищем. Вже стає складно уявити собі складський або бухгалтерський облік без застосування спеціалізованого програмного забезпечення, торгові представники використовують спеціальні програми для оформлення та відправлення замовлення в офіс прямо з комунікаційних пристроїв, таких, як смартфон чи планшет.

Для компаній та фірм, які володіють великими потужностями, необхідно чітко керувати ресурсами підприємства, саме це і дозволяє реалізувати різноманітні ERP системи.

Впровадження ERP-системи дає можливість автоматизації управління дебіторською і кредиторською заборгованостями, зменшення складських запасів, калькуляції всіх видів продукції, статистичної обробки архівних даних, а також оптимізації внутрішніх бізнес-процесів, звільненні менеджерів від рутинної роботи і, як наслідок, поліпшення ефективності діяльності підприємства та підвищення конкурентоспроможності.

Перевагою ERP-системи є не тільки прискорення виконання певних видів робіт, наприклад, обробка замовлень, розрахунок фінансових показників, формування звіту з прибутків, зведення балансу. Основним ефектом є можливість прийняття оперативних управлінських рішень на основі повної, достовірної інформації завдяки створеній єдиній базі даних. При цьому скорочується час на виконання рутинних робіт і збільшується відповідно для аналітичної роботи.

За даними веб-сайту livebusiness можна виділити основні ERP системи, яким надають перевагу користувачі.

Найбільш популярним продуктом є розробка німецької компанії SAP AG, а саме - покоління S. Самі розробники позиціонують свій проект, як ERP-система орієнтована на великі і середні підприємства. Перевагами даної системи є велика база модулів, які призначені для максимального розширення спектру можливого функціоналу програмного продукту.

Другою за популярністю ERP системою є Oracle NetSuite ERP.

Netsuite ERP - це програмне забезпечення ERP, яке дозволяє користувачам оптимізувати бізнес-процеси, такі як управління фінансами, закупівлі і багато іншого. Його функції також включають в себе бізнес-аналітику і масштабовану систему управління бізнесом.

Dynamics 365 є серед найбільш популярних ERP систем. Даний продукт був створений у 2016 році компанією Microsoft. Великою перевагою Dynamics 365 є те, що розширювати його функціонал можна за допомогою плагінів написаних на JavaScript, який з кожним роком стає все популярнішим та розширює сферу свого використання.

Більшість популярних ERP систем є справді потужними інструментами, але через велику кількість функціоналу та сторонніх модулів система стає вразливою до хакерських атак.

Кіберзлочинність зараз розвинена як ніколи - адже майже кожна компанія має свій сайт в інтернеті, а зловмисник у мережі може легко залишатися анонімним.

Кількість загроз зростає пропорційно зростанню бізнесу, проте, як показує багаторічна статистика, 99% атак відбуваються через десяток стандартних помилок валідації даних, або виявлені вразливості у встановлених компонентах програмного забезпечення сторонніх виробників, або банально, через недбальство системних адміністраторів, які використовують налаштування і паролі, встановлені за замовчуванням.

Класифікацією векторів атак і вразливостей займається спільнота OWASP. Це міжнародна некомерційна організація, зосереджена на аналізі та поліпшення безпеки програмного забезпечення.

OWASP створив список з десяти найбільш небезпечних векторів атак на Web-додатки. Клієнтські компоненти ERP - систем часто працюють через web-інтерфейс, які зазвичай містять у собі критичні вразливості, такі я веб форми і поля для завантаження файлів на сервер. Даний список вразливостей отримав назву OWASP TOP-10 і в ньому зосереджені найнебезпечніші уразливості, які можуть коштувати деяким людям великих грошей, або підриву ділової репутації, аж до втрати бізнесу.

До цього списку потрапили:

- ін'єкції – Injections;
- недоліки системи аутентифікації і зберігання сесій;
- міжсайтовий скриптинг – XSS;
- небезпечні прямі посилання на об'єкти;
- небезпечна конфігурація;
- незахищеність критичних даних;
- відсутність функцій контролю доступу;
- міжсайтова підробка запиту;
- використання компонентів з відомими вразливостями;
- неперевірені переадресації та пересилання.

У другому розділі — “ Методи розробки та захисту ERP-систем” — Оглянуто та проведено порівняльний аналіз методів розробки захищених ERP-систем.

За результатами дослідження В.В. Голян та О.К. Кравченко було представлено декілька варіантів життєвих циклів програм. Найбільш придатними до використання у нашій роботі є модель водоспаду, модель Agile та RAD.

У своїй статті О.К. Кравченко описує водоспадну модель наступним чином: “Модель водоспаду розвиває програмне забезпечення поступово - операційний аналіз, експлуатаційні специфікації, специфікації проектування і кодування, розробка, тестування, розгортання, оцінка”.

Найголовнішим плюсом самописних проектів є суттєва перевага у гнучкості. Жодна CMS не дозволить створити настільки гнучку систему.

Мінуси у самописних проектів теж присутні. Перший і основний - ціна розробки.

Для прикладу, реалізація класу з методами для роботи з базою даних може зайняти більше 30 годин роботи програміста, при тому не виключено, що при реалізації даного функціоналу не буде допущено критичної помилки у валідації даних.

Також підтримка таких проектів суттєво складніша, якщо порівнювати з проектами реалізованих на популярних фреймворках чи CMS.

У більшості випадків для популярних фреймворків та CMS передбачено документації. Звідси з'являється ще один мінус, а саме те, що будь-які двигуни після своєї розробки та запуску проекту вимагають оновлень, наприклад, для додавання нових функції, не компетентні розробники, або ті, які не були залучені до розробки даного ПЗ можуть відчути складнощі при роботі з ядром.

Для більшості типових задач, які притаманні веб-проектам, вже є готові рішення у вигляді бібліотек, на які можна покласти роботу з БД, дії з поштою, роботу із зображеннями, графіками тощо.

Для роботи з базами даних можна виділити 3 основні бібліотеки, а саме:

1. Doctrine ORM,
2. Query Builder,
3. ADOdb.

З CMS все доволі зрозуміло: широкий функціонал з коробки, багатий набір як платних, так і безкоштовних модулів і плагінів, швидка установка і настройка сайту.

Різниця починає з'являтись, коли виникає потреба змінити / доповнити функціонал веб-проекту. Основна перевага використання фреймворка в розробці - гнучкість і широкі можливості.

Використання фреймворка не накладають на розробника обмежень, що існують в розробці під CMS. Фреймворки функціонують однаково, позбавляючи вас від необхідності постійно створювати одні й ті ж методи та класи.

Laravel - це безкоштовний PHP фреймворк з відкритим вихідним кодом, створений Тейлором Отвеллом для розробки веб-додатків за архітектурним шаблоном MVC.

Він був створений як альтернатива такому фреймворку, як Codeigniter, в якому було недостатньо корисних функцій для розробки веб-додатків. В якості основи Laravel виступають компоненти іншого фреймворка - Symfony.

Після виходу PHP 7 в порівнянні з PHP 5, скрипти стали швидше і почали використовувати набагато менше оперативної пам'яті, а в зв'язці з Zend OPCache показують чудові результати. Зокрема сервіс Laravel Forge налаштовує Zend OPCache для досягнення максимальної продуктивності.

Саме тому, коли йде мова про продуктивність того чи іншого PHP-фреймворку, то завжди проводять тестування без кешування, роботи з БД або файлами, в основному роблячи мільйони викликів до звичайної PHP сторінки. В цьому плані даний PHP-фреймворк істотно нічим не відрізняється від всіх інших, але коли мова йде про масштабованість, гнучкість, універсальність вбудованих механізмів

кешування і швидкість розробки, саме тоді Laravel показує всю свою гнучкість і переваги.

Symfony - другий за популярністю PHP-фреймворк. Він побудований на основі патерну проектування MVC, у вигляді штатного шаблонізатора використовується Twig.

Для роботи з БД застосовується Doctrine Object Relation Mapper, що надає потужний Dependency Injection Container, включає в себе парсер конфігурації з форматів XML і YAML, конструктор легко валідує форми, інструменти для тестування, кешування, роботи з мультимовами, а також продуману Security-компоненту для роботи з аутентифікацією і авторизацією користувачів.

Фреймворк YII 2 реалізує парадигму MVC і підходить для розробки додатків будь-якої складності, особливо якщо мова йде про великий проект: форуми, інтернет-магазини, портали чи не стандартні веб-проекти.

Yii можна вважати одним з лідируючих за популярністю фреймворком.

Переваги Yii - це висока продуктивність та швидкість роботи і хороша підтримка ООП. Yii включає в себе велику кількість бібліотек. Завдяки їм можна без підключення зовнішніх сервісів створити веб-додаток, яке відповідатиме всім сучасним стандартам. Вбудовані методи дозволяють значно скорочувати кількість коду.

Zend Framework 3 є фреймворком з відкритим вихідним кодом для розробки web-додатків на PHP 5.3 +. Використовує тільки об'єктно-орієнтований код і всі нововведення PHP від версії 5.3 і вище, а саме: namespaces, late static binding, lambda functions and closures. Більш ніж 15 мільйонами сайтів використовують його.

На відміну від Zend Framework при розгортанні Bitrix Framework ми отримуємо не тільки набір класів, а й розвинений інтерфейс адміністрування. У базовій поставці йде великий набір компонентів, і саме він забезпечує швидке розгортання і впровадження проектів.

Великою перевагою Bitrix є те, що розробнику не доводиться працювати з прямими запитами до БД. Замість цього у даній CMS реалізована система інформаційних блоків.

Інформаційні блоки - ключовий момент Bitrix Framework. Практично все, що робиться в системі в тій чи іншій мірі зав'язано на цей модуль, навіть якщо це і не відображається явно.

Інформаційні блоки представляють собою черговий рівень абстракції над звичайними таблицями СУБД, своєрідна "база даних в базі даних". Тому до них частково застосовні всі ті правила, яких дотримуються при проектуванні БД.

Інфоблоки - сутність, яка в фізичну структуру БД створює 4 таблиці, не змінюються при зміні структури даних: типи об'єктів, екземпляри об'єктів, властивості об'єктів і значення властивостей об'єктів.

Плюси такого підходу:

- зручний контроль над даними такої структури зі свого додатка,
- універсальність методів,
- загальна структура даних для будь-якого проекту,

- можливість багаторазово змінювати типи даних для полів без знищення самих даних.

Мінуси такого підходу:

- підвищені вимоги до продуктивності,
- непрозорість при прямому доступі до даних.

У третьому розділі — “ Практичне застосування Bitrix Framework для реалізації захищеної ERP-системи” —

CMS 1-С Бітрікс, яка побудована на базі Bitrix Framework вже з коробки містить у собі величезний функціонал призначений для запобігання можливих вразливостей самої системи.

Проактивний фільтр (WAF - Web Application Firewal) забезпечує захист від більшості відомих атак на веб-додатки. У потоці зовнішніх запитів користувачів проактивний фільтр розпізнає більшість небезпечних загроз і блокує вторгнення на сайт. Проактивний фільтр - найбільш ефективний спосіб захисту від можливих помилок безпеки, допущених при реалізації інтернет-проекту (XSS, SQL Injection, PHP Including і ряду інших). Дія фільтра заснована на аналізі і фільтрації всіх даних, що надходять від користувачів через змінні і куки.

У Журналі вторгнень реєструються всі події, що відбуваються в системі, в тому числі незвичайні або зловмисні. Оперативний режим реєстрації цих подій дозволяє переглядати відповідні записи в Журналі відразу ж після їх генерації. У свою чергу, це дозволяє виявляти атаки і спроби атак в момент їх проведення. Це означає, у вас є можливість негайно вживати відповідних заходів, і, в деяких випадках, навіть попереджати атаки.

Після встановлення Бітрікс на період розробки нами було встановлено додаткова форма авторизації на рівні веб-серверу, налаштовано резервне копіювання, увімкнено двохфакторну авторизацію. Після створення функціональних скриптів було проведено цементування – заборона внесення змін на рівні операційної системи веб-сервера.

Якою б добре захищеною не була інформаційна система, у ній завжди залишаються певні вразливості, які можуть з’являтись під час додавання правок у готовий проект чи виправлення старих помилок.

Забезпечення захисту має здійснюватися як на етапі проектування і розробки самого web-додатку, шляхом створення безпечного коду web-додатку і планування раціонального складу системи захисту, так і в процесі його експлуатації з внесенням у разі необхідності своєчасних коригувань. Оскільки навіть якщо web-додаток написано без помилок і уразливості в ньому немає, необхідний комплексний захист, що враховує наявність бази даних додатків, веб-сервера і інших елементів IT-платформи.

Це досягається за рахунок застосування наступних засобів і методів захисту:

- недопущення помилок в скриптах при розробці web-додатку;
- сканування коду web-додатку на наявність вразливостей і установка спеціальних водяних знаків;

- використання систем багатофакторної аутентифікації користувачів (наприклад, парольна аутентифікація з секретним кодом, E-num, сертифікати, цифрові підписи, біометрична аутентифікація);
- застосування антивірусного програмного забезпечення;
- застосування захищених каналів зв'язку і мережевих протоколів під час активного з'єднання клієнта.

Всі ці заходи потрібно виконувати в комплексі, оскільки захист окремих аспектів не принесе бажаного ефекту. Таким чином, життєвий цикл розробки і супроводу захищеного web-додатку пропонується реалізовувати у вигляді циклічного процесу.

В свою чергу ми пропонуємо обмеження доступу до інформаційного ресурсу, у певні години для користувачів, які не є у "білому листі" сервісу.

Таким чином вдається суттєво зменшити можливість доступу до ресурсу сторонніх осіб.

У якості "білого листа" IP адрес використовується інформаційний блок, властивостями є IP адреса, посада та електронна скринька користувача, яка використовується для авторизації у ERP-систему.

Для контролю дій користувача на сайті у позаробочий час реалізовано функціонал логування всіх переходів та відвіданих сторінок.

ВИСНОВКИ

У даній дипломній роботі було проведено комплексний аналіз та порівняння існуючих методів розробки захищених ERP-систем.

У ході дослідження і аналізу існуючих проектів було виявлено основні переваги таких рішень.

Перевагою ERP-системи є прискорення виконання багатьох видів робіт, таких, як обробка замовлень, розрахунок фінансових показників, формування звіту з прибутків.

Проведено дослідження по збору інформації щодо можливих вразливостей притаманних веб-проектам. На основі зібраних даних та інформації від видання OWASP було виділено найбільш поширені та небезпечні загрози.

Після дослідження та збору даних про можливі загроз нами було проведено порівняльний аналіз методів розробки ERP-систем. Серед варіантів розробки було обрано метод з використанням багатофункціональних бібліотек, а саме комплексних фреймворків. Серед лідерів на території України було виділено Laravel, Symfony, YII, Zend Framework та Bitrix Framework.

У результаті порівняння функціоналу, який забезпечить стабільну роботу ERP-системи, а також здатний запропонувати варіанти захисту критично важливих модулів системи, нами було обрано Bitrix Framework.

У третьому розділі нами було продемонстровано чіткий механізм по налаштуванню всіх пунктів модулю "Проактивний захист", який містить у собі функціонал захисту від DDOS атак, відслідковування змін у функціональних файлах скриптів, безпечна авторизація без SSL, проактивний фільтр та інструмент аудиту для безпечного PHP-коду.

На період розробки ERP-система була захищена паролем, який був реалізований за допомогою правил роботи веб-сервера у файлі .htaccess.

Після реалізації проекту усім виконуваним файлам встановлено дозволи тільки на читання, що унеможливлює їх зміну за допомогою можливих вразливостей.

Для інформаційних блоків проведено комплексне налаштування, що дозволяє запобігти зміни інформації користувачами, які мають недостатні права.

На основі наукових робіт було виявлено, що основною проблемою ERP-системи є можливість несанкціонованого доступу. Дану проблему ми вирішили за допомогою розширення стандартного функціоналу 1С:Бітрікс, за допомогою фільтрації вхідних запитів.

Фільтрація відбувається на основі перевірки часу запиту на вхід, IP-адреси, якої відбувається спроба увійти та наявність користувацького аккаунту у “білому листі”.

Отже в кінцевому результаті нами було реалізовано ERP-систему, яка відповідає усім критеріям безпеки, що унеможливлює витоки інформації за межі системи, а також забезпечує захист від атак типу “відмова у обслуговуванні”.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Захист cms 1с:бітрікс від атак типу «міжсайтовий скриптинг» засобами bitrix framework, VII науково-технічної конференція «Snформаційні моделі, системи та технології.

АНОТАЦІЇ

Потикевич М. Дипломна робота на тему «Аналіз методів розробки захищених ERP-систем».

Об'єктом дослідження є процес проектування, розробки та підтримки ERP-системи із забезпеченням збереження даних.

Предметом дослідження є методи розробки захищених ERP-систем у вигляді веб-сайту.

Мета роботи – запропонувати та реалізувати спосіб захисту від несанкціонованого доступу.

Для досягнення мети в даній роботі нами було проаналізовано та вирішено ряд завдань:

1. Розглянуто список існуючих ERP-систем.

2. Проаналізовано можливі методи розробки ERP-системи.

3.Запропоновано метод захисту від несанкціонованого доступу на базі 1С:Бітрікс.

За результатам досліджень було проведено порівняльний аналіз CMS, на базі яких можлива реалізація ERP-системи. Реалізовано скрипт захисту від несанкціонованого доступу на базі Bitrix Framework, що працює за рахунок порівняння IP-адреси користувача, та наявності привілейованого користувача в системі.

Ключові слова: РОЗРОБКА ERP-СИСТЕМИ, BITRIX FRAMEWORK, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ.

Potykevych M. Thesis on "Analysis of methods of development of secure ERP-systems".

The object of the study is the process of designing, developing and maintaining an ERP system to ensure data retention.

The subject of the study is the methods of developing secure ERP systems in the form of a website.

The purpose of the work is to offer and implement an additional method of protection against unauthorized access.

To achieve this goal in the work has been solved a number of problems:

1. The list of existing ERP-systems is considered.

2. Possible methods of development of ERP-System are analyzed.

4. The method of protection against unauthorized access based on 1C: Bitrix is proposed

According to the results of the studies, a comparative analysis of CMS on the basis of which ERP-system implementation is possible was carried out. A Bitrix Framework tamper-proof script is implemented that works by comparing the user's IP address and having a privileged user on the system.

Keywords: ERP-SYSTEM DEVELOPMENT, BITRIX FRAMEWORK, UNAUTHORIZED ACCESS, CONFIDENTIAL DATA PROTECTION.