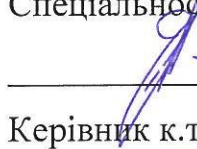


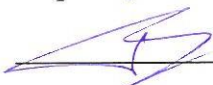
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра на
тему: «Проект підсистеми захисту ресурсів
Web-серверів організації»

Виконав студент 4-го курсу, групи КІ-3
Спеціальності 123 «Комп'ютерна інженерія»


_____ Д.А. Кулик

Керівник к.т.н., доцент, доцент кафедри КІ та КБ


_____ О.В. Пірог

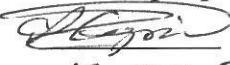
Рецензент к.п.н., доцент, доцент кафедри КІ та КБ


_____ О.С. Головня

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри КІ та КБ

 Сфіменко А. А.
12.04.2021р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Кулика Дениса Артемовича

Тема роботи: Проект підсистеми захисту ресурсів Web-серверів організації

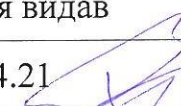
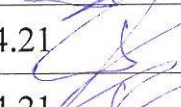
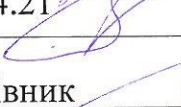
Затверджена Наказом університету від «12» квітня 2021 р. № 133\С

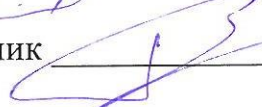
Термін здачі студентом закінченої роботи – 28.06.2021

Вихідні дані для роботи (зазначається предмет і об'єкт дослідження):

- 1) Теоретичні відомості про типи атак на веб-додатки.
- 2) Аналіз ряду способів захисту від веб-атак.
- 3) Реалізація атак.
- 4) Науково-технічна література. Рекомендації.

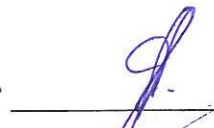
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

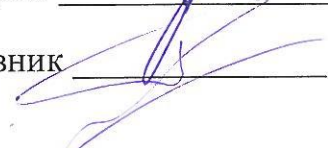
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.	12.04.21 	25.06.21
2	Пірог О.В.	12.04.21 	25.06.21
3	Пірог О.В.	12.04.21 	25.06.21

Керівник  Пірог О.В.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.21	Виконано
2	Розробка плану	15.04.21 – 17.04.21	Виконано
3	Розробка розгорнутого плану	18.04.21 – 19.04.21	Виконано
4	Побача чернетки керівнику для перевірки	25.04.21	Виконано
5	Доопрацювання роботи та перевірка керівником	26.04.21 – 30.05.21	Виконано
6	Затвердження графічних планів у керівника	01.06.21 – 04.06.21	Виконано
7	Проведення попереднього захисту	05.06.21	Виконано
8	Отримання відгуку керівника	21.06.21	Виконано
9	Допуск завідувача кафедри	28.06.21	Виконано
10	Подання роботи на рецензування	28.06.21	Виконано
11	Захист	29.06.21	Виконано

Студент  Кулик Д.А.

Керівник  Пірог О.В.

АНОТАЦІЯ

Текстова частина бакалаврської роботи: 99 сторінок, 60 рисунків, 25 джерел.

Об'єкт дослідження — захист Web-ресурсів.

Мета роботи — використання веб-ресурсу, над яким буде проводитися дослідження.

Предмет дослідження — методи і типи атак на веб-сайти.

Методи дослідження — системний аналіз, порівнювальна характеристика, аналіз сучасних концепцій.

В роботі приведено основні відомості щодо найпопулярніших веб-атак, основ забезпечення безпеки веб-додатків. Сформульовано основні етапи реалізацій веб-атак. Проаналізовано веб-атаки які відбулися за 2019-2020 рік та вразливості, які сприяли цьому.

Проаналізовано веб-атаки, принцип за яким реалізуються веб-атаки та можливі варіанти захисту від них. Також наведено список інструментів для моніторингу безпеки веб-додатків.

Запропоновано підходи можуть бути використані при плануванні та реалізації системи фізичного захисту ІКС будь-якої організації.

Галузь застосування — комп'ютерна мережа.

БЕЗПЕКА, ЗАГРОЗА, АНАЛІЗ, ПОРІВНЯННЯ, ВЕБ-САЙТ, ПОРУШНИК, АТАКА НА ВЕБ-САЙТ, MAGENTO, ЗАХИСТ ВЕБ-САЙТУ, СТАНДАРТИ, ВЕБ-СЕРВІСИ, МЕРЕЖЕВИЙ ПРОСТІР, ІНСКЦІЇ.

КІ.КР.Б – 123 - 21 - ПЗ

					КІ.КР.Б – 123 - 21 - ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту ресурсів Web-серверів організації	Літ.	Арк.	Аркушів	
Розроб.		Кулик Д.А.		28.06.21					
Керівник		Пірог О.В.		28.06.21			4	100	
Реценз.		Головня О.Є.		28.06.21		ФІКТ, гр. КІ-3			
Н. Контр.									
Затверд.		Ефіменко А.А.		29.06.21					

ЗМІСТ

«ПРОЕКТ ПІДСИСТЕМИ ЗАХИСТУ РЕСУРСІВ WEB-СЕРВЕРІВ ОРГАНІЗАЦІЇ».....	Error! Bookmark not defined.
ВСТУП.....	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ТИПИ АТАК НА ВЕБ-ДОДАТКИ	12
1.1 Типи атак на веб-додатки.....	12
1.2 Приклади веб-атак сьогодні.....	21
1.2.1 Підсумки минулого року.....	21
1.2.2 Серед можливих негативних сценаріїв.....	24
1.3 Статистика веб-атак.....	26
1.4 Статистика по галузям	30
1.5 Статистика атак на веб-додатки	36
Висновки до першого розділу.....	42
РОЗДІЛ 2. АНАЛІЗ РЯДУ СПОСОБІВ ЗАХИСТУ ВІД ВЕБ-АТАК.....	44
2.1 Захист від веб-атак.....	40
2.2 Захист веб-ресурсу.....	54
2.3 Порівняння захисту в Україні за період.....	56
2.4 Порівняння тестових і продуктивних систем.....	58
Висновок до другого розділу.....	61
РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАК	64
3.1 Теоретичні відомості про систему керування контентом Magento.....	64
3.2 Знайомство з Magento.....	67
3.3 Реалізація захисту CMS Magento від відповідних атак.....	76
Висновки до третього розділу	95
ВИСНОВКИ.....	96
ПЕРЕЛІК ПОСИЛАНЬ	99

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ASP	– Active Server Pages – технологія що дозволяє динамічно формувати оновлювальні веб-сторінки з боку веб- сервера
API	- Application Programming Interface – інтерфейс програмування додатків, програмний інтерфейс програми
CMS	– Content Management System – система керування вмістом
CSRF	– Cross Site Request Forgery – міжсайтова підробка запиту
DDoS	– Denial-of-Service Attack – розподілена атака на відмову в обслуговуванні
DoS	– Denial of Service – атака на відмову в обслуговуванні
HTML	– HyperText Markup Language – мова розмітка гіпертекстових документів
HTTP	– Hyper Text Transfer Protocol – протокол передачі гіпертекстових документів
IP	– Internet Protocol – протокол мережевого рівня
LDAP	– Lightweight Directory Access Protocol – полегшений протокол доступу до директорій/каталогів
PHP	– Hypertext Preprocessor – мова програмування
SQL	– Structured Query Language – мова програмування для взаємодії користувача з базою даних
SSI	– Server Side Includes – мова для динамічної збірки веб-сторінок
TCP/IP	– набір протоколів мережі інтернет
TLS	– Transport Layer Security – криптографічний протокол
XML	– Extensible Markup Language – розширювана мова розмітки
XSS	– міжсайтовий скриптинг

ВСТУП

Актуальність теми: захист інформації, як відомо — це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам її власника. Основними об'єктами захисту при цьому є:

По-перше, інформація з обмеженим доступом (ІзОД), а саме інформаційні ресурси, що містять відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України і доступ до яких правомірно обмежений власником таких відомостей:

По-друге, технічні засоби приймання, обробки, зберігання та передавання інформації (ТЗПІ), а саме системи та засоби інформатизації (обчислювальна техніка, інформаційно-комунікаційні системи, ІКС), програмні засоби (операційні системи, системи управління базами даних та інше загальне і прикладне програмне забезпечення), автоматизовані системи управління; системи зв'язку, технічні засоби отримання, передання та обробки ІзОД (звукозапис, звукопідсилення, звуковий супровід, переговорні та телевізійні пристрої; засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації, їх інформативні фізичні поля).

По- третє, допоміжні технічні засоби і системи (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де оброблюється ІзОД (технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, систему енергопостачання, радіотрансляційні мережі, системи класифікації тощо, а також самі приміщення, де циркулює ІзОД).

У зв'язку з тим, що весь світ розвивається, та все більше й більше людей отримують можливість використовувати інтернет. Люди можуть набагато легше знаходити певну інформацію, не виходячи з дому, купувати собі речі, спілкуватися. Суспільство все дедалі більше намагається проводити всі можливі маркетингові

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

заходи в інтернеті. Бізнес в цьому питанні, також не відстає. На даний момент, майжекожна більш-менш серйозна організація має свій веб-сайт. Здавалося б, що інтернет, це майже панацея, та це не так. Через те, що інтернет набуває все більшої популярності, та впливу, через нього проходить дуже великі суми фінансових коштів, і було б дивно, якби хтось не захотів їх привласнити собі, незаконним шляхом. Тож разом з розвитком інтернету, розвивається і інтернет-злочинність. На сьогодні, існує досить багато різновидів злочинності в інтернеті, й метою цього дослідження, буде випробувати один з різновидів злочинності в інтернеті. Будуть проводитись захисти ресурсів Web-серверів, використовуючи досить відому CMS «Magento»

Мета і завдання дослідження: мета роботи полягає у використанні веб-ресурсу, над котрим буде проводитися дослідження. Для цього слід виконати наступні завдання:

- 1) Використати сам веб-ресурс за допомогою CMS Magento.
- 2) Захистити цей веб-ресурс
- 3) Описати захист веб-ресурсу.

Виходячи з такого, у роботі об'єктом дослідження є процес захисту веб-сайту, та інформацію, що в ньому зберігається та циркулює. Предмет дослідження — методи і типи атак/захисту на веб-сайти.

Методи дослідження: для вирішення означеного вище наукового завдання в роботі використані CMS Magento та теоретичні навички проведення захисту веб-ресурсів.

Новизна одержаних результатів: новими науково-обґрунтованими результатами, які отримані в роботі, є: обґрунтування вдалого забезпечення безпеки, системою керування контентом Magento v2.2.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Практичне значення одержаних результатів: нові наукові результати, отримані в роботі, у сукупності складають підґрунтя вирішення, чи є CMS Magento v2.2, досить стійкою для того, щоб забезпечити високий рівень захисту інформації, та керування самим сайтом.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ТИПИ АТАК НА ВЕБ-ДОДАТКИ

Проблема з веб-додатками полягає в тому, що вони відкрито піддаються мільярдам інтернет-користувачів, багато з яких захочуть порушити свої заходи безпеки – з будь-яких причин.

У перші дні Інтернету, одним з найбільш поширених методів атак була проста груба сила. Боти зазвичай виконували ці атаки – або люди з великою кількістю вільного часу – які пробували мільйони комбінацій імен користувачів і паролів, поки не знайшли таку, яка надала б доступ до цільового додатку.

Атаки грубою силою більше не є загрозою завдяки політиці паролів, обмеженим спробам входу в систему і капчі. Але кіберзлочинці полюбляють відкривати нові подвиги і використовувати їх для виконання нових типів атак. Давним-давно вони виявили, що текстові поля в додатках або на веб-сторінках можна використовувати, вводячи або вводячи в них несподіваний текст, який змусить додаток робити те, що воно не повинно було робити. Таким чином, на сцену вийшли так звані ін'єкційні атаки.

1.1 Типи атак на веб-додатки

1) Впровадження коду

Впровадження коду є одним з найбільш поширених типів атак. Якщо зловмисники знають мову програмування, структуру, базу даних або операційну систему, використовувану веб-додатком, вони можуть ввести код через поля введення тексту, щоб змусити веб-сервер робити те, що він хоче.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Ці типи ін'єкційних атак можливі для додатків, в яких відсутня перевірка вхідних даних. Якщо поле введення тексту дозволяє користувачам вводити все, що вони хочуть, тоді додаток потенційно може використовуватися. Щоб запобігти цим атакам, додаток повинен максимально обмежити вхідні користувачі.

Наприклад, необхідно обмежити обсяг очікування даних, перевірити формат даних перед його прийняттям і обмежити набір дозволених символів..

Уразливості впровадження коду можна легко знайти, просто протестувавши введення тексту веб-додатку з різними типами контенту. Виявлені уразливості помірно важко використовувати. Але коли зловмисникові вдасться використовувати одну з цих вразливостей, це може привести до втрати конфіденційності, цілісності, доступності або функціональності програми.

2) SQL-ін'єкція

Подібно впровадження коду, ця атака вставляє сценарій SQL - мова, яка використовується більшістю баз даних для виконання операцій запиту - в поле введення тексту. Сценарій відправляється з додатком, яке виконує його безпосередньо у своїй базі даних. В результаті зловмисник може пройти через екран входу в систему або здійснювати більш небезпечні дії, такі як читання конфіденційних даних безпосередньо з бази даних, зміна або знищення даних бази даних або виконання операцій адміністратора в базі даних. Схема атаки SQL-ін'єкції показана на рис. 1.1

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

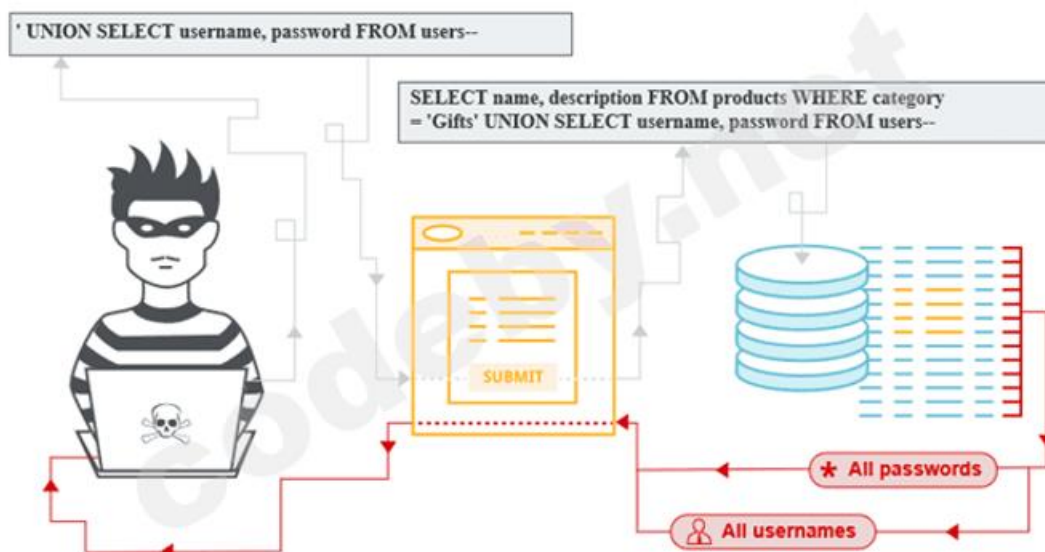


Рис. 1.1 Схема процесу SQL-ін'єкції

Додатки PHP і ASP схильні до атак впровадження SQL через своїх старих функціональних інтерфейсів. Додатки J2EE і ASP.Net зазвичай більш захищені від цих атак. Коли виявляється вразливість SQL-ін'єкції - і їх легко знайти - масштаб потенційних атак буде обмежений тільки умінням і уявою зломисника. Таким чином, вплив атаки SQL-ін'єкції, безсумнівно, є високим.

3) PHP-ін'єкція

PHP-ін'єкція - один із способів злому веб-сайтів, що працюють на PHP. Він полягає в тому, щоб впровадити спеціально сформований зломисний сценарій в код веб-додатку на серверній стороні сайту, що призводить до виконання довільних команд. Схема PHP-ін'єкції наведена нижче, на рис 1.2.

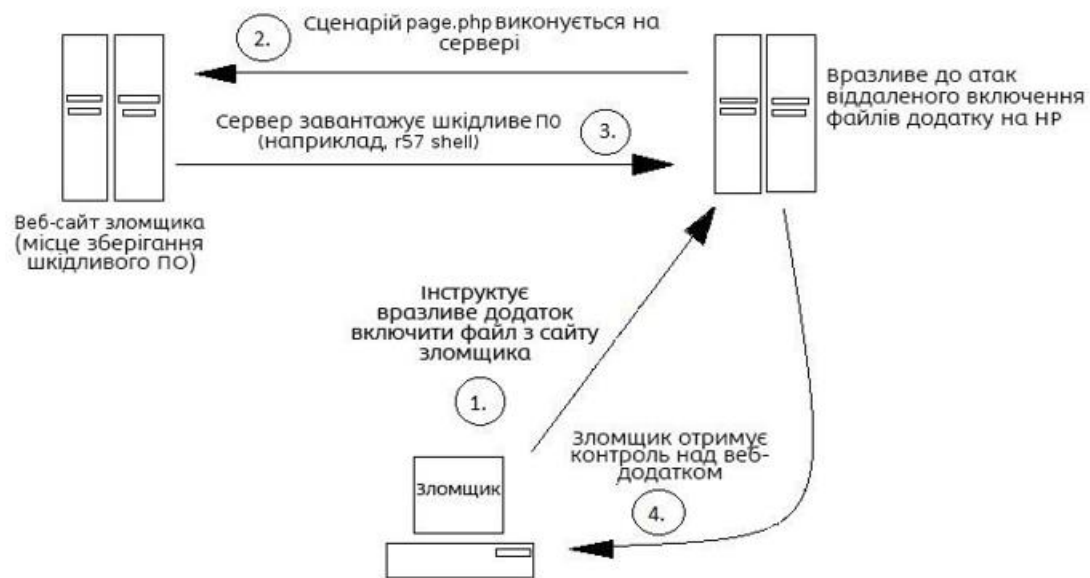


Рис.1.2. Схема RHP-ін'єкції

4) Командна ін'єкція

Ці атаки також можливі, в основному через недостатню перевірки введення. Вони відрізняються від атак впровадження коду тим, що зловмисник вставляє системні команди замість фрагментів програмного коду або сценаріїв. Отже, хакеру не потрібно знати мову програмування, на якому базується додаток, або мова, яка використовується базою даних. Але вони повинні знати операційну систему, використовувану хост-сервером.

Вставлені системні команди виконуються операційною системою хоста з привілеями додатки, які можуть дозволити виставляти вміст довільних файлів, що знаходяться на сервері, показувати структуру каталогів сервера, серед іншого, змінювати паролі користувачів.

Ці атаки можливо запобігти системним адміністратором, шляхом обмеження рівня доступу до системи веб-додатків, що працюють на сервері ..

5) Міжсайтовий скриптинг

Всякий раз, коли додаток вставляє введення від користувача в висновок, який воно генерує, не перевіряючи і не кодуючи його, воно дає зловмиснику можливість відправляти шкідливий код іншому кінцевому користувачу. Атаки з використанням міжсайтових сценаріїв (XSS) використовують ці можливості для впровадження шкідливих сценаріїв в надійні веб-сайти, які в кінцевому підсумку відправляються іншим користувачам додатка, які стають жертвами зловмисника .

Браузер жертви виконає шкідливий скрипт, не знаючи, що йому не можна довіряти. Тому браузер надає йому доступ до токени сеансів, cookie-файлів або конфіденційної інформації, що зберігається в браузері. При правильному програмуванні, сценарії можуть навіть переписати вміст файлу HTML.

Атаки XSS зазвичай можна розділити на дві категорії : збережені і відображені.

В збережених При атаках XSS шкідливий скрипт постійно знаходиться на цільовому сервері, в форумі повідомлень, в базі даних, в журналі відвідувань і т. Д Жертва отримує його, коли браузер запитує збережену інформацію. У відображених В XSS-атаках шкідливий скрипт відбивається у відповіді, що включає вхідні дані, відправлені на сервер. Це може бути повідомлення про помилку або результат пошуку, наприклад.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

6) XPath-ін'єкція

Цей тип атаки можливий, коли веб-додаток використовує інформацію, надану користувачем, для створення запиту XPath для даних XML. Ця атака працює аналогічно SQL-ін'єкції: зловмисники відправляють перекручену інформацію в додаток, щоб дізнатися, як структуровані дані XML, а потім знову атакують, щоб отримати доступ до цих даних.

XPath - це стандартна мова, за допомогою якого, подібно SQL, ви можете вказати атрибути, які ви хочете знайти. Щоб виконати запит до даних XML, веб-додатки використовують для користувача введення для установки шаблону, з яким повинні відповідати дані. Посилаючи некоректний введення, шаблон може перетворитися в операцію, яку зловмисник хоче застосувати до даних ..

На відміну від того, що відбувається з SQL, в XPath немає різних версій. Це означає, що впровадження XPath може бути виконано в будь-якому веб-додатку, що використовує дані XML, незалежно від реалізації. Це також означає, що атака може бути автоматизована; отже, на відміну від SQL-ін'єкції, він може бути запущений проти довільного числа цілей.

7) Впровадження команди Mail

Цей метод атаки може використовуватися для експлуатації поштових серверів і додатків, які створюють оператори IMAP або SMTP з неправильно перевіреним призначенням для користувача введенням. Іноді сервери IMAP і SMTP не мають надійного захисту від атак, як це було б у випадку з більшістю веб-серверів, і тому могли б бути більш уразливими. Входячи через поштовий сервер, зловмисники

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

можуть обійти обмеження, такі як капчи, обмежена кількість запитів і т.д ..

Щоб використовувати SMTP-сервер, зловмисникам потрібна діюча обліковий запис електронної пошти для відправки повідомлень з введеними командами. Якщо сервер уразливий, він буде відповідати на запити зловмисників, дозволяючи їм, наприклад, перевизначати обмеження серверу і використовувати свої служби для розсилки спаму..

Впровадження IMAP може здійснюватися в основному в додатках веб-пошти з використанням функції читання повідомлень. У цих випадках атаку можна виконати, просто ввівши в адресному рядку веб-браузера URL-адресу з введеними командами.

8) CRLF ін'єкція

Вставка символів повернення каретки і переведення рядка - комбінації, відомої як CRLF, - в поля введення веб-форми є метод атаки, званий впровадженням CRLF. Ці невидимі символи вказують на кінець рядка або кінець команди в багатьох традиційних інтернет-протоколах, таких як HTTP, MIME або NNTP.

Наприклад, вставка CRLF в HTTP-запит з наступним певним HTML-кодом може відправляти призначені для користувача веб-сторінки відвідувачам веб-сайту.

Ця атака може бути виконана на вразливих веб-додатках, що не застосовують належну фільтрацію до призначеного для користувача введення. Ця вразливість відкриває двері для інших типів атак з використанням ін'єкцій, таких як XSS і впровадження коду, а також може відбуватися на зламаному веб-сайті.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

9) Впровадження Host Header

На серверах, на яких розміщується безліч веб-сайтів або веб-додатків, заголовок вузла стає необхідним для визначення того, який з резидентних веб-сайтів або веб-додатків, кожне з яких відомо як віртуальний хост, повинен обробляти вхідний запит. Значення заголовка вказує серверу, на який віртуальний хост відправляти запит. Коли сервер отримує неприпустимий заголовок вузла, він зазвичай передає його першого віртуального вузла в списку. Це являє собою вразливість, яку зломисники можуть використовувати для відправки довільних заголовків вузлів на перший віртуальний вузол на сервері ..

Маніпуляції з заголовком вузла зазвичай пов'язані з додатками PHP, хоча це також може бути зроблено за допомогою інших технологій веб-розробки. Атаки на хост-заголовки працюють як активатори для інших типів атак, таких як отруєння веб-кеша. Її наслідки можуть включати виконання чутливих операцій зломисниками, наприклад, скидання пароля.

10) Ін'єкція LDAP

LDAP - це протокол, розроблений для полегшення пошуку ресурсів (пристроїв, файлів, інших користувачів) в мережі. Це дуже корисно для інтрамереж, і коли воно використовується як частина системи єдиного входу, воно може використовуватися для зберігання імен користувачів і паролів. У запитах LDAP використовуються спеціальні керуючі символи, які впливають на його управління. Зломисники можуть змінити передбачуване поведінку запиту LDAP, якщо вони можуть вставити в нього керуючі символи. Схема ін'єкції LDAP показана на рис. 1.3.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

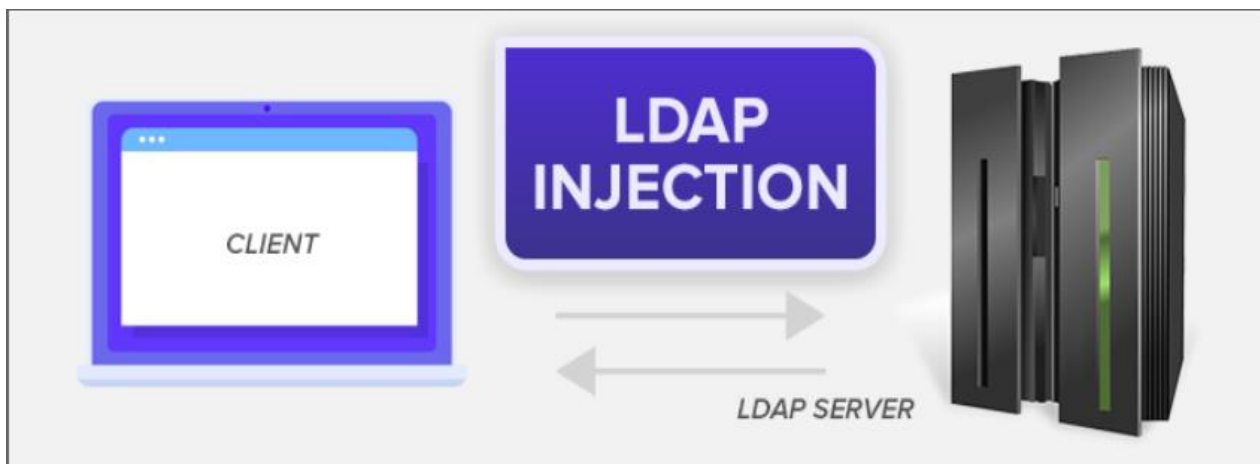


Рис. 1.3. Схема LDAP ін'єкції

Знову ж таки, основною проблемою, яка допускає атаки з використанням LDAP, є неправильно перевірений для користувача введення. Якщо текст, що відправляється користувачем в додаток, використовується як частина запиту LDAP без його очищення, запит може закінчитися отриманням всіх осіб і його відображенням зломисникові, просто використовуючи зірочку (*) праворуч помістити всередині рядка введення.

11) DoS та DDoS атаки

Це зловмисні спроби порушити нормальну роботу цільового сервера, послуги або мережі, переповнивши її потоком інтернет-трафіку.

DoS-атаки досягають цього зриву, надсилаючи зловмисний трафік з однієї машини - зазвичай це комп'ютер. Вони можуть бути дуже простими; базова ping flood attack може бути здійснена шляхом надсилання на цільовий сервер більше ICMP (ping) requests ніж він здатний ефективно обробляти та реагувати на них.

Тим часом DDoS-атаки використовують більше однієї машини для пересилання зловмисного трафіку до своєї цілі. Часто ці машини є частиною botnet - сукупності комп'ютерів чи інших пристроїв, заражених шкідливим програмним забезпеченням, які, таким чином, можуть віддалено контролюватися окремими зловмисниками. В інших обставинах декілька окремих зловмисників запускають DDoS-атаки, працюючи разом надсилаючи трафік зі своїх окремих комп'ютерів.

DDoS-атаки більш поширені та завдають шкоди в сучасному Інтернеті з двох причин:

По-перше, сучасні засоби безпеки розвинулись, щоб зупинити деякі звичайні атаки DoS.

По-друге, засоби атаки DDoS стали порівняно дешевими та простими в експлуатації.

1.2 Приклади веб-атак сьогодні

Переглянемо підсумки минулого року та прогнози на 2021 рік.

1.2.1 Підсумки минулого року

1) Зворотній бік «віддалення».

Перехід на віддалений режим роботи спровокував у всьому світі зростання числа атак, спрямованих на експлуатацію вразливостей в корпоративних сервісах,

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

доступних з інтернету. Адже компанії в терміновому порядку виводили сервіси на периметр. Зросла кількість вузлів російських компаній з доступним для підключення RDP. Як наслідок, частка атак з експлуатацією вразливостей в ПО і недоліків конфігурації ближче до кінця 2020 року зросла до 30% (в I кварталі було 9%). Ще один тренд, що з'явився на тлі пандемії, - атаки, спрямовані на крадіжку облікових даних для підключення до систем аудіо- і відеозв'язку Skype, Webex і Zoom, а також втручання в конференції.

2) «Бум» шифрувальників

Протягом 2020 роки ми спостерігали постійне збільшення числа атак шифрувальників. Якщо в першому кварталі для організацій частка шифрувальників в атаках з використанням ВПО становила 34%, то в третьому кварталі вона досягла 51%. Оператори шифрувальників все рідше проводять масові атаки, вони цілеспрямовано вибирають великі компанії, які в змозі заплатити великий викуп, або організації, для яких припинення діяльності небезпечна, і завдають точкових ударів.

3) Атаки на ланцюжок поставок

Справжнім болем в 2020 році стали supply chain attacks. На практиці спостерігаються атаки на : розробників ПЗ, розробників засобів захисту, на ІТ-інтеграторів, підрядників ІТ-компаній, на портали державних організацій в різних країнах. Рівень захищеності великих компаній підвищується, і їх стає все складніше зламувати, особливо якщо метою зловмисників є довгострокова присутність, а не разова атака. І тому АРТ-угруповання все частіше стали атакувати партнерів

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

і постачальників жертви. Захиститися від подібних атак дуже складно, це під силу тільки висококласним фахівцям в області ІБ.

4) Проблеми промислового сектору як на долоні.

Зростає число атак на промислові та енергетичні компанії. У 2020 році було зафіксовано близько 200 атак на підприємства з цих галузей, що майже на 60% більше, ніж в 2019 році (125 атак). У дев'яти з десяти атак на промисловість зловмисники використовували шкідливе ПЗ. На частку шифрувальників довелося 38% атак, а шпигунське ПЗ було помічено в 30% випадків. На початку року увагу багатьох фахівців з кібербезпеки привернув новий шифрувальник Snake, який вміє видаляти тіньові копії та зупиняти процеси, пов'язані з роботою промислових систем управління. Першими жертвами Snake стали автомобільний виробник Honda і гігант ПЕК - компанія Enel Group. Сьогодні регулярно з'являється інформація про зломи найбільших енергетичних і виробничих компаній по всьому світу. Такі атаки складно приховати.

5) Зловмисники націлилися на логічні уразливості в банківських додатках.

У 2020 році була позитивна динаміка щодо забезпечення безпеки банківських веб-додатків, а саме тенденція до переходу на мікросервісну архітектуру, яка підвищувала відмовостійкість системи, і зменшувала кількість стандартних веб-вразливостей (XSS, SQLi, RCE). З негативних варто відзначити тенденцію до збільшення числа логічних вразливостей, які можуть призвести до крадіжки грошових коштів, отримання злочинцями додаткової інформації про користувачів, відмови в

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

обслуговуванні. Таким чином, зловмисники зараз націлені не на повну компрометацію системи банківського веб-додатки, а на логічну уразливість.

1.2.2 Серед можливих негативних сценаріїв 2021 року експерти відзначають:

1) Експлуатація теми COVID-19 і нові методи фішингу.

Очікується, що в 2021 році будуть удосконалюватися методи соціальної інженерії, які експлуатують теми, пов'язані з обстановкою в світі, зокрема тему COVID-19: наприклад, однією з популярних схем можуть стати сайти, на яких шахраї будуть пропонувати замовити препарати для лікування коронавірусу, записатися на платну вакцинацію, отримати довідку про проходження вакцинації і т.п. Можна очікувати також, що фішинг стане більш індивідуальним, зловмисники будуть виходити на жертв через месенджери і соціальні мережі. Для подолання корпоративних засобів захисту злом все частіше буде проводитися через домашні комп'ютери працівників.

2) Зростання числа кіберзлочинних картелів і поява нових майданчиків в дарквебі

У цьому році ми, ймовірно, побачимо нові об'єднання кіберзлочинців і майданчики для продажу вкрадених даних. Швидше за все, шифрувальники збережуть відпрацьовану в 2020 році стратегію шантажу: запитувати викуп за відновлення працездатності інфраструктури і окремо - за те, щоб злочинці не продали або не опубліковані вкрадені дані.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

3) Інтерес хакерів до великих компаній і зростання розмірів викупу

Злочинці продовжать атакувати промислові підприємства і будуть орієнтуватися на якомога більші організації, в той же час вважаючи за краще дотримуватися найменших витрат на злом або на покупку готового доступу в інфраструктуру. Варто очікувати, що ми почуємо про безліч витоків і про зупинку виробництва і в 2021 році. Швидше за все, підвищиться і розмір викупів, сьогодні в окремих випадках він вже становить десятки мільйонів доларів, але збільшення числа жертв, готових платити, лише стимулює злочинців. Будуть з'являтися і нові групи атакуючих, вони продовжать кооперуватися і заробляти на уразливості промислових організацій.

Масова віддалена робота не могла не позначитися на стані кібербезпеки як бізнесу і держустанов, так і звичайних користувачів. Соціальна інженерія стала часто застосовуватися для проникнення в мережі організацій. Глобальний новинний привід - пандемію - використовували всі типи хакерських угруповань. З темою COVID-19 були пов'язані як масові, так і АРТ-атаки, число яких продовжило рости в 2020 році. При цьому, як відзначають експерти Positive Technologies, пандемія, безсумнівно, сприяла прискореній цифровізації. Поява нових електронних сервісів обов'язково зацікавить злочинців і зажадає особливої уваги з точки зору ІБ. Виходом з цифрового колапсу можуть стати спеціалізовані кіберполігони, створені для тестування об'єктів інфраструктури, сервісів і технологій в безпечному середовищі, вважають експерти.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

1.3 Статистика веб-атак

У I кварталі 2020 році було зафіксовано на 22,5% більше атак, ніж в останньому кварталі 2019 року. Початок року став важким періодом для всього світу. Епідемія коронавірусної інфекції COVID-19 внесла корективи в світову економіку і в життя звичайних людей. Ситуація відбилася і на інформаційну безпеку, як можна побачити на рис. 1.4, 1.5, 1.6, 1.7

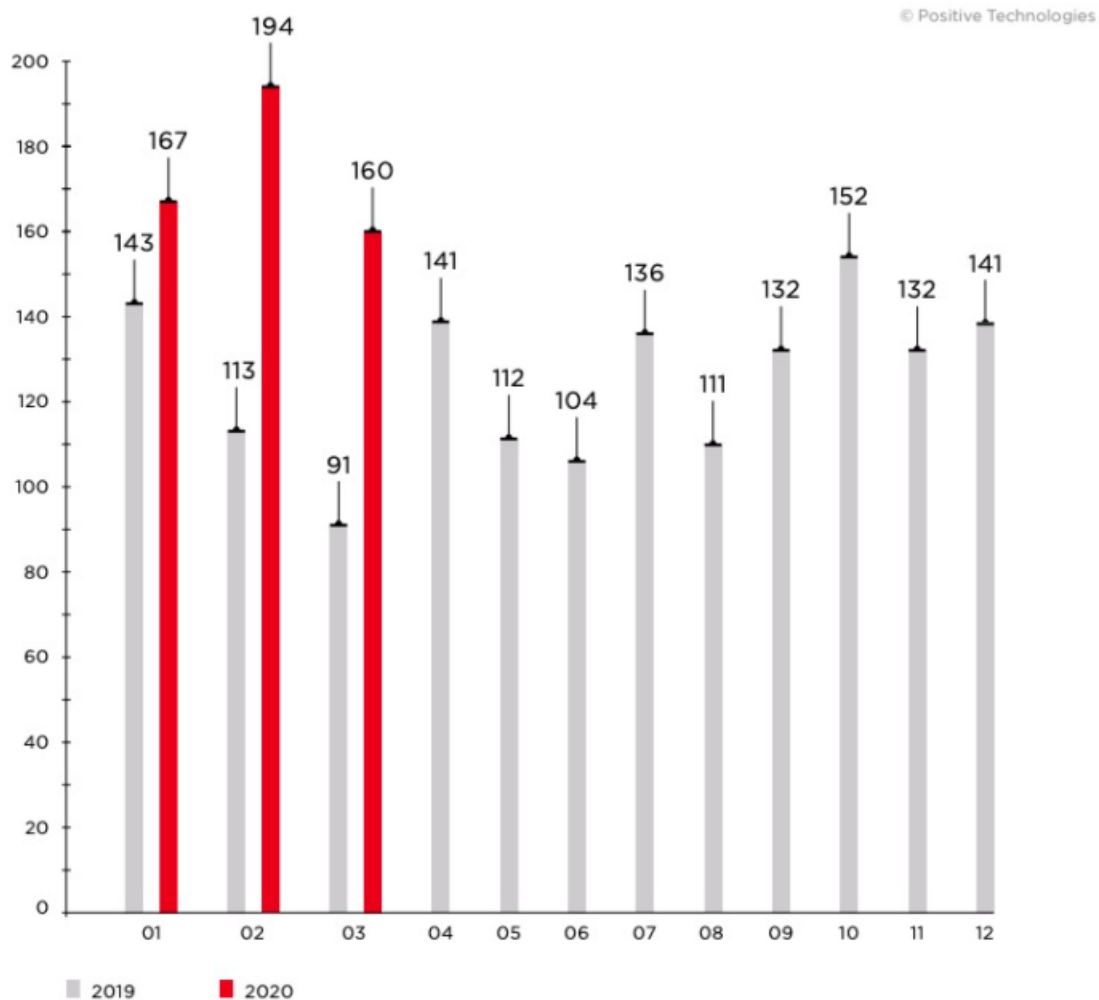


На 22,5%

більше кібератак, ніж в IV кварталі 2019 року

Рис. 1.4 Зміни атак протягом року

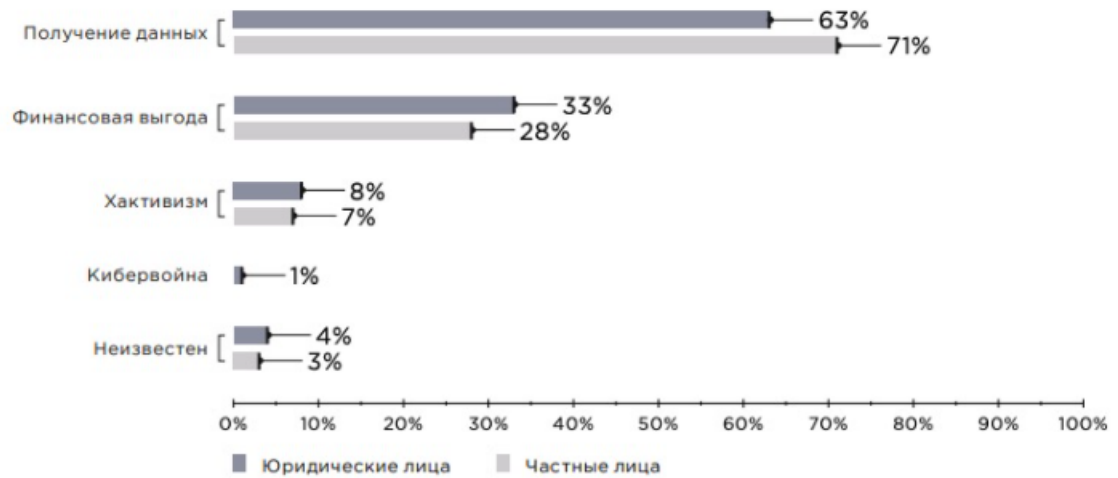
		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24



Малюнок 1. Кількість атак в 2019 і 2020 роках по місяцях

Рис. 1.5 Статистика кількості атак

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25



Малюнок 2. Мотиви зломисників (частка атак)

Рис. 1.6 Статистика мотивів зломисників

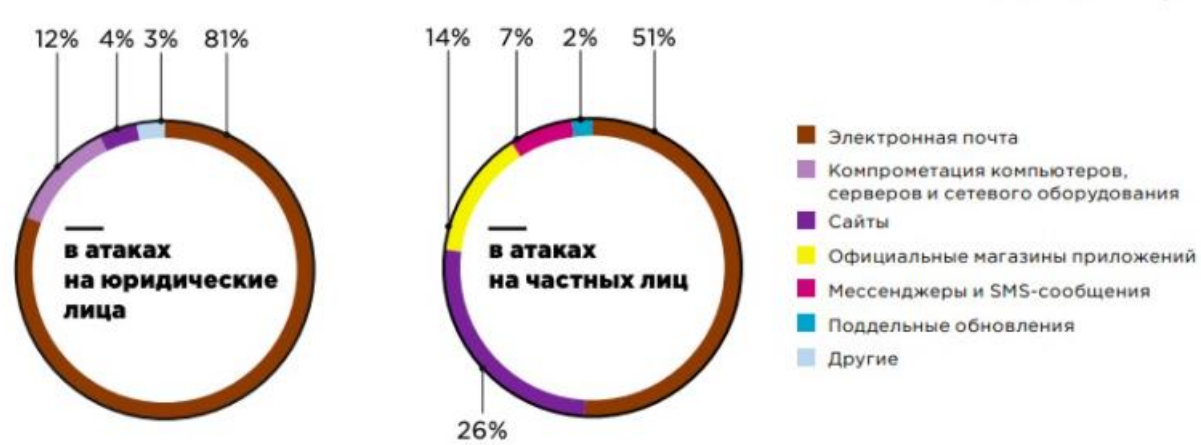


Малюнок 4. Категорії жертв серед юридичних осіб

Рис. 1.7 Статистика жертв серед юридичних осіб

		Кулик Д.А.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

Як і раніше, шкідливі компанії, націлені на організації, у восьми з десяти випадків починалися з розсилки електронних листів із вкладеннями. Для приватних осіб високий ризик заразити комп'ютер не тільки через електронну пошту, але і в результаті відвідування сайтів і завантаження програм з сумнівних веб-ресурсів. Наприклад, в І кварталі зловмисники скомпрометували ряд сайтів на базі WordPress і перенаправляли їх відвідувачів на фішингові сторінки, де під виглядом оновлення браузера Chrome поширювався бекдор. Шкідливе ПО було завантажено більше 2000 разів. На рис. 1.8 можемо побачити статистику способів поширення ВПО.



Малюнок 8. Способи поширення ВПО

Рис. 1.8 Статистика способів поширення ВПО

1.4 Статистика по галузям

1) Держані установи

Починаючи з 18 лютого 2021 року Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони фіксує масовані DDoS атаки на український сегмент Інтернету, переважно на веб-сайти сектору безпеки і оборони.

Зокрема атаки здійснювалися на сайти Служби безпеки України, Ради національної безпеки і оборони України, ресурси інших державних установ та стратегічних підприємств.

Під час атаки вразливі веб-сервери державних органів інфікуються вірусом, який приховано робить їх елементом бот-мережі, що використовується для DDOS-атак на інші ресурси. При цьому системи безпеки інтернет-провайдерів визначають скомпрометовані веб-сервери як джерело атак, та починають блокувати їх роботу шляхом автоматичного внесення до «чорних списків». Таким чином, навіть після закінчення фази DDoS атаківані веб-сайти залишаються недоступними для користувачів.

У порівнянні з останнім кварталом минулого року істотно зросла частка атак на держустанови з використанням ВПО і методів соціальної інженерії. Цьому могла сприяти епідемія. Багато зловмисників розсилали в держустанови різних країн листи з шкідливими вкладеннями на тему коронавірусної інфекції. У січні 2020 року фахівці РТ ESC зафіксували дві атаки АРТ-групи SongXY. В якості приманки зловмисники використовували текст на монгольській мові, що, найімовірніше, говорить про їх вузької регіональної спрямованості. У тексті була інформація про спалах нового вірусу COVID-19 в Китаї. Документ в форматі RTF з експлойтів для уразливості.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

CVE-2018-0798 зберігав на жорсткий диск комп'ютера жертви зашифрований завантажувач, розшифровував, запуслав, після чого було завантажено основний корисного навантаження. Документ-приманку можемо спостерігати на рис. 1.9

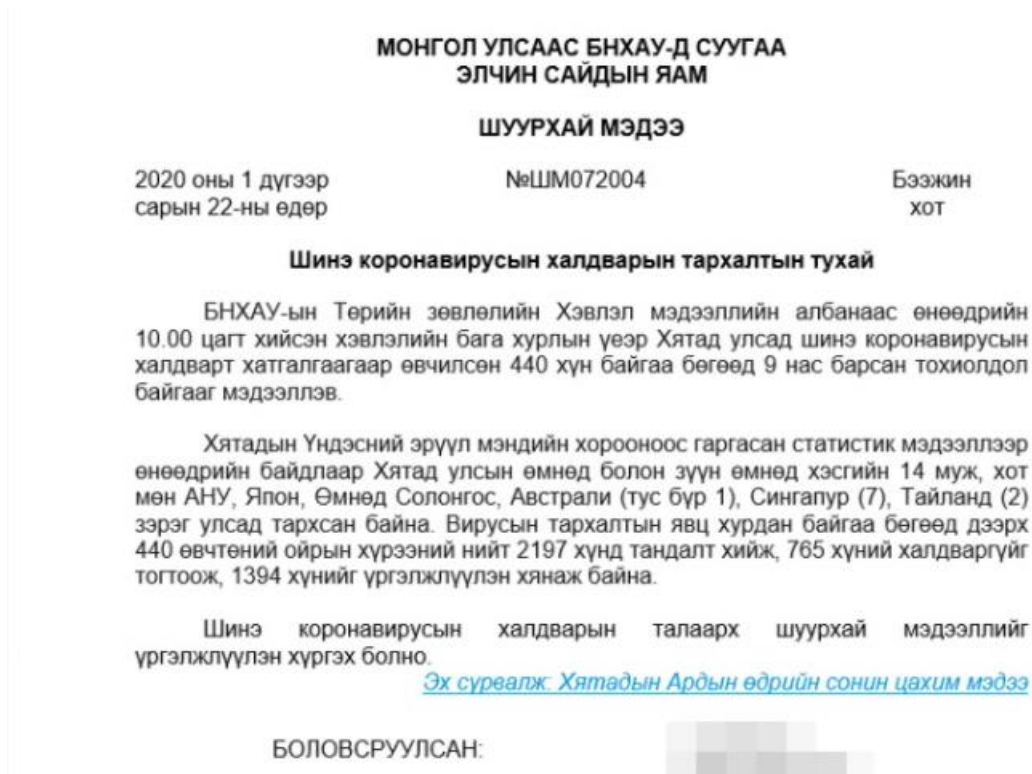


Рис. 1.9. Документ-приманки

		Кулик Д.А.			KI.KP.Б – 123 - 21 - ПЗ	Арх.
		Єфіменко А.А.				
Змн.	Арх.	№ докум.	Підпис	Дата		29

Приклад методів атак на державні установи рис. 1.10

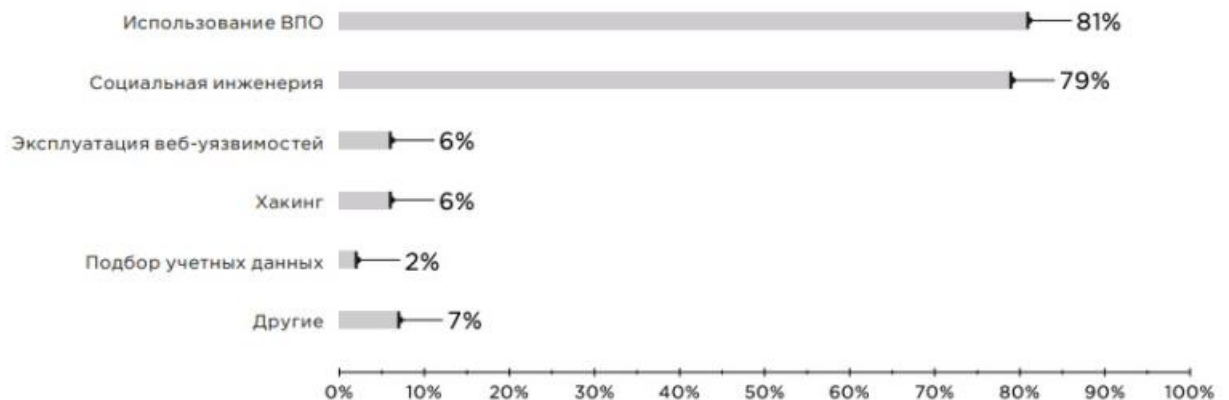


Рис.1.10. Методи атак на державні установи

2) Охорона здоров'я

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України фіксує активне зростання "фішингових" атак з використанням теми вакцинації проти COVID-19 в Україні.

Під час атаки на популярній хостинговій платформі було створено фейкову веб-сторінку, що імітувала сайт Міністерства охорони здоров'я України. Для розміщення сторінки атакуючі зареєстрували кілька доменів, які нагадували офіційний домен МОЗ України. На цій фейковій сторінці було розміщено інформацію щодо початку з 25 січня обов'язкової вакцинації від COVID-19 із пропозицією завантажити файл (документ Word) із подробицями. У цей документ було вбудовано шкідливий код (макрос), який при відкритті файлу приховано від користувача завантажує та виконує

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

інший шкідливий скрипт, що забезпечує віддалене управління зараженим комп'ютером. Таким чином, атакуючі отримували повний доступ до комп'ютера жертви. Схема атаки продемонстрована на рис. 1.11.

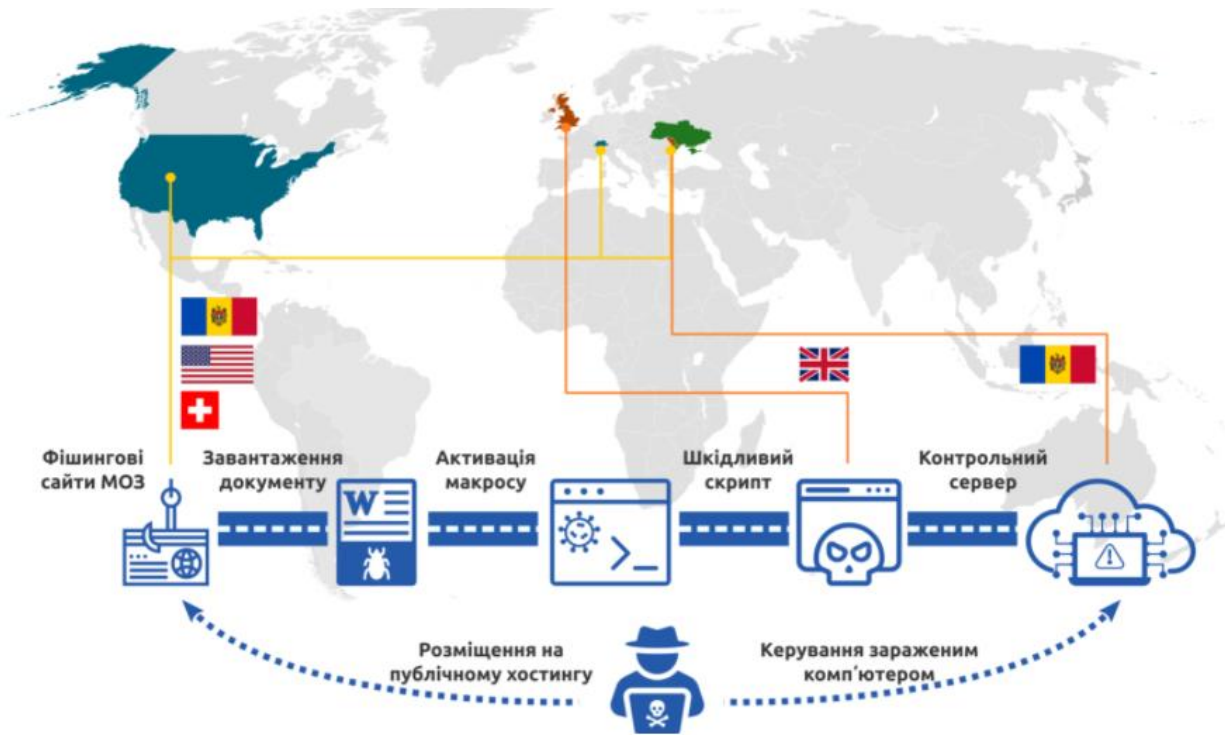


Рис. 1.11. Схема атаки

3) Веб-атаки на освіту України

У другому півріччі в сфері освіти переважали атаки, спрямовані на отримання контролю над веб-додатком або сервером і на отримання даних, зокрема «Віддалене виконання коду і команд ОС», «Вихід за межі призначеного каталогу», «SQL-ін'єкція». Атакуючими, є найчастіше самі учні, які прагнуть поліпшити таким

способом свою успішність. Вже стають відомі випадки злому електронних щоденників з цією метою, наприклад інцидент в школі Києва, коли школяр протягом місяця виправляв оцінки собі та однокласникам. На результати, отримані в першому кварталі, ймовірно, вплинув невеликий обсяг вибірки. Найбільш популярні атаки на веб-додатки в сфері освіти можна побачити на рис. 1.12.



Рис 1.12. Топ-5 атак на веб-додатки в сфері освіти

Атака на корпоративну мережу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

19.10.2020 року з 9 години ранку розпочалась масована розподілена атака типу «відмова в обслуговуванні» (DDoS) на корпоративну мережу університету. Першим об'єктом атаки були серверні системи електронного кампусу. Атака виконувалась зі світового сегменту Інтернет. Кількість Інтернет-вузлів, які були задіяні в атаці, становила 74063 вузли. В результаті вхідні ємності зовнішніх каналів університету в світовий Інтернет були повністю завантажені «паразитними» запитами (запити направлялися в зовнішні канали університету на сумарній швидкості до 20 Гб/с). Після визначення об'єкту атаки технічним персоналом НТО «КПІ-Телеком» та побудови відповідних фільтрів атаку було призупинено. Але, в 12-40 почалась чергова хвиля

атаки вже на інші об'єкти (ряд хостингових серверів університету, сервер аудіо-відео конференцій). В районі 17 години 19.10.20 атака розпочалась на центральний маршрутизатор університету, що призвело на деякий час до повного призупинення усіх інтернет-послуг. Ряд проведених НТО «КП-Телеком» контрзаходів дозволило дещо стабілізувати ситуацію. Було відновлено доступ до українського сегменту мережі Інтернет, вночі вдалося запустити канали доступу у світовий Інтернет, хоча кількість атакуючих вузлів вночі 20.10.20 р. досягла 189259 одиниць. З 8-ї години ранку 20.10.20 р. розпочалась чергова хвиля атак. Нажаль, існуючі засоби захисти від подібних атак не є достатньо ефективними - їх можна застосовувати тільки постфактум – після початку атаки, шляхом визначення об'єкту атаки та його блокування. В результаті реакція на атаку завжди є запізнілою. Недоліком можливих контрзаходів є також те, що повністю блокується доступ до вузлів, які є об'єктом атаки.

4) Фінанси

Банки незмінно залишаються однією з головних цілей атак зловмисників. На щастя, фінансові організації це чудово розуміють і не хочуть втрачати ні клієнтів, ні гроші через кібератаки. Для мінімізації ризиків компанії самотійно або із залученням сторонніх експертів проводять аналіз захищеності використовуваних систем дистанційного банківського обслуговування (ДБО). Це дозволяє виявити уразливості загальнодоступних веб-і мобільних додатків і вжити необхідних заходів для їх усунення.

В цьому році фінансові програми, побудовані на готових вендорських рішеннях, містили менше критично небезпечних вразливостей, ніж ті, що банки розробили самотійно. Це говорить про те, що вендори стали більше уваги приділяти питанням безпеки, в той час як банкам як і раніше не вистачає в штаті досвідчених розробників

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

і грамотно вибудованого процесу безпечної розробки. Рівень ризику виявлених вразливостей знизився, як показано на рис. 1.13.

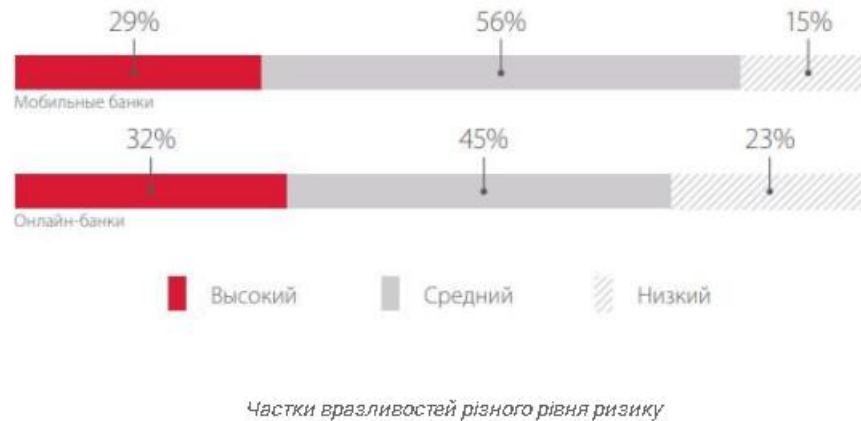


Рис. 1.13 Статистика рівню ризику банки

1.5 Статистика атак на веб-додатки

Рівень захищеності веб-додатків продовжує поступово зростати, але все ще залишається досить низьким.

У 9 з 10 веб-додатків злочинці можуть проводити атаки на користувачів. У тому числі - перенаправляти клієнтів на підконтрольний їм ресурс, викрадати облікові дані за допомогою фішингових атак, заражати комп'ютер шкідливим ПЗ.

Несанкціонований доступ до додатка можливий на 39% сайтів. Крім того, в 2020 році повний контроль над системою був отриманий в 16% веб-додатків, а в 8% систем повний контроль над сервером веб-додатки дозволяв проводити атаки на локальну мережу організації.

82% вразливостей містилися в коді програми. Число вразливостей, яке в середньому припадає на одне веб-додаток, знизлося в порівнянні з 2018 роком в півтора рази. В середньому на одну систему припадають 22 уразливості, чотири з яких мають високий рівень ризику. Кожна п'ята вразливість - високого рівня ризику.

1.5.1 Тенденції

У 2019 році значно (на 17 процентних пунктів у порівнянні з 2018 роком) знизилася частка веб-додатків, що містять уразливості високого рівня ризику. Число критично небезпечних вразливостей, яке в середньому припадає на один додаток, знизлося в порівнянні з минулим роком майже в півтора рази. Це ми можемо спостерігати на рис. 1.14.

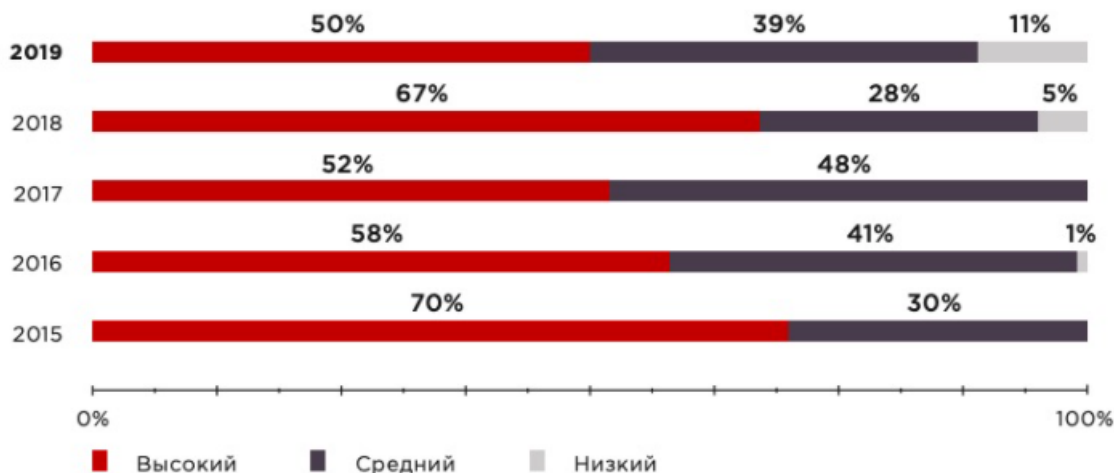


Рис. 1.14. Статистика вразливих додатків

Аналізуючи дані за останні п'ять років, ми бачимо закономірне зниження частки додатків, що містять критично небезпечні веб-вразливості, і, відповідно, загальне підвищення рівня захищеності, про це свідчить рис. 1.15.

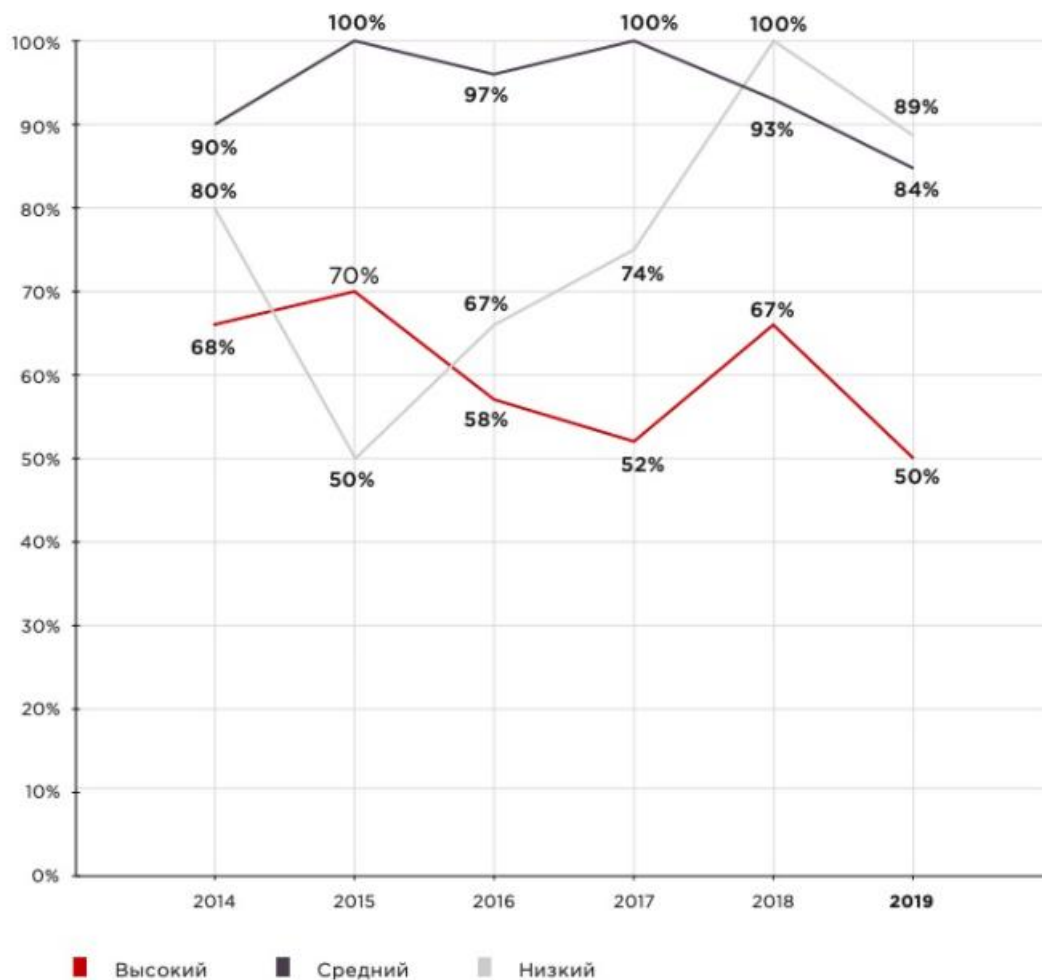


Рис. 1.15. Статистика вразливих додатків

1.5.2 Аналіз захищеності веб-додатків

81% - частка вразливостей коду в веб-додатках, згідно статистики, яка також проілюстрована на рис. 1.16 та на рис. 1.17

		Кулик Д.А.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІ.КР.Б – 123 - 21 - ПЗ

Арк.

36

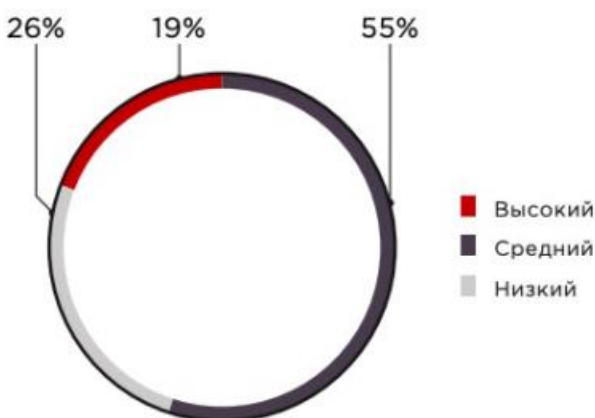


Рис. 1.16 Частка вразливостей різного ступеня

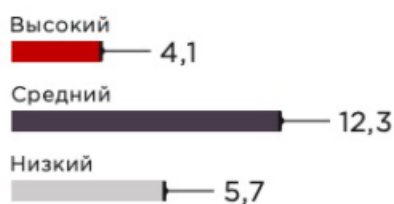


Рис. 1.17 Середнє число вразливостей на одну систему

1.5.3 Поширені уразливості

Частіше за всіх інших в 2019 році в веб-додатках зустрічалися уразливості, пов'язані з некоректними параметрами безпеки (Security Misconfiguration). Так, в кожному п'ятому проаналізованому додатку були виявлені вразливості, що дозволяють проводити атаку на сесію, зокрема відсутність прапорів HttpOnly і Secure у конфіденційних Cookie-параметрів. За допомогою даних недоліків зловмисник може, наприклад, провести атаку типу «міжсайтовий виконання сценаріїв» (Cross-Site Scripting, XSS), щоб перехопити ідентифікатор сесії користувача і від його імені виконувати різні дії в додатку.

У 45% веб-додатків були виявлені недоліки аутентифікації (Broken Authentication). Майже третина виявлених вразливостей з цієї категорії - це некоректне обмеження кількості невдалих спроб аутентифікації. В результаті експлуатації цієї уразливості зловмисник може підібрати облікові дані користувача і таким чином отримати доступ до веб-додатку. Так, наприклад, для однієї програми треба було всього 100 спроб, щоб успішно увійти з правами адміністратора. Ілюстрації щодо цих вразливостей можна побачити на рис. 1.18.

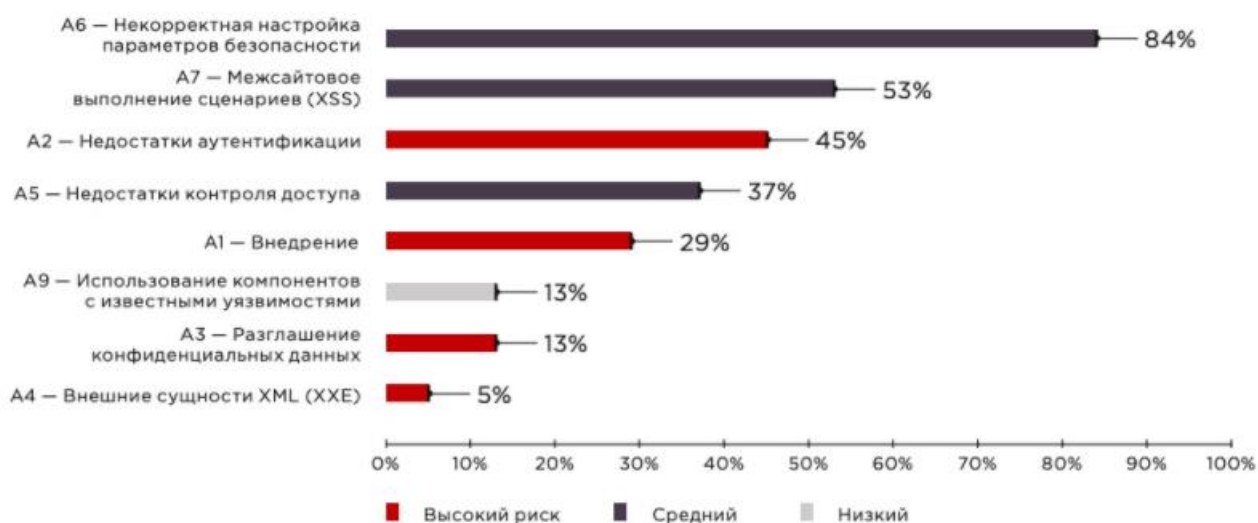


Рис. 1.18 Уразливості топ-10

Більшість атак на аутентифікацію пов'язано з використанням виключно паролів. Раніше вважалися хорошими вимоги до зміни пароля і його складності сприяють використанню ненадійних паролів користувачами. Згідно з останніми рекомендаціями NIST, організаціям слід застосовувати багатофакторну аутентифікацію. Демонстрація на рис. 1.19

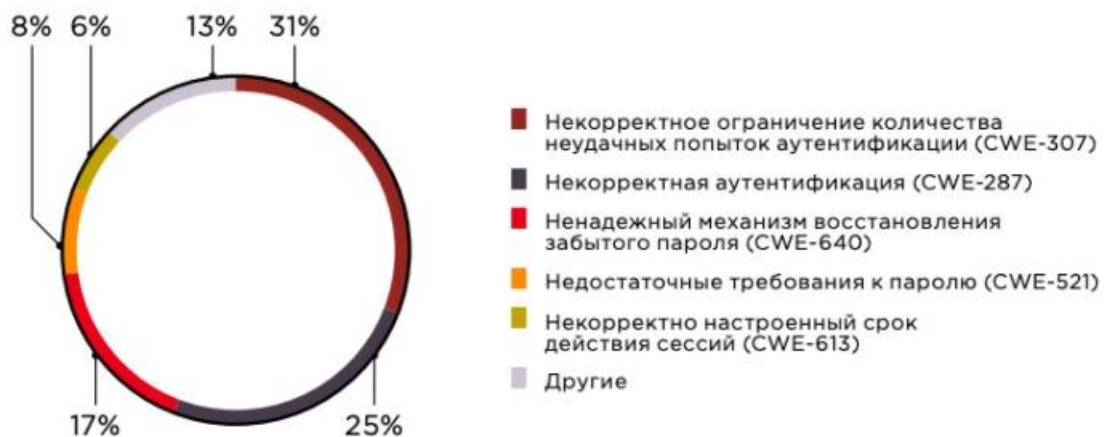


Рис. 1.19 Уязвимості, пов'язані з недоліками аутентифікації

Недоліки контролю доступу (Broken Access Control) в 2019 році зустрічалися в кожному третьому додатку. Обхід обмежень доступу зазвичай призводить до несанкціонованого розголошення, зміни або знищення даних. Так, наприклад, в одному з проектів небезпечно авторизація дозволяла змінювати вміст профілю будь-якого користувача. Фахівці Positive Technologies дізналися логін адміністратора додатку, в його профілі змінили адресу електронної пошти на власний, а потім через стандартну процедуру відновлення пароля отримали доступ до сайту з правами адміністратора.

Кількість вразливостей, пов'язаних з аутентифікацією і авторизацією, як правило, можна мінімізувати, якщо при розробці веб-додатки дотримуватися практик безпечного програмування SSDLC.

Крім вразливостей зі списку Top 10-2019, співтовариство OWASP виділяє ряд недоліків, наявність яких рекомендується перевіряти. Третина веб-додатків виявилися вразливими для атаки типу Clickjacking (містили вразливість «Некоректне уявлення важливої інформації інтерфейсом користувача», CWE-451) і стільки ж для атаки «Підробка міжсайтового запиту» (Cross-Site Request Forgery, CSRF).

В ході CSRF-атаки зломисник за допомогою спеціально сформованих сценаріїв може виконувати дії від імені користувача, авторизованого в уразливому веб-додатку. Уявімо ситуацію: ви авторизовані на сайті, уразливому для підробки міжсайтового запиту (нехай це буде якийсь онлайн-банк). У цей час вам приходить фішинговий лист з посиланням, і ви по ній переходите. А далі від вашого імені на уразливий сайт (в ваш онлайн-банк) відправляється спеціально сформований хакером запит, який виконує потрібні зломисникові дії (наприклад, переводить гроші на його рахунок). Онлайн-банк не зможе відрізнити цей несанкціонований запит від легітимних, якщо не використовується захист від CSRF-атак. Захист від даного типу атак найчастіше ґрунтується на використанні унікальних одноразових ключів (CSRF-токенів), підтвердження справжності (наприклад, за допомогою пароля) або доказі, що запит виконується реальним користувачем (наприклад, за допомогою CAPTCHA), на встановлення додаткового прапора SameSite для Cookie-параметрів.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Висновки до першого розділу

Проаналізовано найпоширеніші веб-атаки, та розглянуто вразливості, які можуть бути використанні для проведення цих атак.

Досліджено веб-атаки та уразливості які можуть використовуватись для реалізації цих атак, також були розглянуті статистичні дані, щодо веб-атак які відбулися в наслідок епідемії COVID-19, які наслідки були в результаті проведених злочинних дій та які сфери найбільш привабливі для веб-злочинців.

Також, було наголошено на тому, що необхідно бути досить уважним до деталей веб-додатку, адже кожна маленька вразливість може призвести до великих втрат.

Підсумовуючи вищесказане, можна сказати, що для забезпечення максимального захисту веб-додатків, слід проводити аналіз захищеності, включаючи аналіз вихідного коду, на всіх стадіях розробки, а також після введення в експлуатацію, з метою виявлення актуальних вразливостей. Крім цього, важливо регулярно оновлювати програмні компоненти веб-додатків. Проте і цих заходів захисту може виявитись недостатньо, оскільки зловмисники уважно стежать за публікаціями про нові вразливості і намагаються експлуатувати їх в найкоротший час.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

РОЗДІЛ 2. АНАЛІЗ РЯДУ СПОСОБІВ ЗАХИСТУ ВІД ВЕБ-АТАК

В попередньому розділі ми дослідили веб-атаки та як вони відбуваються. Тож в другому розділі досліджуються можливі способи захисту від них.

2.1 Захист від веб-атак

1) DoS / DDoS

Оскільки атаки DoS та DDoS приймають різноманітні форми, для їх пом'якшення потрібні різноманітні тактики. Загальна тактика зупинки DDoS-атак включає:

- Обмеження швидкості: Обмеження кількості запитів, яку сервер прийме протягом певного періоду часу
- Брандмауери веб-додатків: засоби, що фільтрують веб-трафік на основі ряду правил
- Дифузія мережі Anycast: розміщення великої розподіленої хмарної мережі між сервером та вхідним трафіком, забезпечуючи додаткові обчислювальні ресурси, за допомогою яких можна відповідати на запити.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

2) Host Header

Щоб запобігти атакам заголовків хостів HTTP, найпростішим підходом є уникнення використання заголовка хосту в коді на стороні сервера. Перевірте, чи дійсно кожна URL-адреса є абсолютною. Часто виявляється, що замість цього ви можете просто використати відносну URL-адресу. Ця проста зміна може допомогти вам запобігти отруєнню вразливостей веб-кешу .

Інші способи запобігання атакам заголовків хосту включають :

- Захист абсолютних URL-адрес

Коли потрібно використовувати абсолютні URL-адреси, вам слід вимагати, щоб поточний домен був вказаний вручну у файлі конфігурації та посилався на це значення замість заголовка Host. Наприклад, такий підхід усуне загрозу отруєння скидання пароля.

- Перевірка заголовку хосту

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Якщо потрібно використовувати заголовок Host, потрібно переконатися, що його правильно перевірено. Це повинно включати перевірку з білого списку дозволених доменів та відхилення або перенаправлення будь-яких запитів на нерозпізнані хост. Слід ознайомитися з документацією фреймворку, щоб отримати вказівки щодо того, як це зробити. Наприклад, фреймворк Django надає ALLOWED_HOSTS опцію у файлі налаштувань. Цей підхід зменшить ваш вплив на атаки введення заголовка хосту.

- Не підтримує заголовки заміни хосту

Важливо також перевірити, чи не підтримуєте ви додаткові заголовки, які можуть бути використані для побудови цих атак, зокрема X-Forwarded-Host. Пам'ятайте, що вони можуть підтримуватися за замовчуванням.

- Білий список дозволених доменів

Щоб запобігти атакам на внутрішню інфраструктуру на основі маршрутизації, слід налаштувати балансування навантаження або будь-які зворотні проксі-сервери для пересилання запитів лише до білого списку дозволених доменів.

- Будьте обережні з внутрішніми віртуальними хостами

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Використовуючи віртуальний хостинг, слід уникати розміщення лише внутрішніх веб-сайтів та програм на тому ж сервері, що і загальнодоступний вміст. В іншому випадку зломисники можуть отримати доступ до внутрішніх доменів за допомогою маніпуляції заголовком хосту.

3) CRLF

Кращий метод запобігання - це не використовувати введення даних користувачем безпосередньо в заголовок відповіді. Якщо це неможливо, ви завжди повинні використовувати функцію для кодування спеціальних символів CRLF. Ще одна хороша практика безпеки - це оновлення мови програмування до версії, яка не дозволяє робити ін'єкції CR і LF всередині функцій, які встановлюють HTTP-заголовки.

4) XPath

Кращий шлях - перевірка всіх отриманих від користувача даних на неправильні символи і слова. Найбільш оптимально створити список дозволених символів, наприклад, для введення номера кредитної карти це будуть цифри від 0 до 9, для, наприклад, імен - тільки літери.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Другий спосіб - параметризація запитів. Замість того, що б збирати рядок запиту в додатку на льоту, динамічно, доцільніше створити прокомпельований запит і вже передавати змінні не виразами, а параметрами.

5) SQL

Як захистити сайт від SQL-ін'єкції?

- Використати білі списки, приклад :

```
$ Keys = "";
```

```
$ Values = "";
```

```
$ First = 1;
```

```
$ Allowed = array ( "login", "password", "email", "nickname");
```

```
foreach ($ _ POST as $ key => $ array) {
```

```
$ AllowedKey = array_search ($ key, $ allowed);
```

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

```

if ($ allowedKey) {

    if ($ first == 0) {

        $ Keys. = ",";

        $ Values. = ",";

    }

    $ Keys. = $ AllowedKey;

    $ Values. = " ". $ Value. "";

$ First = 0;

}

}

```

Тепер в змінні *\$ key* і *\$ values* потраплять тільки ті значення, які входять в білий список *\$ allowed* .

- Не використовуйте методом GET в формах

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Передавати змінні цим способом дуже небезпечно, тому що вони кидаються в очі у користувачів. Якщо інформація важлива, то краще використовуйте POST. З посилення зловмисник може дізнатися не тільки імена змінних, а й які значення повинні бути в них - так він зможе вибрати оптимальну змінну для введення ін'єкції.

Не потрібно використовувати змінні прямо з супермасиву – краще помістити їх в іншу змінну, попередньо перевіривши дані.

- Перевіряйте, звідки прийшли дані

Недостатньо просто обробити дані - потрібно дізнатися, звідки вони прийшли. Відстежити джерело можна декількома способами:

- перевіряти його в `$ _SERVER [ 'HTTP_REFERER' ]` ;
- створити приховане поле в формі;
- вказати ім'я форми;
- вказати ім'я кнопки відправки і так далі.

Звичайно, це лише незначний бонус до захисту, але зате він відсіває частина недосвідчених зломщиків, які кинуть свої потуги після кількох спроб.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

- Використовуйте PDO

За допомогою PDO і плейсхолдерів можна значно знизити ризик ін'єкції, тому що дані і запит відправляються окремо. Спочатку проводиться підключення до бази, потім готується запит, потім окремо вказуються змінні, і, нарешті, запит виконується. Виглядає це так:

```
$ Db = new PDO ( 'mysql: host = localhost; dbname = test', $ user, $ pass);
```

```
$ Stmt = $ db-> prepare ( "SELECT * FROM articles WHERE id = ': id'");
```

```
$ Stmt-> bindParam ( ': id', $ id);
```

```
$ Stmt-> execute ();
```

Дані відправляються вже в вигляді змінних. Тобто якби в змінної хтось поставив зайву лапки, сервер б не подумав, що вона - частина запиту. Тому спроба зіпсувати запит через змінну не спрацювала б.

Цей спосіб, мабуть, ефективніше інших, тому переходите на PDO якомога швидше. Хоча його використання не означає, що інші заходи безпеки вже не потрібні - чим більше захисних механізмів ви встановите, тим захищена буде інформація.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Часто перевірки нехтують самоучки, які вивчають теми «по верхівках», - вони можуть вирішити задачу, але рідко замислюються про те, щоб усунути уразливості. Тому ми пропонуємо курс з системним навчанням - ви навчитеся створювати ефективні та надійні системи, яким не будуть страшні ін'єкції і витоку даних.

6) PHP

Ця атака полягає в тому, що зломисник вставляє зловмисний PHP-код в сайт. Способи боротьби з цією атакою (використовуються виключно адміністраторами ресурсів):

Перевіряти, чи не містить змінна *\$name* (в нашому прикладі) сторонні символи:

```
<?
```

```
$name = $_GET['name'];
```

```
if (strpos($name, '?:/')) die('Blocked');
```

```
... ?>
```

Перевіряти, що *\$name* присвоєно одне з допустимих значень:

```
<?
```

	..	Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

```
$name = $_GET['name'];
```

```
$arr = array('main', 'about', 'links', 'forum'); if (!in_array($name,$arr)) $name = $arr[0];
```

```
...
```

```
?>
```

7) Міжсайтовий скриптинг (XSS)

Топ-8 захистів від XSS уразливостей :

- Захист функцією htmlspecialchars ()

Ця функція перетворює переданий їй аргумент в HTML-суті, причому відбувається перетворення саме тих символів, які є потенційно небезпечними.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

- Захист функцією strip_tags ()

На відміну від htmlspecialchars () дана функція видаляє з рядка аргументу тільки самі теги, причому другий аргумент служить для вказівки винятків, які не потрібно видаляти. Через неї спокійно проходять рядки: <,>, <img.

- Заборонити включення безпосередньо параметрів \$ _GET, \$ _POST, \$ _COOKIE в HTML-сторінці що генерується.

- Заборонити завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів.

- Всі завантаженні файли зберігати в базі даних, а не в файловій системі.

- ВВ-коди

Пропуск тільки певних тегів, іноді зовсім в іншій формі, ніж дозволяють стандарти HTML.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

- Регулярні вирази

Хтось регулярні вирази любить, хтось ні, а хтось навіть вважає за краще написати свою власну, через яку не проходять потенційно небезпечні символи або теги. Зручно у разі виключення аргументів з впроваджуваного тегу без зміни HTML-суті решти.

- Самописні функції

Всілякі рекурсивні парсери рядків, які дуже гнучко борються з XSS, також досить популярні. Хоча в самописних функціях набагато частіше можна знайти будь-яку вразливість.

2.2 Захист веб-ресурсу

Щодо захисту від веб-атак ми розглянули раніше, але цього недостатньо, тому є кілька порад, для зменшення ризику взлому.

Передовсім, щоб захистити веб-ресурс, потрібно використовувати інструменти для пошуку вразливостей. Ось перелік деяких інструментів :

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Інструментів пошуку вразливостей досить багато. Є комерційні продукти: Acunetix, Nessus Scanner, Nexpose, але є і безкоштовні пробні версії з обмеженим функціоналом. А є і повністю безкоштовні: Wapiti , Nikto , Vega , SQLmap .

З комерційними продуктами все в основному просто і зрозуміло. Вони розробляються для максимальної функціональності і зручності користувачів. Як правило, при їх використанні від користувача практично ніяких дій не потрібно - все відбувається автоматично, варто лише вказати мету сканування. З повністю безкоштовними рішеннями справа йде трохи інакше. Вони самі по собі вимагають від користувача участі протягом усього процесу сканування і до того ж багато з них часто бувають вузькоспеціалізованими, що не дозволяють охопити весь спектр вразливостей для їх пошуку.

Засоби пошуку вразливостей в основному працюють за принципом відправки спеціально складених запитів до веб-додатку і аналізу відповідей від нього, після чого приймається рішення про наявність чи відсутність уразливості. Але досить часто веб-додатки використовують Web Application Firewall - популярний інструмент для протидії атакам. Як правило, він дозволяє блокувати все вищеописане.

Різні WAF використовують і різні алгоритми виявлення і блокування атак. Проте, знаючи, який інструмент захищає веб-додаток, зловмисник може спробувати обійти обмежувальні правила для подальшої експлуатації вразливостей. А щоб перед цим дізнатися який для захисту веб-додатки використовується WAF можна використовувати інструмент Wafw00f .

Підводячи підсумки, варто зазначити, що як і раніше загальний рівень захищеності веб-додатків залишається низьким. У кожній програмі присутні недоліки різного ступеня небезпеки. Зловмисники можуть експлуатувати критично небезпечні уразливості більш ніж в половині додатків, отримуючи доступ до чутливих даними, можливість виконання команд на сервері і повний контроль над системою.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Успішні атаки можуть проводитися щодо підприємств з різних сфер економіки, від інтернет-магазинів до державних підприємств. Частка додатків, в яких кінцеві користувачі не потрапляють під загрозу, становить всього 4%. При цьому в результаті атаки на веб-додаток в кожному четвертому випадку зловмисник може отримати персональні дані, які самі по собі представляють високу цінність.

Питанням безпеки як і раніше приділяється недостатня увага, щорічно ми спостерігаємо одні й ті ж помилки, що здійснюються розробниками та адміністраторами систем, а питання впровадження процесів забезпечення безпеки протягом усього життєвого циклу веб-додатків як і раніше залишається невирішеним.

2.3 Порівняння захисту в Україні за період

Фахівці Держспецзв'язку з 26 травня по 1 червня 2021 року заблокували 44,9 тис. кібератак на державні інформаційні ресурси.

Системою захищеного доступу державних органів до мереж Інтернет:

- Заблоковано 44 900 різних видів атак, що на 2% більше ніж попереднього тижня. Переважна більшість – мережеві атаки прикладного рівня (98%)
- Зафіксовано і заблоковано 10 DDoS-атак.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки на об'єктах моніторингу зафіксовано 625 361 підозрілу подій (на 38% менше ніж попереднього тижня):

- спроб отримання прав користувача – 46%
- спроб отримання прав адміністратора – 20%
- порушень корпоративної політики безпеки – 14%
- підозрілого виконувального коду – 7%
- застосування нестандартних протоколів – 7%

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Про це свідчить наступна статистика, рис. 2.1



Рис. 2.1 Порівняння за період

2.4 Порівняння тестових і продуктивних систем

Спостерігається збільшення частки продуктивних систем, що містять уразливості високого рівня ризику, майже в три рази (з 25% у 2020 році до 71% в 2021- м). Крім того, в кілька разів зросла і середня кількість вразливостей в одному веб-додатку; це відноситься як до тестових, так і до продуктивних систем. Статистику з приводу цього можна побачити на рис.2.2. та рис.2.3.

Порівняння методів тестування. Порівняння методів тестування щороку підтверджує більш високу ефективність аналізу веб-додатків методом білого ящика. Наприклад, при наявності доступу дослідників до вихідного коду число критично небезпечних вразливостей, виявлених в одній системі, істотно більше, ніж при тестуванні методами сірого і чорного ящика. Зокрема, число виявлених вразливостей впровадження коду (A1 - Injection) при тестуванні методом білого ящика зростає в 3 рази. Статистику з приводу методів тестування можна побачити на рис. 2.2, рис. 2.3



Рис. 2.2. Частка систем по максимальному рівню



Рис. 2.3. Середня кількість вразливостей на одну систему

Якщо на сайті є сторінки, які доступні тільки після аутентифікації, спробуйте видати себе за іншого користувача.

Також слід зауважити, що веб-ресурси зроблені спеціалістами з нуля, зламати важче, ніж сайти зроблені на відомих двигунах, CMS (Wordpress, Magento, Joomla). Так як всі вразливості які є в певній системі керування контентом (CMS) властиві всім веб-ресурсам, які її використовують.

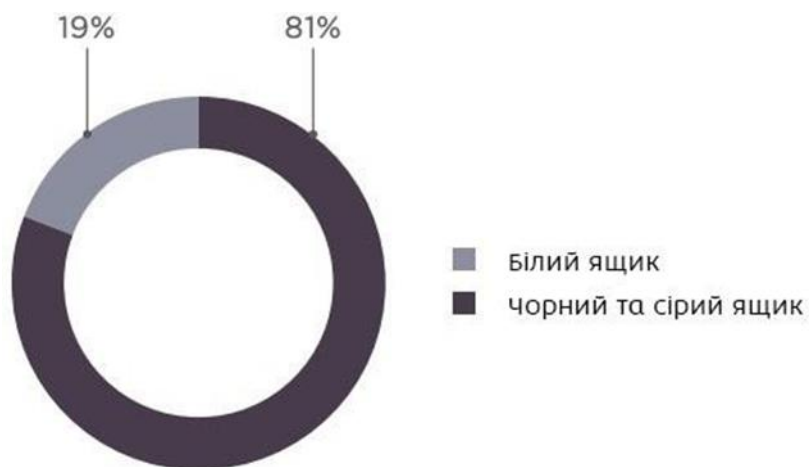


Рис. 2.3 Методи тестування

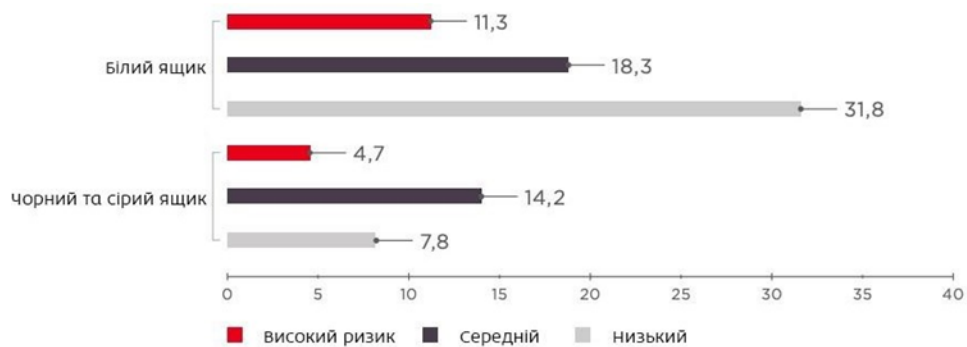


Рис. 2.4. Кількість виявлених вразливостей на одну систему

Висновки до другого розділу

Дослідженні методи захисту від веб-атак, та можливі засоби моніторингу стану захищеності веб-додатків, та вразливості які можуть призвести до вдалих веб-атак, а саме було наведено частини вразливого коду веб-додатків до веб-атак. Була наведена порівняльна статистика, щодо захисту від кібер злочинців в Україні.

Визначено, що навіть одна не вірна команда, що використовується в коді певного веб-додатку може звести всю безпеку ресурсу нанівець, тому слід бути обачним.

Підсумовуючи сказане, розробники ПЗ не завжди мають змогу вчасно вжити заходів щодо усунення вразливостей і випуску оновлень. Тому, щоб ефективно протистояти злочинцям, необхідно спостерігати і запобігати атакам на користувачів, аналізувати і зіставляти безліч подій для виявлення ланцюжків атак, виявляти експлуатація вразливостей нульового дня. Зазначенні заходи дозволять своєчасно зупинити зловмисників.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

РОЗДІЛ 3. РЕАЛІЗАЦІЯ АТАК

Метою даного розділу є захист веб-ресурсу від шкідливих запитів. В першому розділі ми переглядали теоретичні відомості про веб-атаки.

В цьому розділі буде описано, як захистити веб-ресурс від різних видів атак за допомогою CMS Magento, та продемонструвати захист цього веб-ресурсу.

3.1 Теоретичні відомості про систему керування контентом Magento

Система керування контентом (CMS) — програмне забезпечення для організації веб-сайтів чи інших інформаційних ресурсів в інтернеті чи окремих в комп'ютерних мережах.

Існують сотні, а може, навіть й тисячі доступних CMS-систем. Завдяки їх функціональності ці системи можна використовувати в різних компаніях. Незважаючи на широкий вибір інструментальних та технічних засобів, наявних в CMS, існують загальні для більшості типів систем характеристики. Перші CMS були розроблені у великих корпораціях для організації роботи з документацією. У 1995-му з'явилась компанія Vignette, яка започаткувала ринок для комерційних CMS. З часом діапазон продукції розширювався і дедалі більше інтегрувався у сучасні мережеві рішення аж до популярних веб-порталів.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Magento – безкоштовна CMS з відкритим кодом. Головна перевага величезна кількість можливостей «з коробки». Зробити магазин без допомоги програміста не вийде. Але зате, якщо клієнт готовий найняти фахівця, він зможе за відносно невеликі гроші отримати справді потужний інструмент. Якщо ви розробник,якому доводиться робити інтернет-магазини, також є ймовірність, що дана CMS вас зацікавить.

Magento сфокусована на роботі з контентом, вирішенні маркетингових завдань і взаємодії з покупцями. Розробляє систему американська компанія Varien. Вони надають платні послуги зі створення і підтримки інтернет-магазинів. У компанії працює більше 50 чоловік. Тобто цією компанією займаються серйозно, і бізнес розробників зрозумілий.

В CMS можна зробити будь-який інтернет-магазин. Серед переваг: можна відзначити величезні вбудовані функціональні можливості, а також масштабованість і розширюваність. Також варто відзначити, що до Magento створено величезну кількість розширень/модулів. Половина з них безкоштовні, а друга половина недорогі в ціні. Теж саме можна сказати і про шаблони: на сайті «Template Monster» до цієї CMS можна знайти 700 шаблонів на всі популярні тематики. Так що переваг дуже багато.

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Структура модуля Magento 2 по готовому прикладу, рис 3.1

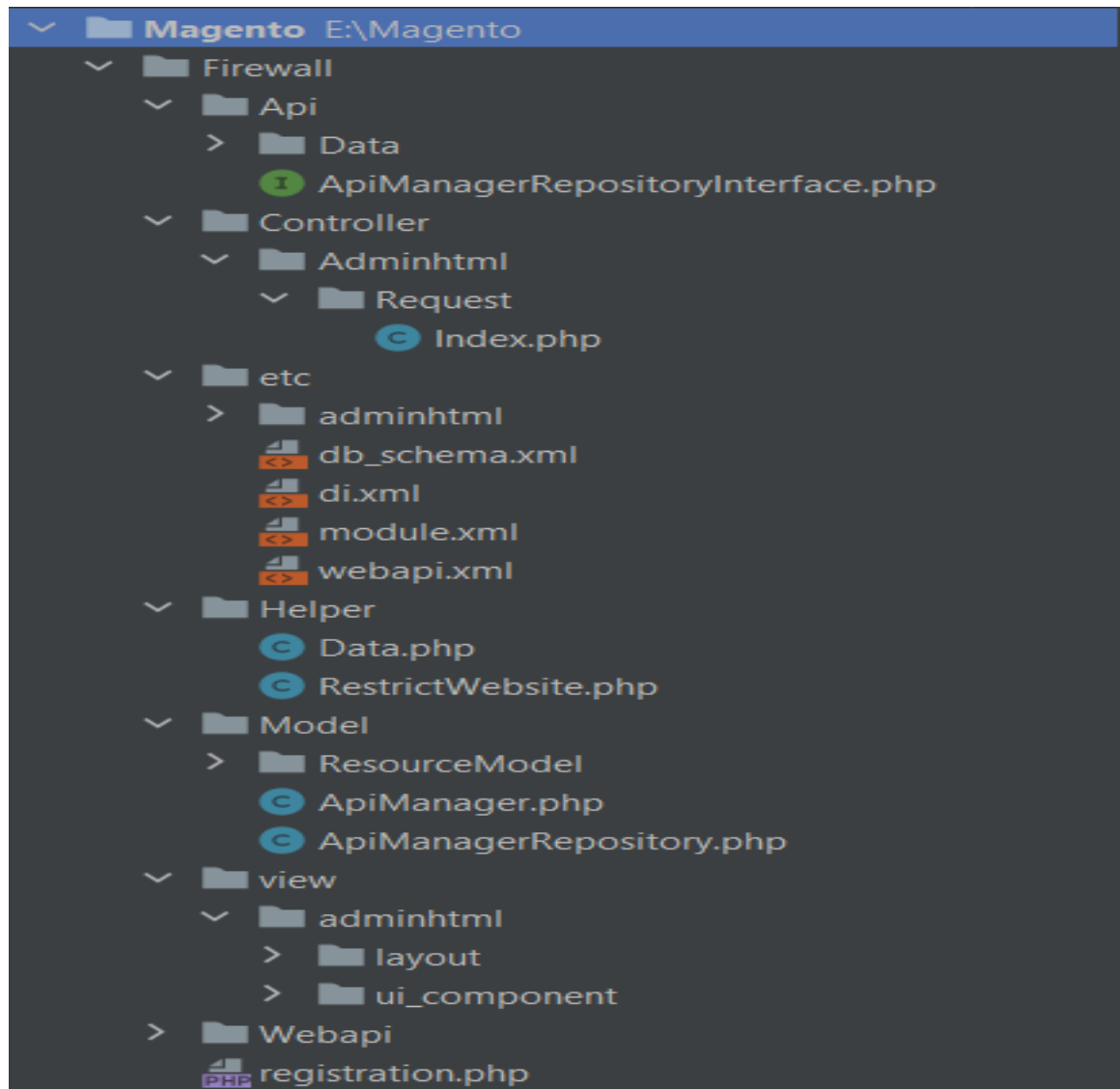


Рис. 3.1. Структура модуля Magento 2

Api – PHP інтерфейси

Controller – PHP контролер-класи (частина MVC);

Adminhtml – контролер-класи, що застосовується в адмін-панелі

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Etc – конфігураційні файли модуля

Helper – PHP класи з допоміжною логікою. Їхні методи використовуються у різних частинах модуля

Model – PHP класи моделей (частина MVC)

View – файли вигляду: макети, темплейти, js, css, html, зображення, шрифти

Webapi – реквест

Registration.php – файл, що реєструє модуль у системі

Така структура не містить усіх можливих директорій і файлів, що можуть знаходитись у модулі Magento 2. Вона лише відображає часто використовувані компоненти модуля.

3.2 Знайомство з Magento

Спершу потрібно зайти на готовий ресурс, тобто на сайт. Після чого нам потрібно зайти в admin панель. Вказуємо ім'я та пароль (в наведеному нижче малюнку, пароль приховано, з конфіденційних міркувань), які вказані на рис 3.2

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65



Рис. 3.2 Вхід в admin панель

Далі потрапляємо на головну сторінку сайту, під тегом адміністратора. Це можемо побачити на рис. 3.3

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

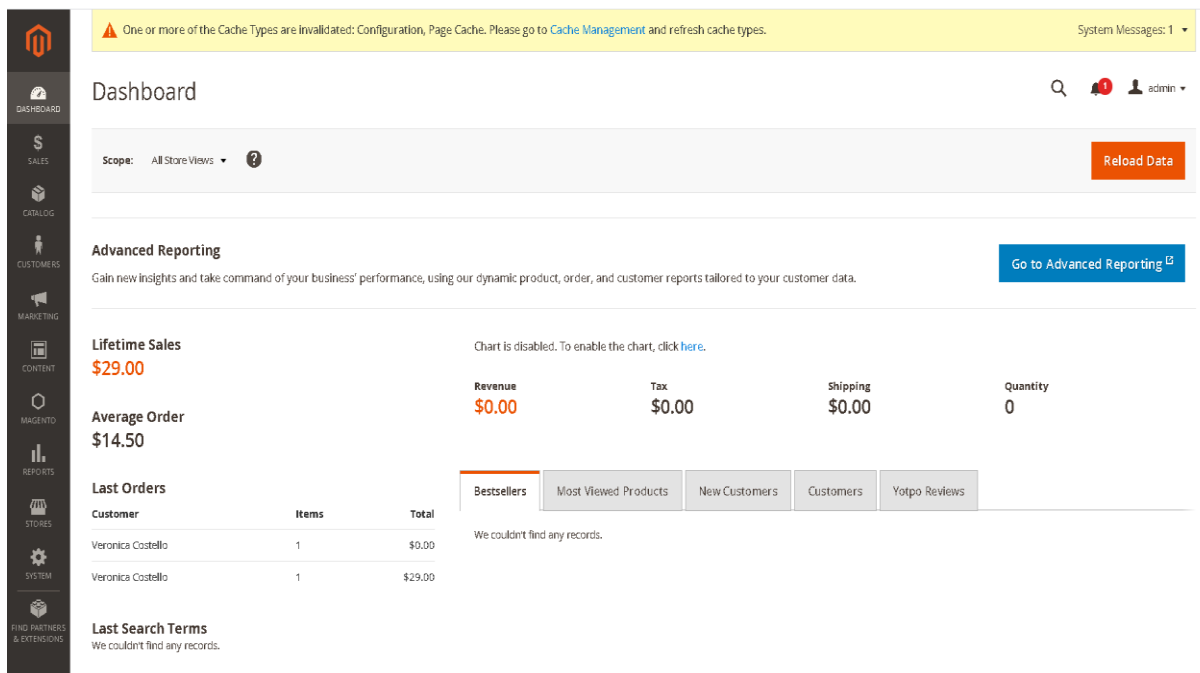


Рис. 3.3 Демонстрація головної сторінки сайту

Перейшовши, до головної сторінки, заходимо до потрібного розділу, розділ – Magento. Рис. 3.4

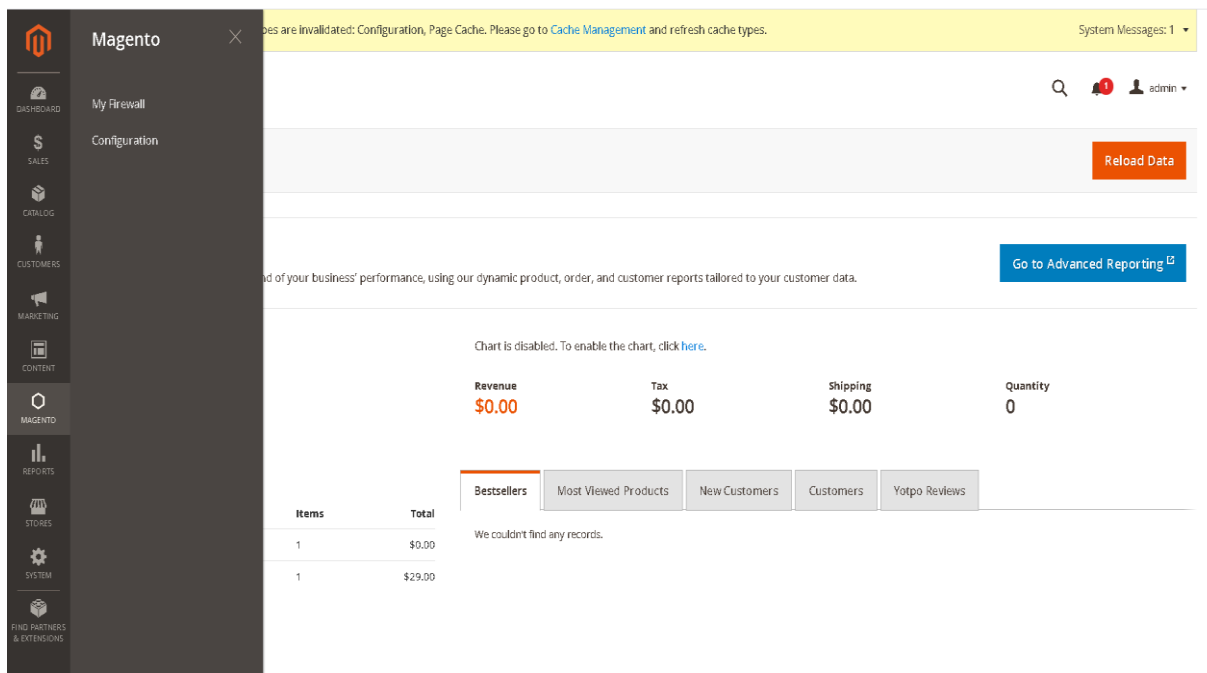


Рис. 3.4 Розділ Magento

В розділі Magento одразу бачимо дві вкладки, це – My Firewall і Configuration.

My Firewall відповідає за Requests, тобто запити, які приходили від різних користувачів, ботів, Google, Yandex аналітики і т.п. як показано на рис. 3.5.

One or more of the Cache Types are invalidated: Configuration, Page Cache. Please go to Cache Management and refresh cache types. System Messages: 1				
DASHBOARD SALES CATALOG CUSTOMERS MARKETING CONTENT MAGENTO REPORTS STORES SYSTEM FIND PARTNERS & EXTENSIONS Requests 35 records found 20 per page < 1 of 2 >				
ID	IP Address	Path	Note	Created At
105	206.189.205.251	/rest/V1/apimanager/createcustomerstring	("status":0,"message":"Displayed Error Message - Block Request By IP Address","host":"apiplus.reqbin.com")	2021-06-04 11:17:21
104	46.219.204.40	/rest/V1/apimanager/createcustomerstring	("status":0,"message":"Displayed Error Message - Block Request By Path","host":"46.219.204.40")	2021-06-04 11:16:59
103	46.219.204.40	/rest/V1/apimanager/createcustomernumber	("status":1,"message":"","host":"46.219.204.40")	2021-06-04 11:16:51
102	206.189.205.251	/rest/V1/apimanager/createcustomerstring	("status":1,"message":"","host":"apiplus.reqbin.com")	2021-06-04 11:14:20
101	206.189.205.251	/rest/V1/apimanager/createcustomerstring	("status":1,"message":"","host":"apiplus.reqbin.com")	2021-06-04 11:14:03
100	206.189.205.251	/rest/V1/apimanager/createcustomerstring	("status":1,"message":"","host":"apiplus.reqbin.com")	2021-06-04 11:12:42
99	206.189.205.251	/rest/V1/apimanager/createcustomerstring	("status":1,"message":"","host":"apiplus.reqbin.com")	2021-06-04 11:12:11
98	46.219.204.40	/rest/V1/apimanager/createcustomerstring	("status":1,"message":"","host":"46.219.204.40")	2021-06-04 11:11:15
97	46.219.204.40	/rest/V1/apimanager/createcustomernumber	("status":1,"message":"","host":"46.219.204.40")	2021-06-04 10:59:04
96	46.219.204.40	/rest/V1/apimanager/createcustomerstring	("status":0,"message":"Displayed Error Message - Block Request By Path","host":"46.219.204.40")	2021-06-04 10:58:03
95	46.219.204.40	/rest/V1/apimanager/createcustomerstring	("status":0,"message":"Displayed Error Message - Block Request By Path","host":"46.219.204.40")	2021-06-04 10:56:59
94	46.219.204.40	/rest/V1/apimanager/createcustomerstring	("status":0,"message":"Displayed Error Message - Block Request By Path","host":"46.219.204.40")	2021-06-04 10:55:26
93	46.219.204.40	/rest/V1/apimanager/createcustomernumber	("status":1,"message":"","host":"46.219.204.40")	2021-06-04 10:54:32

Рис. 3.5 Requests

В Requests є сортування даних по ID, Path, Note і Created at. Дані зберігаються, тому є можливість переглянути потрібну для нас інформацію в будь-який час.

Configuration відповідає за загальні налаштування Magento, як показано на рис 3.6.

Configuration

Scope: Default Config

Save Config

GENERAL

CATALOG

SECURITY

CUSTOMERS

SALES

YOTPO

DOTDIGITAL

SERVICES

MAGENTO FIREWALL

My Firewall

ADVANCED

General

Enable

Yes

Enable/Disable extension

Block Request By IP Addresses

127.0.0.1,127.0.0.2

Please enter IP address with comma separated. For example : 127.0.0.1,127.0.0.2

Block Request By Path

/rest/V1/apimanagers/createcustomer,/rest/V1/apimanagers/createcustomerstring

Please enter request path with comma separated. For example : /rest/V1/apimanagers1,/rest/V1/apimanagers2

Displayed Error Message

Displayed Error Message

Рис. 3.6 Configuration

У вкладці Configuration є багато під-вкладок, завдяки яким можливе додавання контенту на сайт, зміна URL і т.п. Нас цікавить під-вкладка Magento Firewall, де можливі такі налаштування, а саме : Включити/виключити веб-сайт, блокування запиту по IP address, блокування запитів за шляхом. Після будь-яких змін в налаштуванні, адміністратор ресурсу може зберегти конфігурації, натиснувши на кнопку Save config.

3.2.1 Реалізація створення Customers

В цьому розділі ми будемо створювати нових користувачів для нашого сайту. Для цього ми будемо використовувати безкоштовні інструменти для тестування API. Перевіривши веб-сайт, надіславши запит POST з браузера або програми, де

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

перевіримо відповіді сервера. Для цього є онлайн-інструмент Reqbin.com і програма Postman. Ми розглянемо тільки програму Postman. Так як, що програма, що веб-сайт – ідентичні в використанні.

Запускаємо програму, вибираємо метод POST і вписуємо HTTP запит, як показано на рис 3.7.

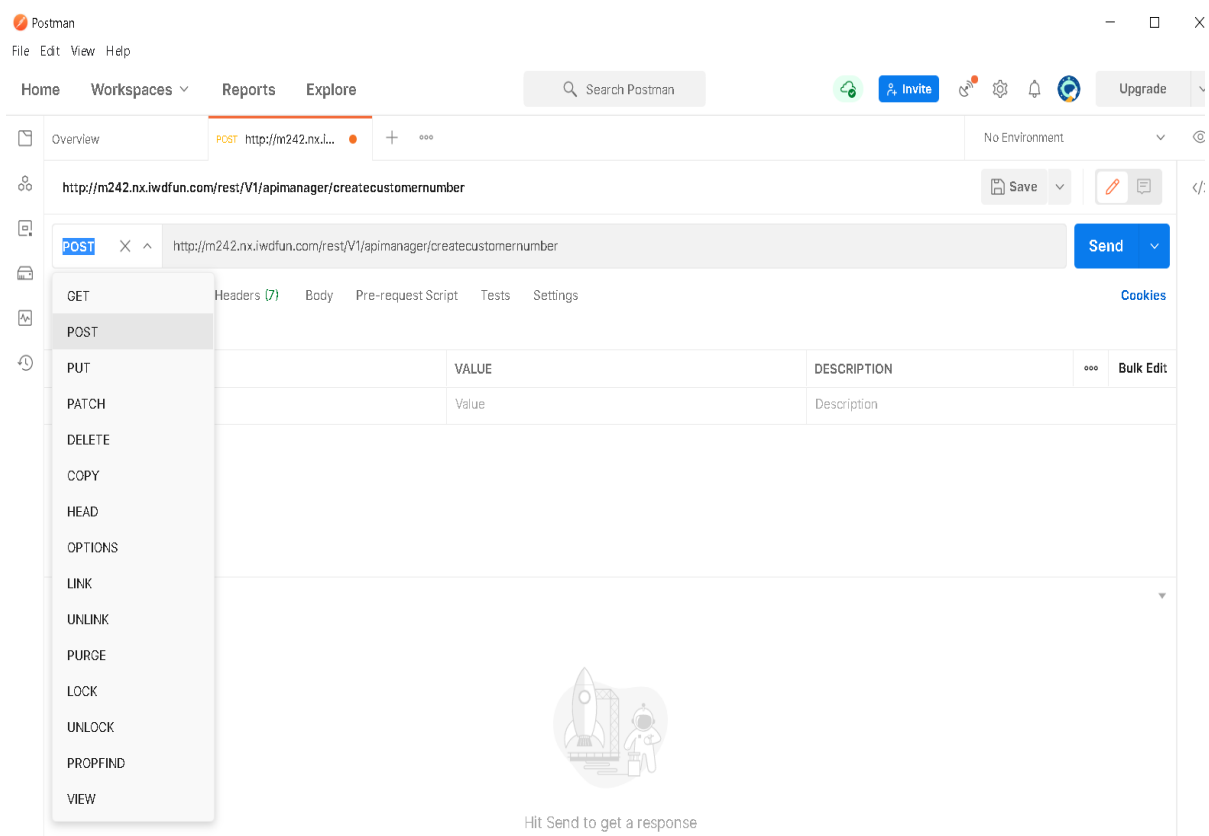


Рис. 3.7 HTTP запит

Request в Magento 2 посилається на /rest/ , це дозволений шлях, через який Magento приймає усі POST і GET запити. Далі створення нового користувача за номером, як показано на рис 3.8.

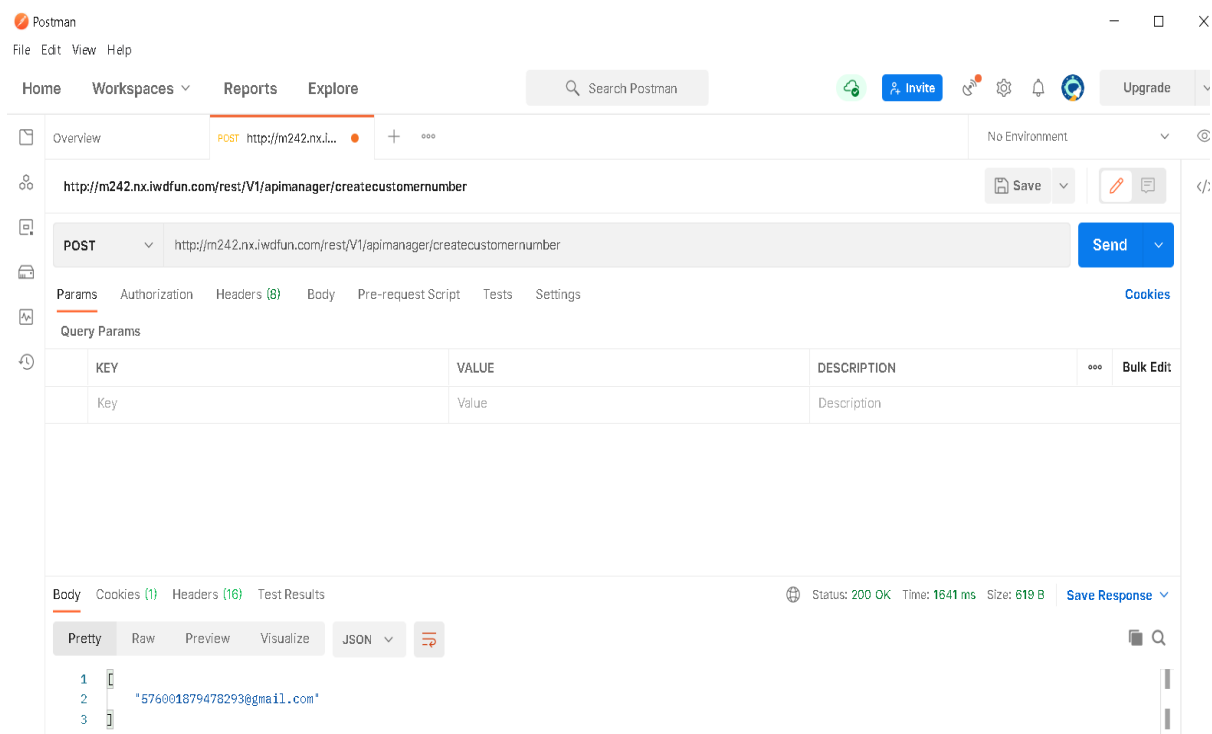


Рис. 3.8 Створення користувача

Як бачимо, POST запит на створення користувача за номером успішно пройдений. Що ж, переглянемо статистику і дані, які прийшли на наш сайт, на рис. 3.9

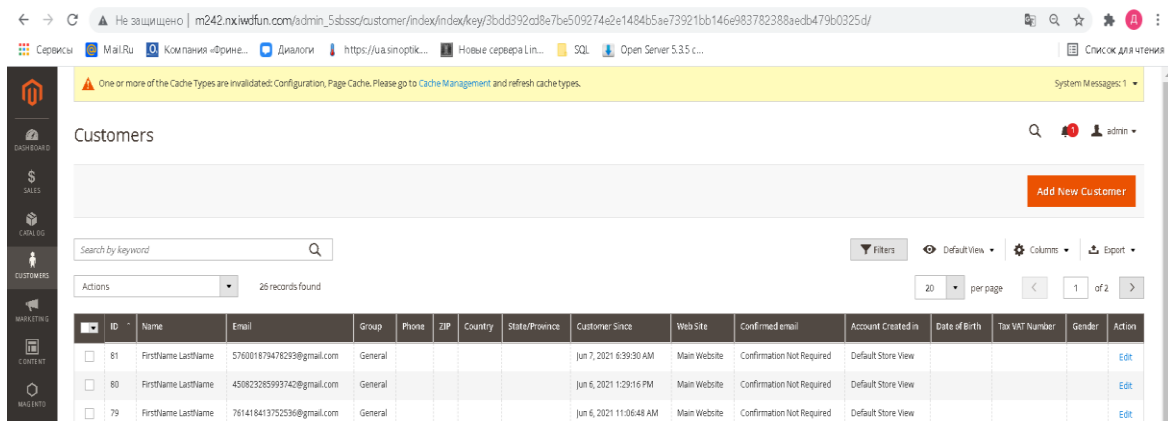
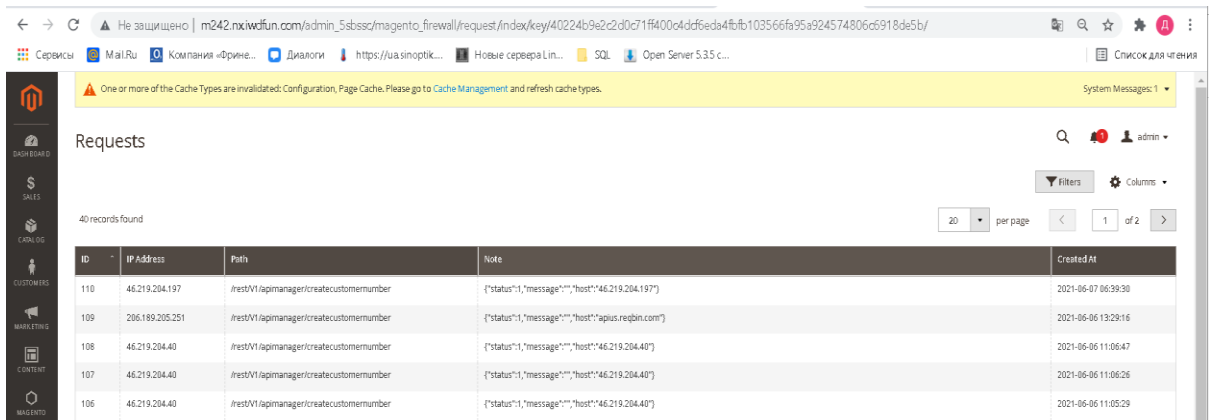


Рис. 3.9 Створення користувача

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Одразу бачимо дані користувача, а саме : id, name, email і т.д. Але нас цікавить сама статистика Magento, для цього переходимо у вкладку Magento і вибираємо пункт Myfirewall, і спостерігаємо за ситуацією, як показано на рис 3.10



ID	IP Address	Path	Note	Created At
110	46.219.204.197	/rest/V1/apimanager/createcustomnumber	{"status":1,"message":"","host":"46.219.204.197"}	2021-06-07 06:39:30
109	206.189.205.251	/rest/V1/apimanager/createcustomnumber	{"status":1,"message":"","host":"apius.reqbin.com"}	2021-06-06 13:29:16
108	46.219.204.40	/rest/V1/apimanager/createcustomnumber	{"status":1,"message":"","host":"46.219.204.40"}	2021-06-06 11:06:47
107	46.219.204.40	/rest/V1/apimanager/createcustomnumber	{"status":1,"message":"","host":"46.219.204.40"}	2021-06-06 11:06:26
106	46.219.204.40	/rest/V1/apimanager/createcustomnumber	{"status":1,"message":"","host":"46.219.204.40"}	2021-06-06 11:05:29

Рис 3.10 Статистика Magento

Запит відображається в статистиці Magento. Номер запиту, ір відправника, шлях через який відправлений запит, нотацію про статус (1 – успішний запит, 0 – невдалий), повідомлення, хост - тобто ір адреса, або сайт, через який був відправлений запит і дата створення.

Тепер створимо користувача за рядком випадкових букв та цифр, демонстрація на рис. 3.11

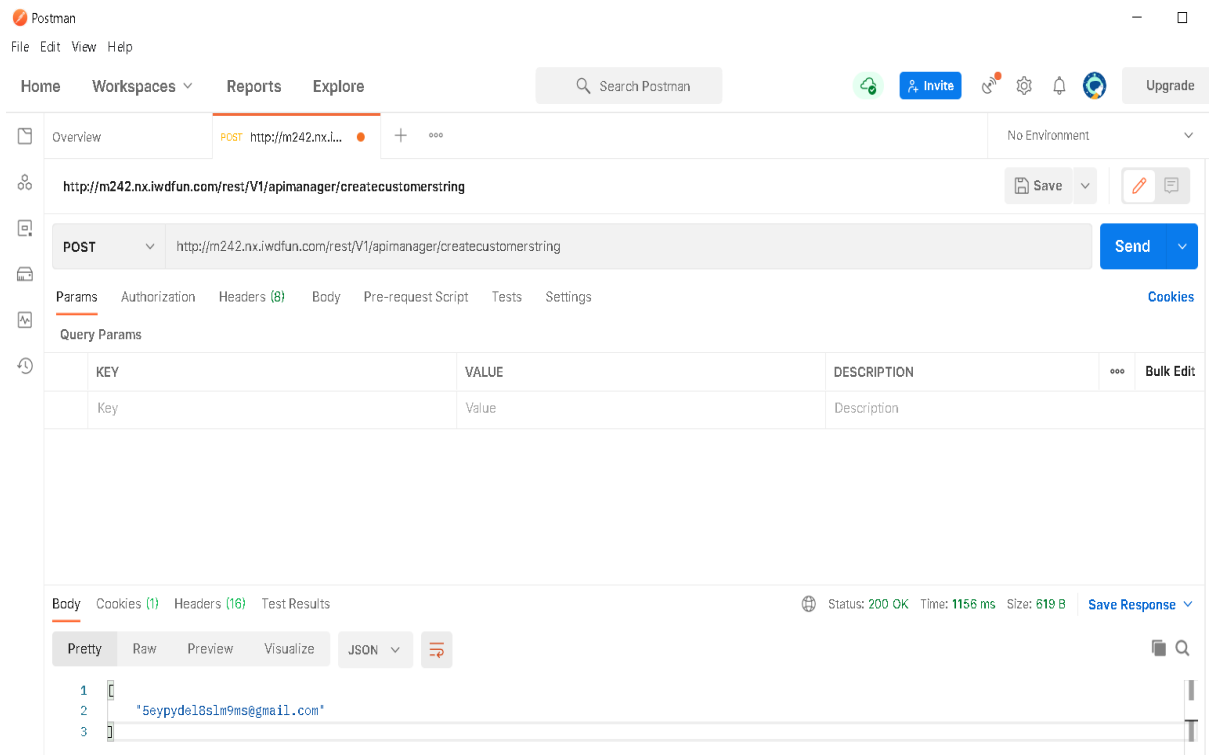


Рис. 3.11 Створення користувача

Користувач успішно створений, статистику немає сенсу демонструвати, так як змінилися лише дані Path, тобто шлях, завдяки якому він був створений.

3.3 Реалізація захисту CMS Magento від відповідних атак

3.3.1 Реалізація захисту від Requests атак

Тепер розглянемо принцип захисту від роду атак по типу Request. Для цього заходимо на наш сайт, переходимо до вкладки Magento. Вибираємо пункт Configuration. Рис. 3.12

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

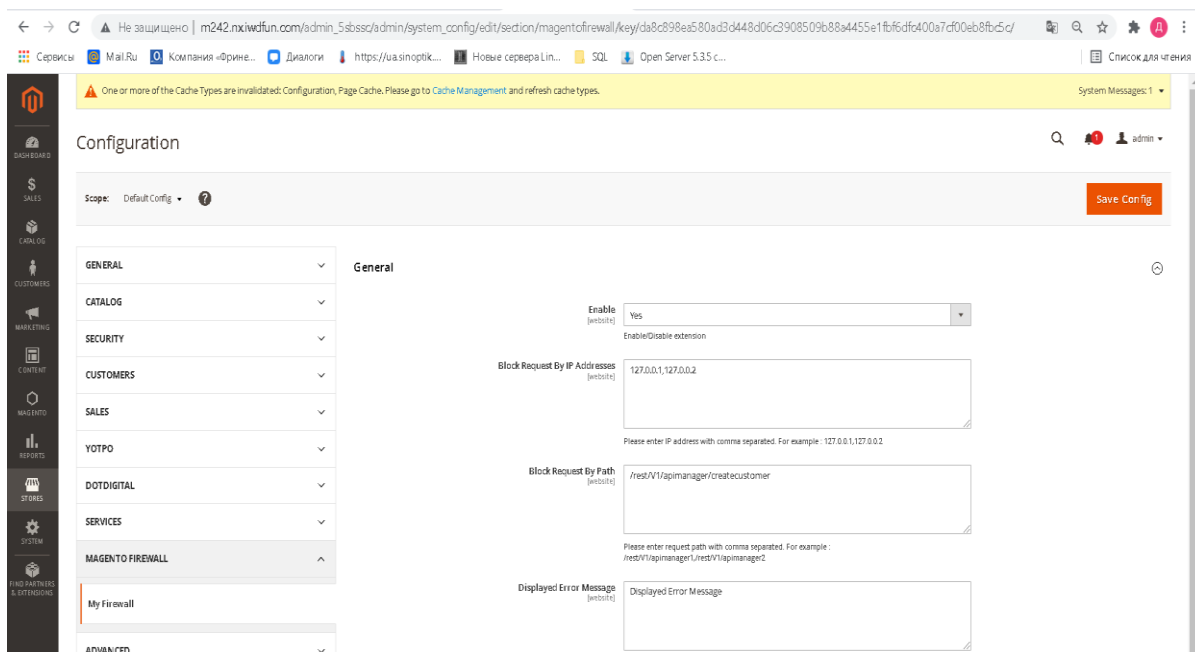


Рис. 3.12 Configuration

Нас цікавлять два блоки, а саме : Block request by ip addresses і block request by path. В першому блоці можливе блокування користувача, бота і т.п. по ір-адресу. В другому блоці можливе блокування за шляхом того самого користувача чи бота, завдяки якому він відправив запит на наш сайт.

Для початку продемонструю перший спосіб, тобто блокування по ір. Для цього, в блоці Block request by ip addresses, вписуємо ір-адрес користувача, як показано на Рис. 3.13

		Кулик Д.А.			КІ.КР.Б – 123 - 21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

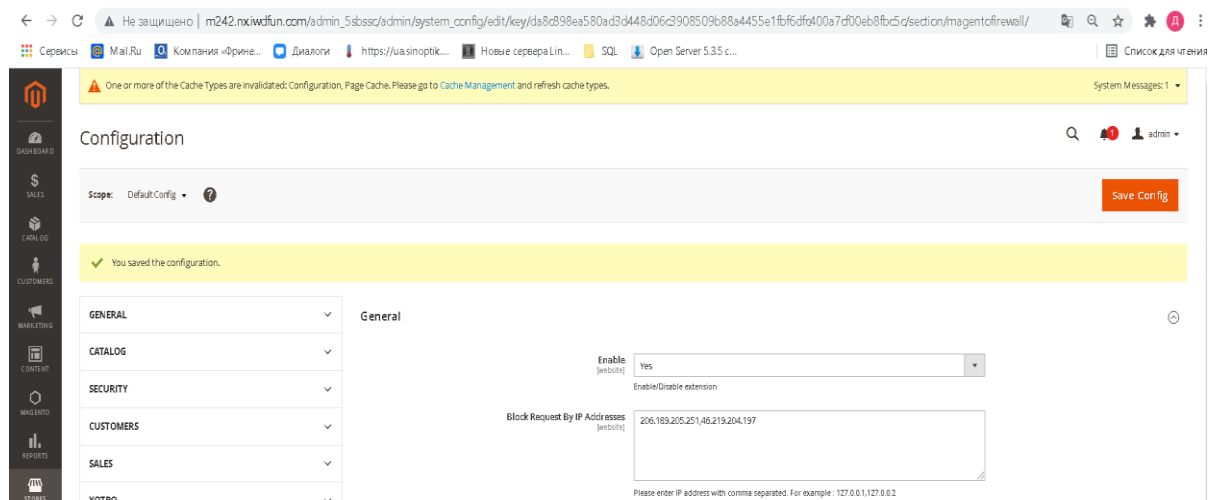


Рис. 3.13 Блокування по Ір

Вписуємо ір-адресу користувача. Для наглядного прикладу, продемонструю блокування своєї ір-адреси. Натискаємо на кнопку Save config. Після чого, дані збережені на сервері. Спробуємо знову відправити запит від мого імені, тобто від моєї ір-адреси, для цього переходимо у програму Postman і повторюємо ті ж самі кроки, що робили раніше і дивимося результат на Рис. 3.14

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

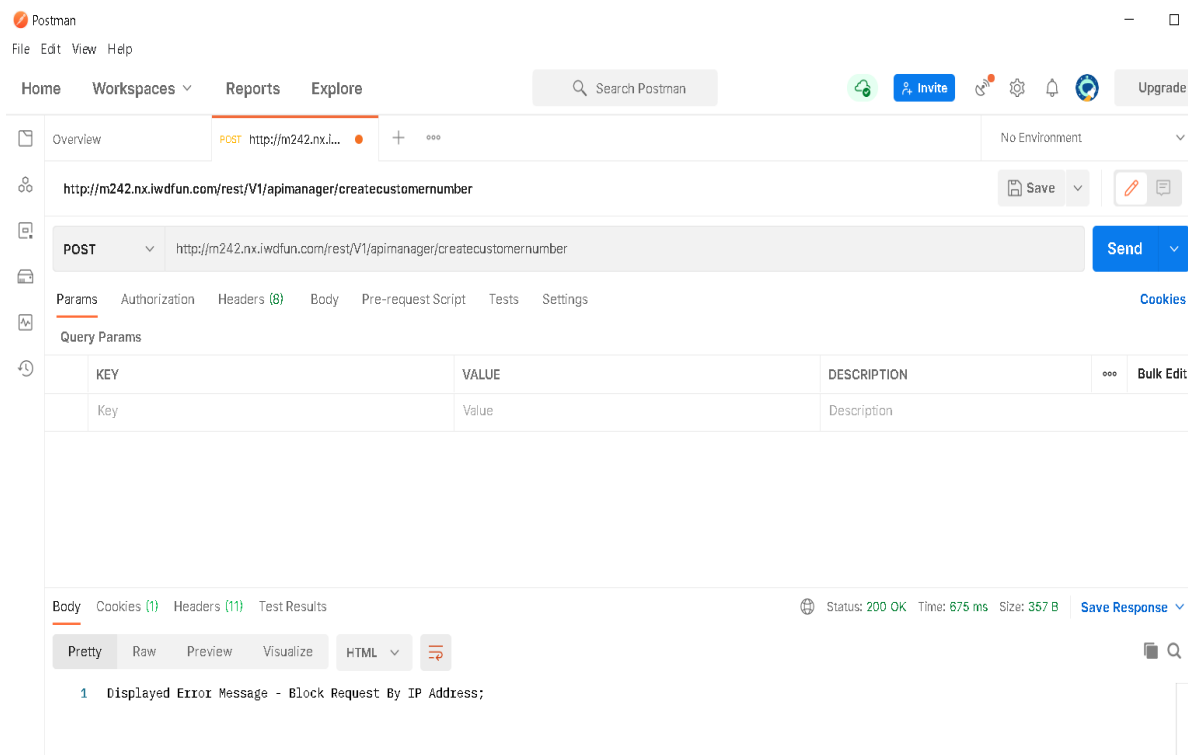


Рис. 3.14 Створення користувача

Програма видала помилку – Displayed Error Message. Блокування по ip-адресі було успішним. Це може свідчити статистика в Magento, як показано на рис 3.15

ID	IP Address	Path	Note	Created At
117	46.219.204.197	/rest/V1/apimanager/createcustomernumber	{\"status\":\"0\",\"message\":\"Displayed Error Message - Block Request By IP Address;\",\"host\":\"46.219.204.197\"}	2021-06-07 09:01:26

Рис 3.15 Статистика requests

Magento успішно блокує мою ір-адресу. Статус запиту 0, тобто неуспішний, повідомлення про помилку і моя ір-адреса. Мій запит на створення користувача за номером не був відправлений на сервер, але відображається в Magento.

Продемонструю другий спосіб блокування, блокування за шляхом. Переходимо на сайт, натискаємо на вкладку Magento, вибираємо пункт Configuration. В блоці Block request by path вписуємо шлях, через який нам не хотілося б бачити запитів, наприклад, створення користувачів за рядком випадкових букв та чисел. Демонстрація на рис. 3.16

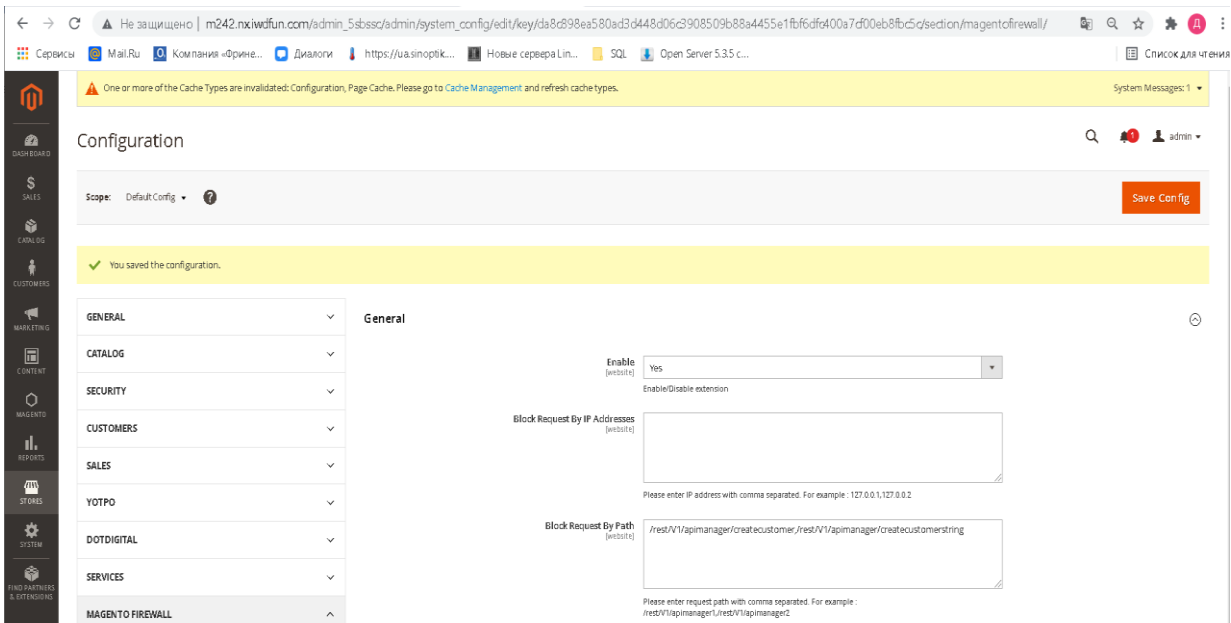


Рис. 3.16 Блокування за шляхом

Після чого нам потрібно зберегти конфігурацію і перейти до програми Postman, і відправити запит на створення користувача за рядком випадкових букв та чисел. Рис. 3.17

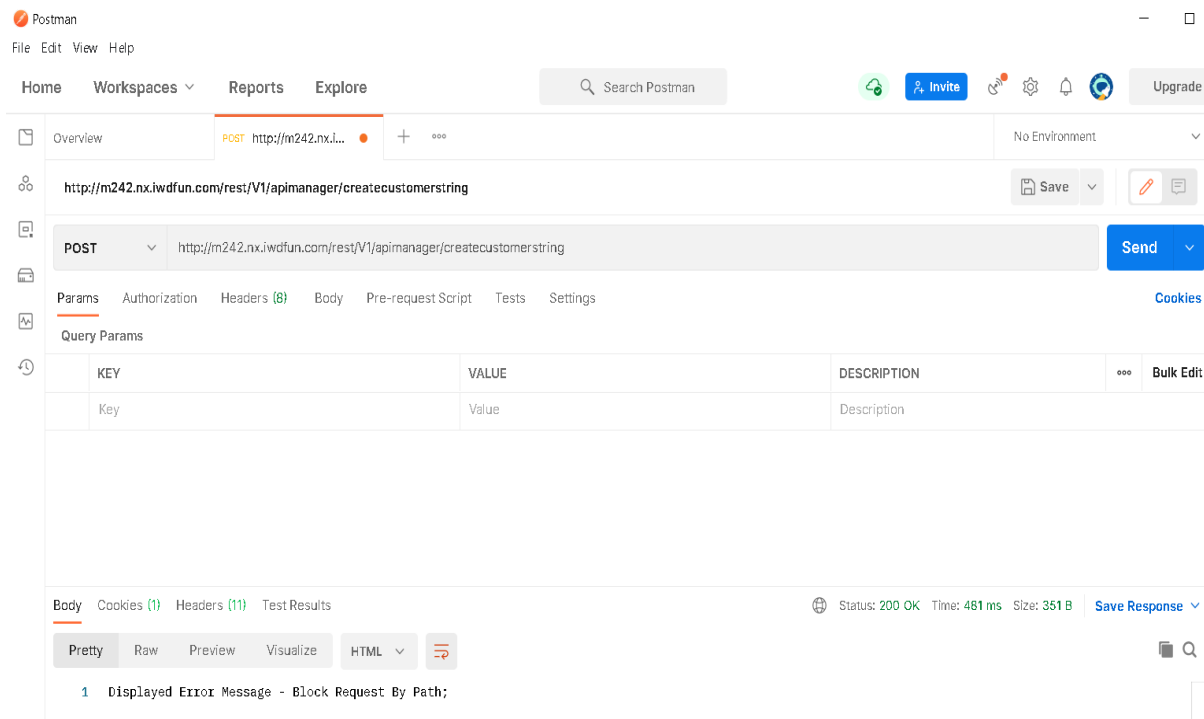


Рис. 3.17 Створення користувача

Як бачимо, програма знову видає помилку, а саме : Displayed Error Message – Block Request By Path. Це свідчить про те, що запит був заблокований за даним шляхом. Переглянемо статистику Magento, що зображено на рис. 3.18

ID	IP Address	Path	Note	Created At
119	46.219.204.197	/rest/V1/apimanager/createcustomerstring	{\"status\":0,\"message\":\"Displayed Error Message - Block Request By Path\",\"host\":\"46.219.204.197\"}	2021-06-07 09:28:25

Рис. 3.18 Статистика requests

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

Запит успішно заблокований за шляхом. Статус запиту 0, повідомлення про помилку і ір-адреса відправника запиту.

В даному під-розділі я продемонстрував, як захистити сайт від запитів, котрі приходять. Я створив декілька користувачів, відправив декілька запитів, а якщо зломисник відправить близько 100 запитів за 1 хвилину, робота сайту стане повільною, при цьому й взагалі можлива зупинка веб-ресурсу.

Все впирається в статистику, тобто я можу блокувати усі requests, котрі, наприклад, повторюються кожних 2 хвилини, і вони викликають підозри. Усі DDOS-атаки, які спрямовані на сайт. Вони або одразу зникають, тобто блокуються сервером, чи ще чимось, або записуються в «Логі від помилок»; всі запити я буду бачити, і можу блокувати.

3.3.2 Реалізація захисту SQL-ін'єкцією

Спробуємо реалізувати SQL-ін'єкцію на нашому сайті. Для того, щоб провести дану атаку, потрібно ввести в форму пошуку на сайті наступний SQL код :

```
SELECT * FROM 'admin_user'
```

Щоб закоментувати залишок рядка, потрібно використати наступні символи :

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

/*...;

--...;

Ввівши, натискаємо “Enter”. І дивимося на результат, який зображений на рис.

3.19

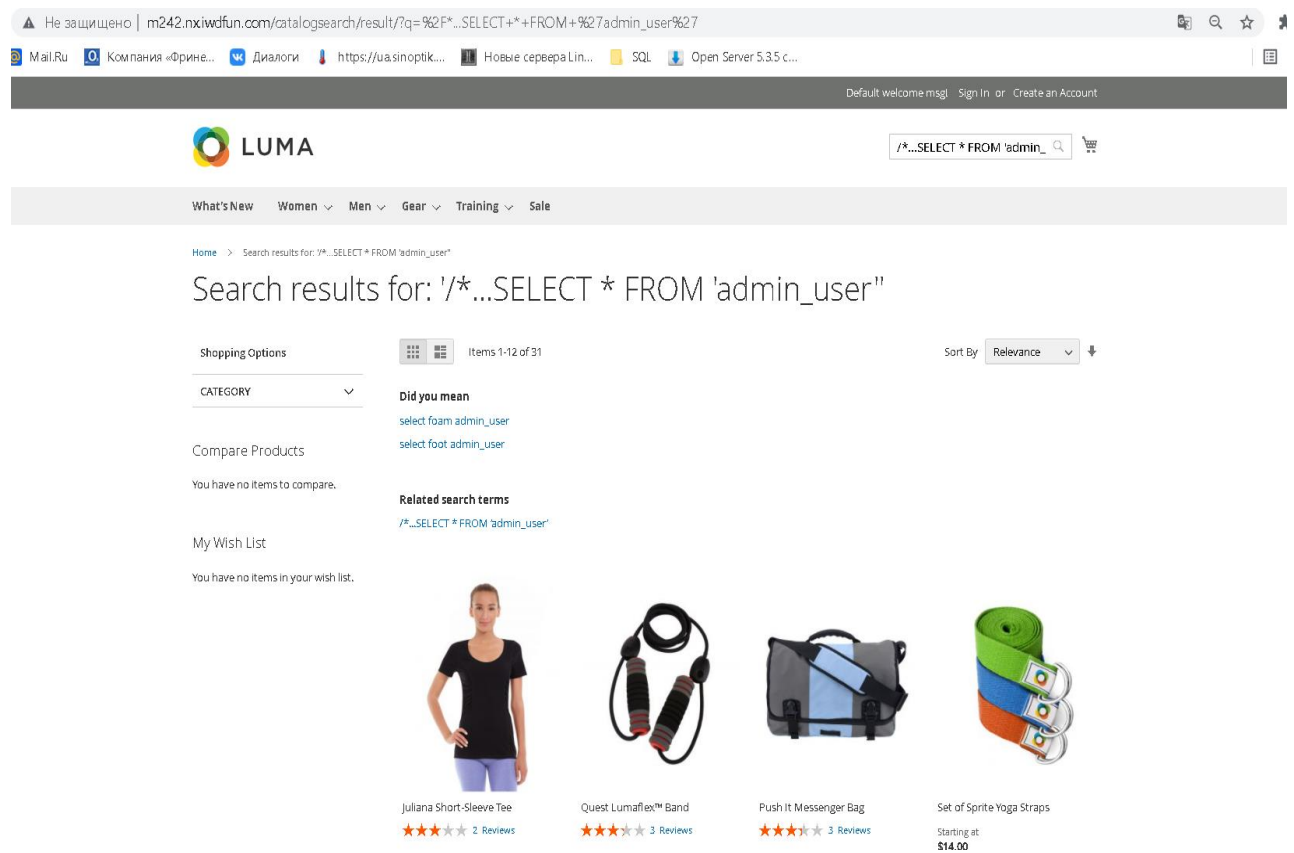


Рис. 3.19. SQL injection

Як бачимо, нічого не вдалось, отже CMS Magento захищає від подібних видів атак.

3.3.3 Реалізація захисту від RHP-ін'єкції

Щоб провести даний тип атаки, потрібно ввести наступну стрічку коду в пошукову форму сайту :

```
echo('aga');
```

Результат показано на рис. 3.20

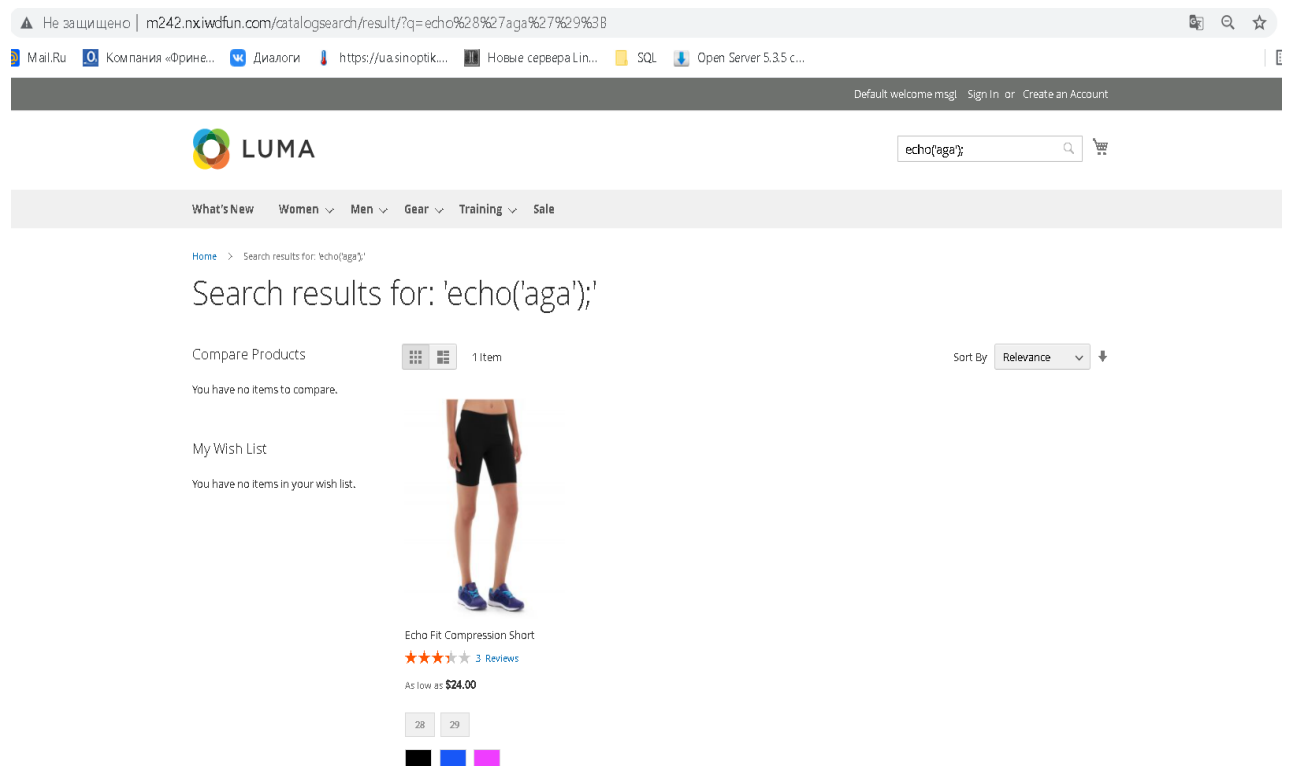


Рис. 3.20. PHP injection

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

Як бачимо, дана атака не була успішною, тому це говорить про добре написану серверну частину Magento.

3.3.4 Реалізація захисту від LDAP-ін'єкції

Є прості спроби LDAP-ін'єкцій, `user=*`, параметру `user` посилаємо символ `*`. Но розробники часто блокують значення `*`, тому спробуємо його обійти наступним шляхом.

Для атаки потрібно ввести в форму пошуку або додати до URL сайту наступне:
`(&(user=admin)(&))(password=q))`

У цьому прикладі коду, в LDAP `(&)` завжди вірна справжньому виразу, тобто назва користувача `admin` і пароль `q` або справжній вираз. Результат спостерігаємо на рис. 3.21.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

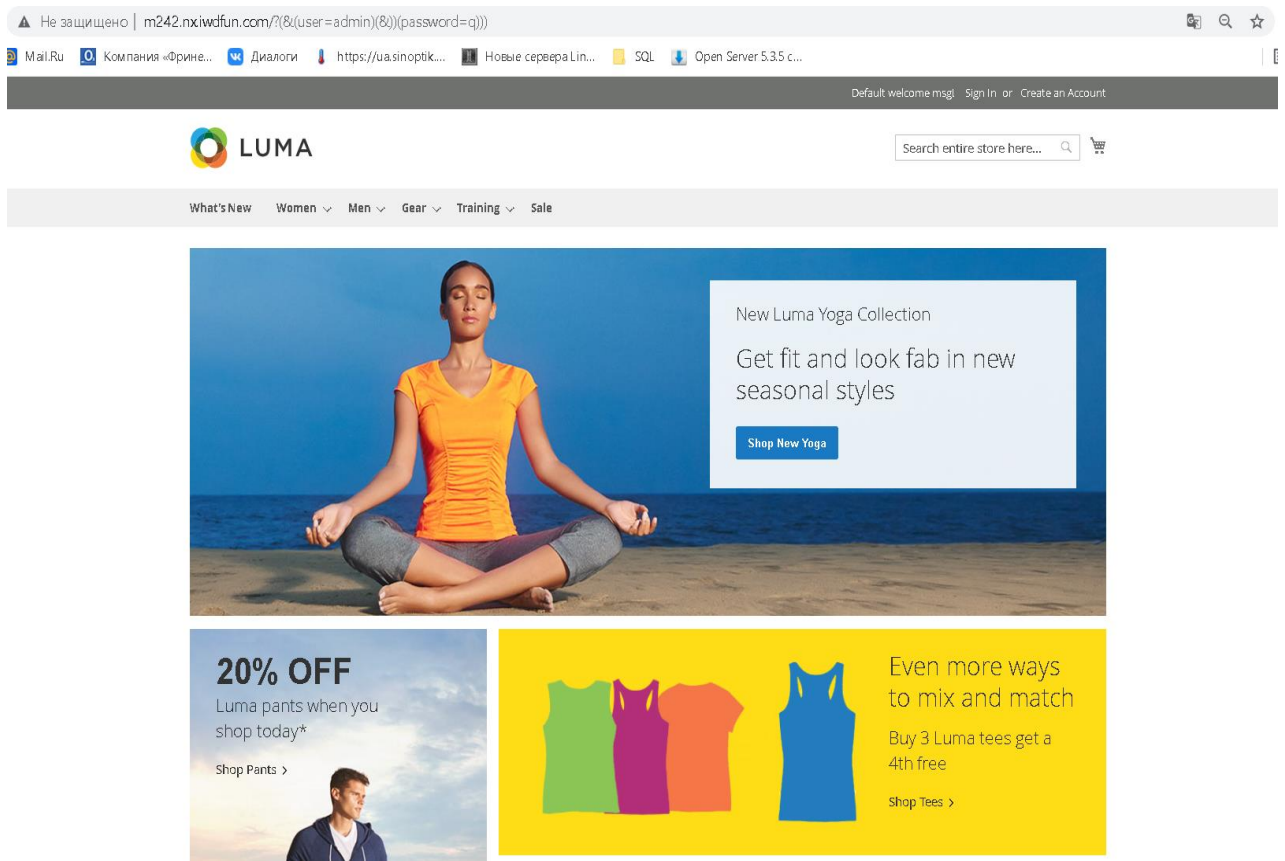


Рис.3.21. LDAP injection

LDAP ін'єкція не вдалась, Magento стійка до даного типу атак.

3.3.5 Реалізація захисту від Xpath-ін'єкції

Реалізуємо цю атаку на нашому інтернет-магазині. Потрібно авторизуватися, тільки не під вірними даними, а напишемо наступний код : ‘ or ‘1’ = ‘1 Результат на рис. 3.22.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

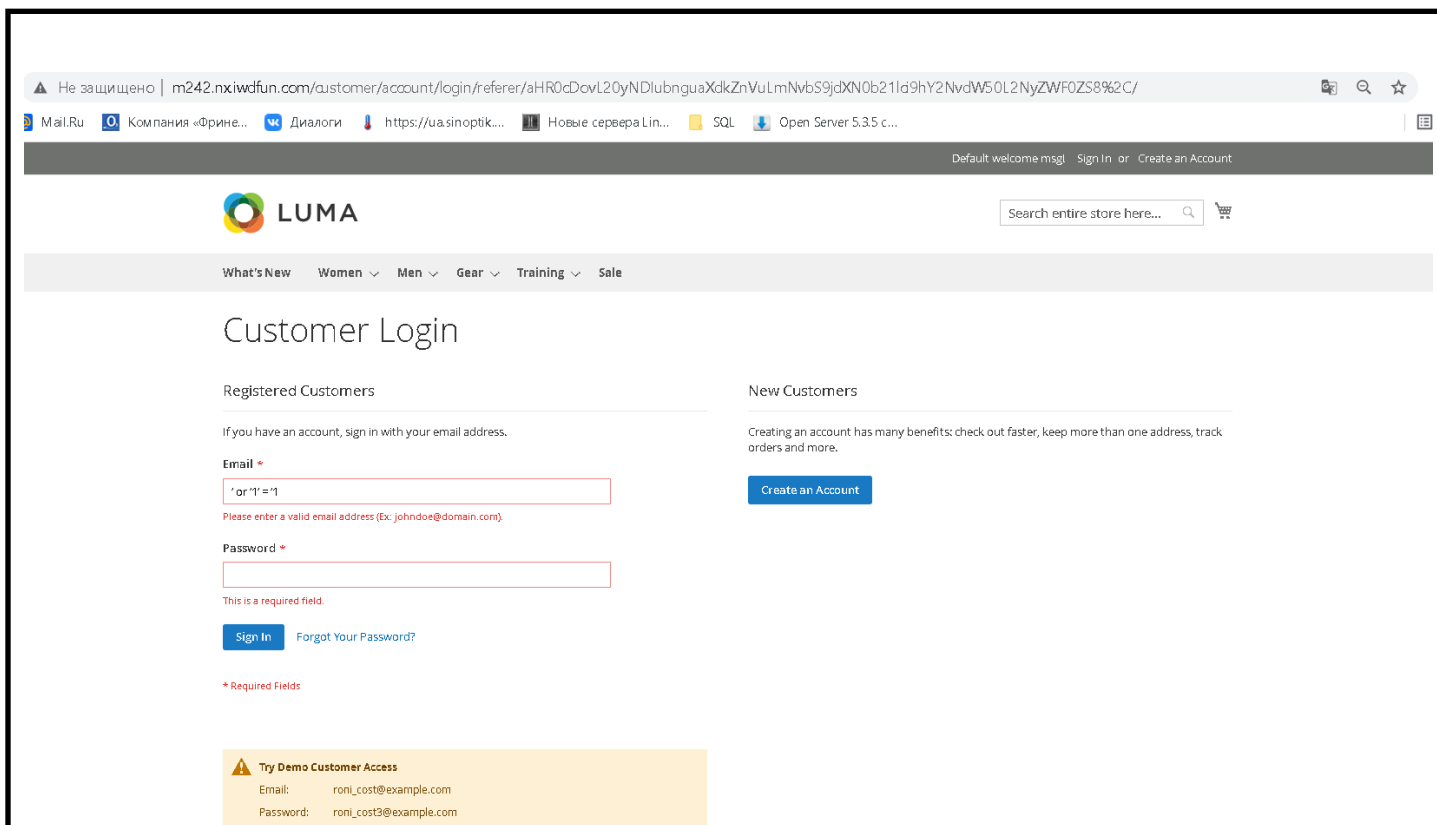


Рис. 3.22. Xpath injection

Як бачимо, Magento стійка до Xpath-інєкції.

3.3.6 XSS скриптинг

Даний тип атаки спрямований на міжсайтовий скриптинг, тобто XSS. Для цього в форму пошуку вписуємо наступний код:

```
<script>alert(22);</script>
```

Якщо атака буде успішною, має з'явитися вікно, зі значенням «22». Результат на рис. 3.23.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

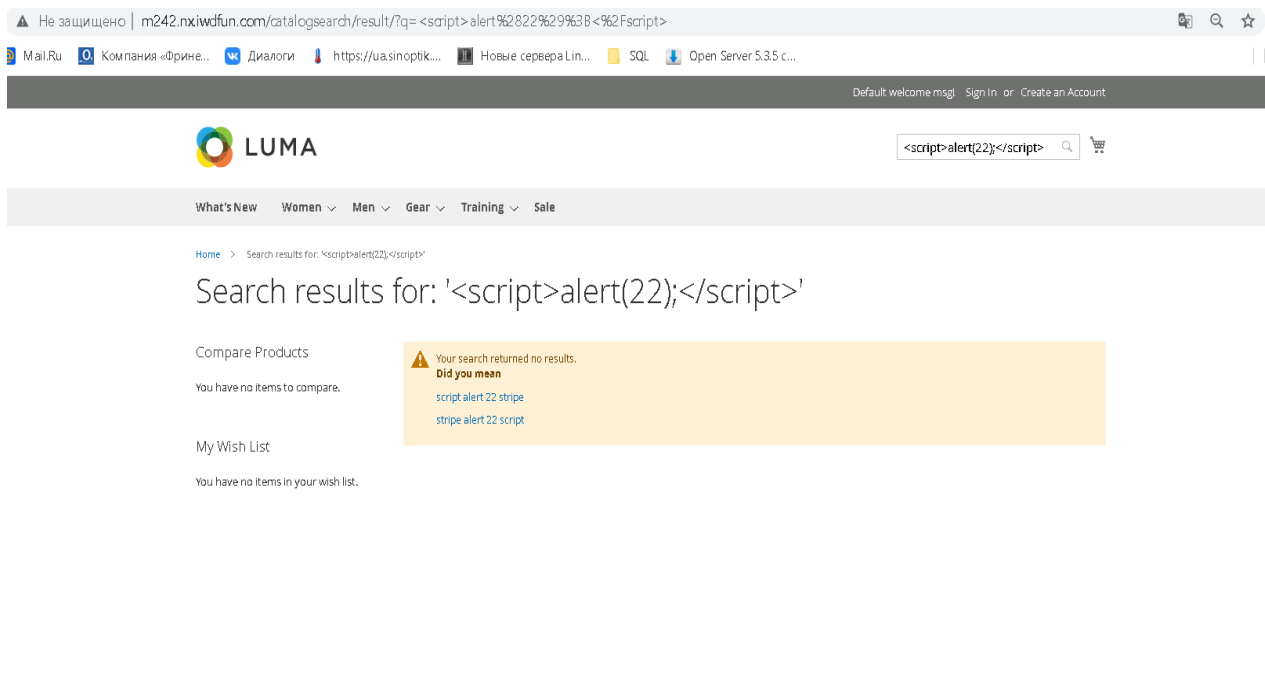


Рис. 3.23. XSS scripting

Нічого не з'явилося, атака не була успішною. CMS стійка до даного типу атак.

3.3.7 Брутфорс

Щоб реалізувати даний тип атаки, потрібно використати програму “Brutus”. В Target вписуємо ір адресу жертви, обираємо порт – 80, та вибираємо протокол. Це можемо побачити на рис. 3.24.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

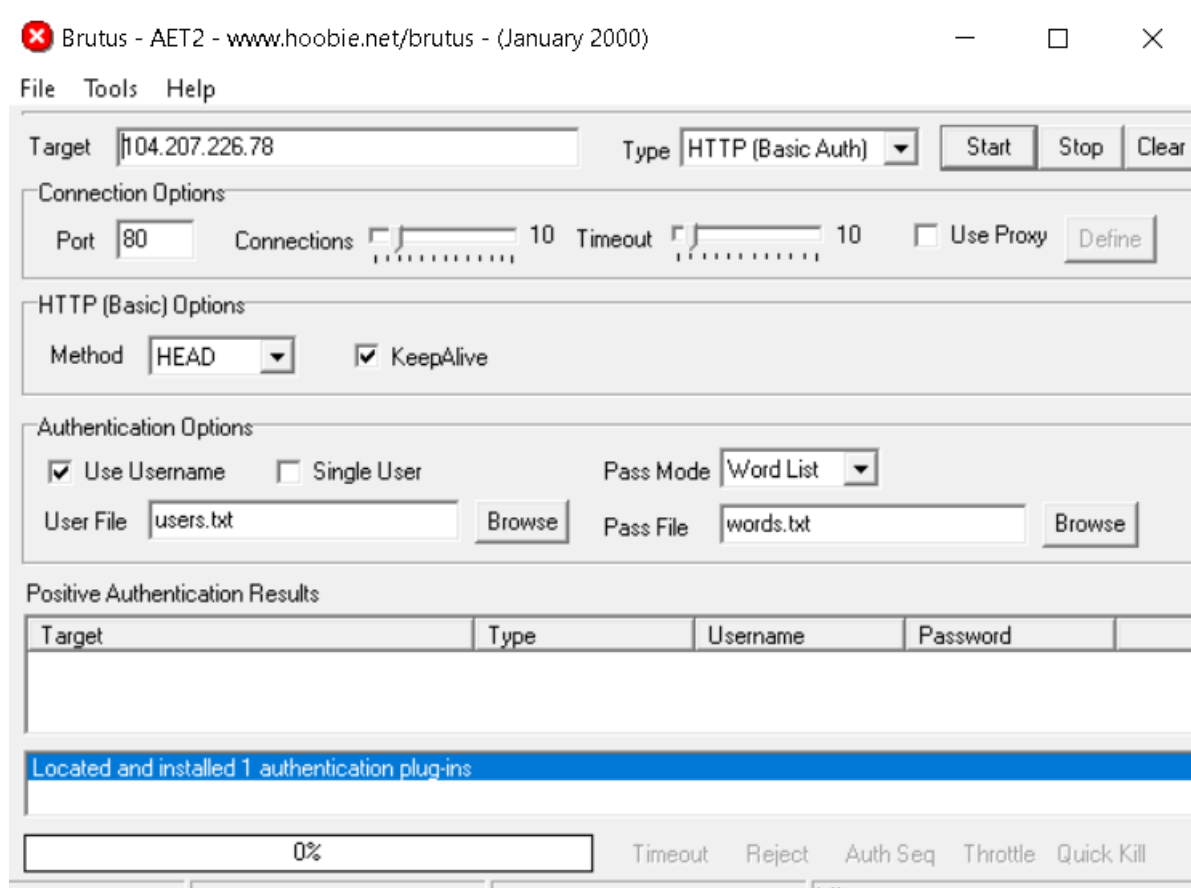


Рис.3.24 Брутфорс

Натискаємо Start і спостерігаємо наступну ситуацію на рис. 3.25

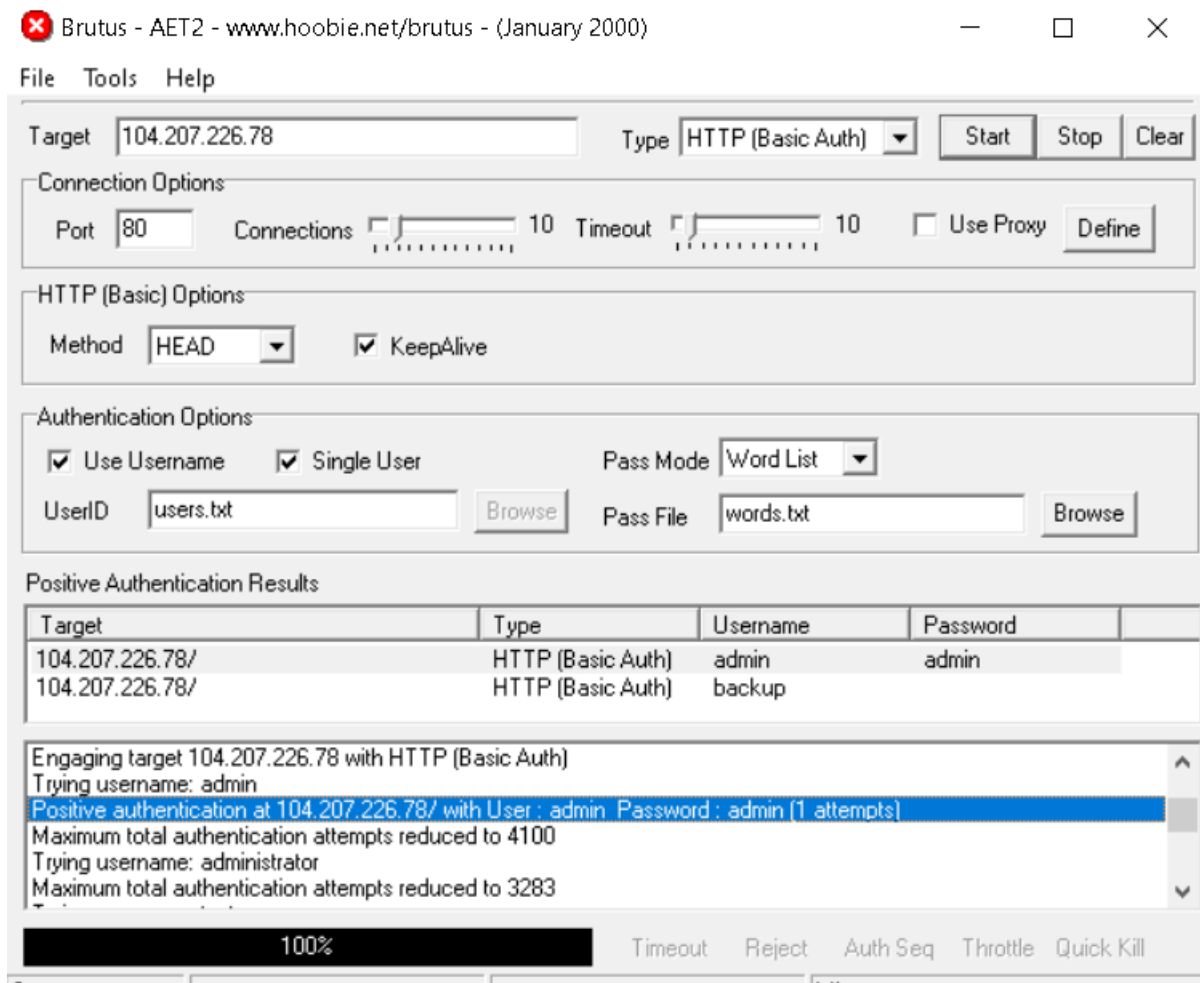


Рис.3.25 Результат Брутфорс

Програма видала логін admin та пароль admin. Логін вірний, а пароль ні, тому можна вважати, що програмі не вийшло реалізувати атаку.

3.3.8 DDoS

Реалізовувати дану атаку ми будемо завдяки програмі LOIC версії 1.0.8. Скачати її можна за посиланням : <https://sourceforge.net/projects/loic/files/latest/download>

Інтерфейс програми зображено на рис. 3.26

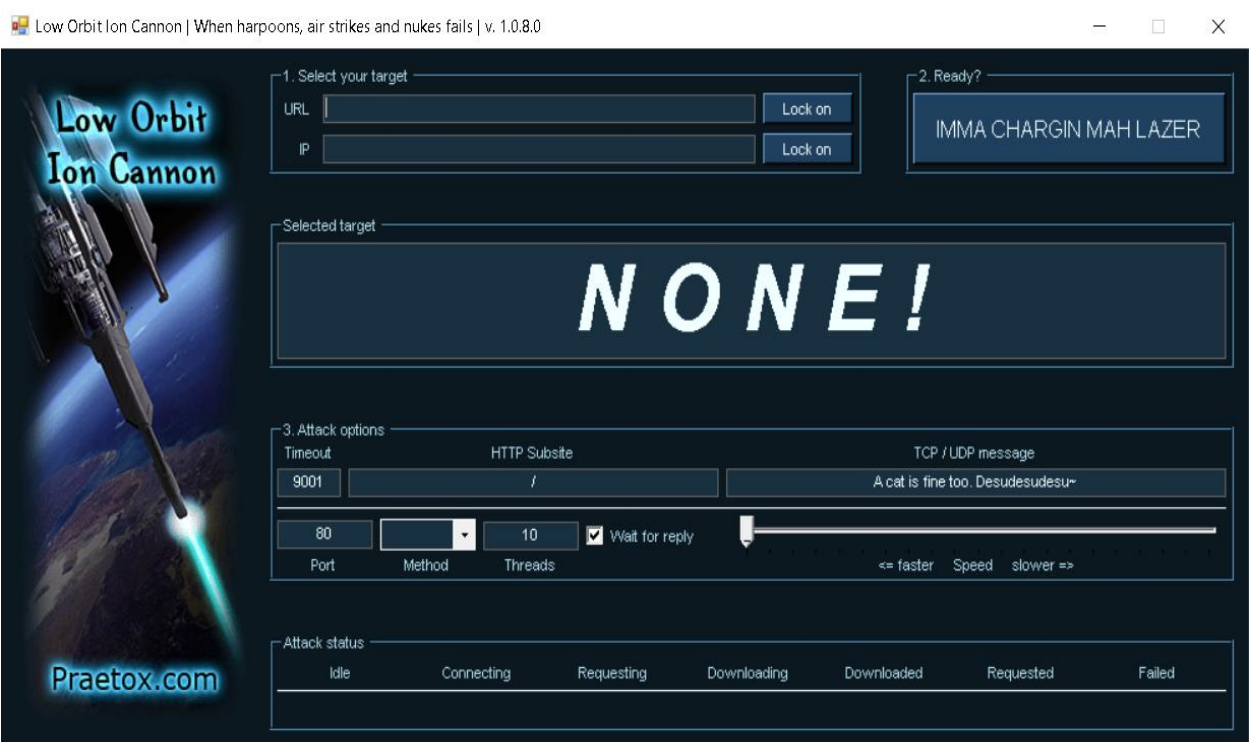


Рис. 3.26 Програма Loic

Для DDoS атаки потрібно ввести URL або IP адресу, далі по стандарту, крім метода. В методі вибираємо пункт UDP. Як показано на рис 3.27

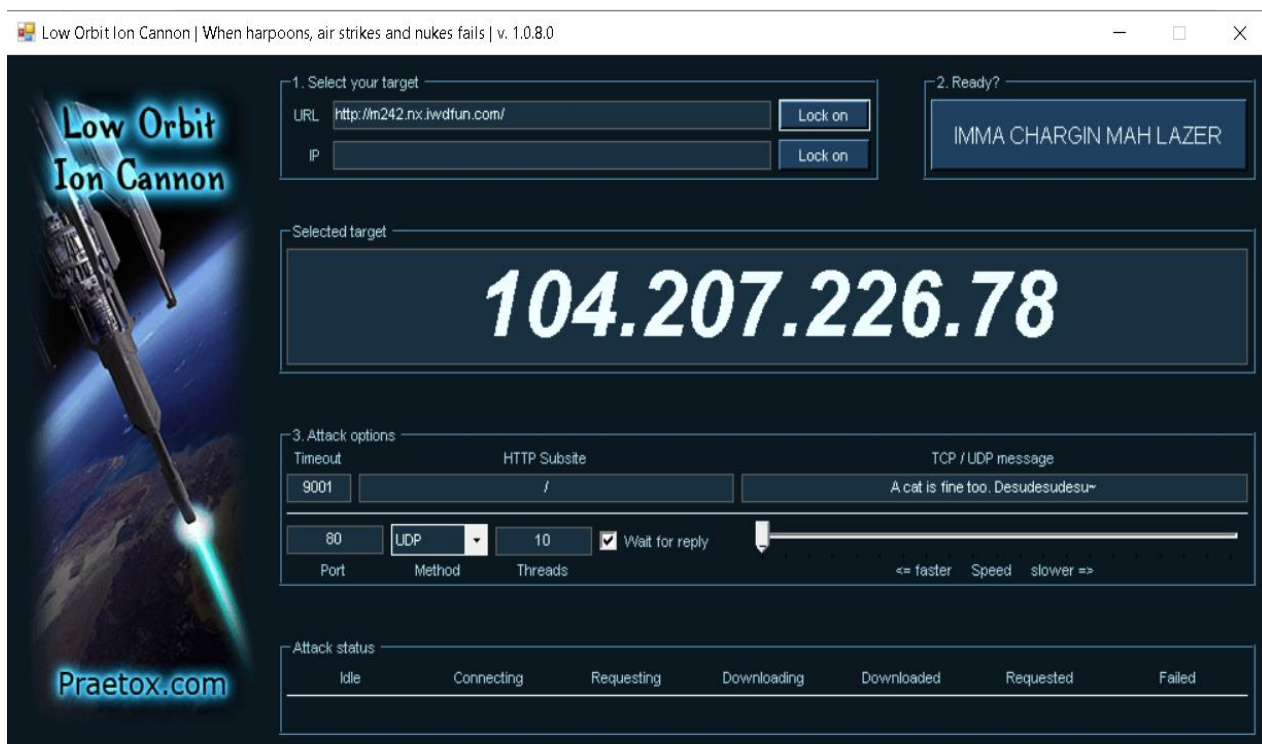


Рис. 3.27. Налаштування програми LOIC

Після того, як налаштували програму, запускаємо атаку.

DDoS атака не спрацювала, сторінка сайту відкривається, повільного робочого процесу сайту не спостерігається. Це зображено на рис. 3.28 і рис. 3.29.



Low Orbit
Ion Cannon

Praetox.com

1. Select your target

URL Lock on

IP Lock on

2. Ready?

Stop flooding

Selected target

104.207.226.78

3. Attack options

Timeout

9001

HTTP Subsite

/

TCP / UDP message

A cat is fine too. Desudesudesu~

80

UDP

10

☒ Wait for reply

<= faster

Speed

slower =>

Port

Method

Threads

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
						1730499

Рис. 3.28. Запуск програми

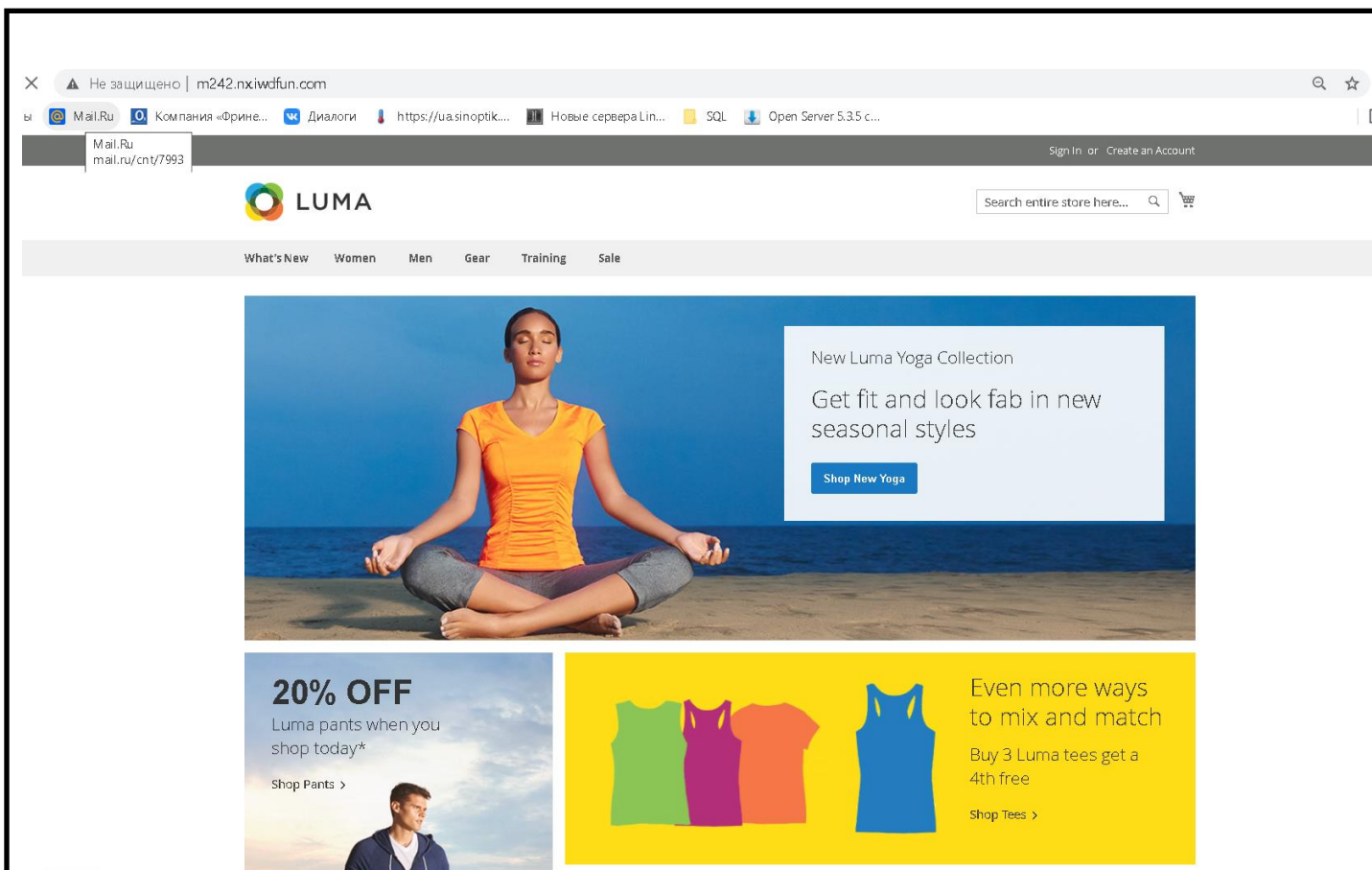


Рис. 3.29. Стан сайту після DDoS атаки

Отже, серверна частина сайту добре захищена від подібних атак. Але, якщо зловмисник буде використовувати більше серйозні інструменти, то все ж таки сайт припинить роботу; або таких зловмисників буде декілька, і одночасно спрямувати атаку на веб-ресурс.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

Висновки до третього розділу

Досліджено принцип роботи системи керування Magento. Реалізований захист від різних типів веб-атак. В розрізі чого ми побачили, за рахунок чого і як відбуваються веб-атаки, на що слід звернути увагу, і як захистити веб-ресурс від шкідливих запитів.

Було продемонстровано прості спроби взлому веб-сайту, від яких Magento має певну роль в захисті. Велику перевагу CMS має в захисті від шкідливих запитів по типу Request, що зважаючи на статистику таких атак, дає можливість побачити безліч переваг в вхідних даних від користувачів чи ботів.

В результаті чого можна сказати, що використання платформи Magento має свої переваги з точки зору безпеки веб-ресурсу. Також має значний вплив на безпеку використання цієї платформи налаштування серверної частини сайту.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

ВИСНОВКИ

При написанні дипломної роботи зроблено наступне :

1. Проаналізовано найпоширеніші веб-атаки, та розглянуто вразливості, які можуть бути використанні для проведення цих атак.

Досліджено веб-атаки та уразливості які можуть використовуватись для реалізації цих атак, також були розглянуті статистичні дані, щодо веб-атак які відбулися в наслідок епідемії COVID-19, які наслідки були в результаті проведених злочинних дій та які сфери найбільш привабливі для веб-злочинців.

Також, було наголошено на тому, що необхідно бути досить уважним до деталей веб-додатку, адже кожна маленька вразливість може призвести до великих втрат.

2. Дослідженні методи захисту від веб-атак, та можливі засоби моніторингу стану захищеності веб-додатків, та вразливості які можуть призвести до вдалих веб-атак, а саме було наведено частини вразливого коду веб-додатків до веб-атак. Була наведена порівняльна статистика, щодо захисту від кібер злочинців в Україні.

Визначено, що навіть одна не вірна команда, що використовується в коді певного веб-додатку може звести всю безпеку ресурсу нанівець, тому слід бути обачним.

Підсумовуючи сказане, розробники ПЗ не завжди мають змогу вчасно вжити заходів щодо усунення вразливостей і випуску оновлень.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

Тому, щоб ефективно протистояти злочинцям, необхідно спостерігати і запобігати атакам на користувачів, аналізувати і зіставляти безліч подій для виявлення ланцюжків атак, виявляти експлуатація вразливостей нульового дня. Зазначенні заходи дозволять своєчасно зупинити зловмисників.

3. Продemonстровано принцип роботи системи керування Magento.

Реалізований захист від різних типів веб-атак. В розрізі чого ми побачили, за рахунок чого і як відбуваються веб-атаки, на що слід звернути увагу, і як захистити веб-ресурс від шкідливих запитів.

Було продемонстровано прості спроби взлому веб-сайту, від яких Magento має певну роль в захисті. Велику перевагу CMS має в захисті від шкідливих запитів по типу Requests, де опираючись на статистику, дає можливість побачити безліч переваг в вхідних даних від користувачів чи ботів.

В результаті чого можна сказати, що використання платформи Magento має свої переваги з точки зору безпеки веб-ресурсу. Також має значний вплив на безпеку використання цієї платформи настройка серверної частини сайту.

4. Ілюстровано статистичні дані.

Зміни кібератак протягом року із-за пандемії, завдяки чому з'явилися нові методи фішингу. Відповідно до галуз, найбільша увага припадала на охорону здоров'я, де були спрямовані атаки на користувачів, завдяки теми про коронавірус, В розрізі чого показано, що деякі галузі мають більший вплив кібератак в Україні.

Якщо підсумувати, усе вище написане, можна зробити висновок, що CMS Magento, а саме версія 2.2, досить добре захищена від атак.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

Зазначено, що однією з важливих переваг Magento є її легкість в розумінні. Весь інтерфейс інтуїтивно зрозумілий. Тож можна сміливо рекомендувати для використання систему керування контентом Magento.

Підкреслено, що якщо досвідчений хакер буде атакувати сайт побудований завдяки CMS Magento, то звісно він найде способи взлому. Однак, не зважаючи на це, від найбільш поширених атак все ж таки Magento захищає.

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

ПЕРЕЛІК ПОСИЛАНЬ

1. Об'єкти захисту інформації та технічні канали її витоку [Електронний ресурс]. –Режим доступу: World Wide Web. – URL: <https://infopedia.su/1x978f.html>
 2. Мережеві атаки, можливості та недоліки мережевих екранів [Електронний ресурс]. –Режим доступу: World Wide Web. – URL <https://ukrbukva.net/page,2,91957-Setevye-ataki-vozmozhnosti-i-nedostatki-setevyh-ekranov.html>
 3. Типи мережевих атак, їх опису, засоби боротьби [Електронний ресурс]. – Режим доступу: World Wide Web. – URL <https://moluch.ru/conf/tech/archive/5/1115/>
 4. Мережеві атаки, можливості та недоліки мережевих екранів [Електронний ресурс]. –Режим доступу: World Wide Web. – URL <https://ukrbukva.net/page,6,91957-Setevye-ataki-vozmozhnosti-i-nedostatki-setevyh-ekranov.html>
 5. XSS-атаки [Електронний ресурс]. – Режим доступу: <http://www.univd.edu.ua/science-issue/issue/3345>
 6. IP-спуфінг [Електронний ресурс]. – Режим доступу: <http://um.co.ua/11/11-3/11-30168.html>
 7. Брутфорс [Електронний ресурс]. – Режим доступу: <https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2018/>
 8. Аналіз існуючих інформаційних атак на веб-ресурси та методів і засобів захисту від них [Електронний ресурс]. – Режим доступу: <http://refua.in.ua/analiz-isnuyuchih-informacijnih-atak-na-veb-resursi-ta-metodiv.html>
- Аналіз сучасних Web-вразливостей [Електронний ресурс]. – Режим доступу: <http://www.rusnauka.com/pdf/255343.pdf>

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

Безпека і переповнення буфера [Електронний ресурс]. – Режим доступу: <http://pautina34.ru/p=167/>

9. Безпека комп'ютерних мереж [Електронний ресурс]. – Режим доступу: <https://svitppt.com.ua/informatika/bezpeka-kompyuternih-merezh.html>

10. Класифікація мережевих атак [Електронний ресурс]. – Режим доступу: <https://asyan.org/potre/%D0%9A%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F+%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D1%85+%D0%B0%D1%82%D0%B0%D0%BAe/main.html>

11. Захист баз даних [Електронний ресурс]. – Режим доступу: <http://ua.waykun.com/articles/zahist-baz-danih-2-stattja-storinka-7.php>

12. Актуальні питання протидії кіберзлочинності та торгівлі людьми. [Електронний ресурс]. – Режим доступу: <http://www.univd.edu.ua/science-issue/issue/3345>

13. Оцінка стійкості роботи комп'ютерної інформаційної системи в умовах дії загрозливих чинників НС [Електронний ресурс]. – Режим доступу: https://studwood.ru/2388680/informatika/otsinka_stiykosti_roboti_kompyuternoyi_informatsionoyi_sistemi_umovah_zagrozlivih_chinnikov

14. Як захистити веб-додатки: основні поради, інструменти, корисні посилання [Електронний ресурс]. – Режим доступу: <https://echo.lviv.ua/dev/6231>

15. Використання інформаційно-комунікаційних технологій у професійній діяльності освітян [Електронний ресурс]. – Режим доступу: <https://repository.kristti.com.ua/wp-content/uploads/2017/07/Tkach-Vordpres.pdf>

16. Огляд CMS Magento [Електронний ресурс]. – Режим доступу: <http://jak.koshachek.com/articles/ogljad-cms-magento-dvizhka-dlja-stvorennja.html>

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		98

17. Magento CMS – одна из самых мощных платформ для создания интернет магазина [Электронный ресурс]. – Режим доступа: World Wide Web. – URL: <http://www.shop-script.su/korobochnye/magento>

18. Компьютер76 //DDOS атака [Электронный ресурс]. – Режим доступа: <https://computer76.ru/2015/04/24/ddos-ataka>

19. LDAP injection [Электронный ресурс] – Режим доступа: https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html

20. Захист від кібератак [Электронный ресурс] – Режим доступа : <https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-zashchititsya-ot-kiberatak/>

21. Аналіз і методи захисту веб-додатків від атак типу XSS [Электронный ресурс] – Режим доступа : <https://cyberleninka.ru/article/n/analiz-i-metody-zaschity-web-prilozheniya-ot-atak-tipa-xss>

22. Безпека веб-додатків Django [Электронный ресурс] – Режим доступа : https://developer.mozilla.org/ru/docs/Learn/Server-side/Django/web_application_security

23. Безпека веб-додатків : міфи і реальність [Электронный ресурс] – Режим доступа : https://www.anti-malware.ru/analytics/Technology_Analysis/web-security-myths-and-reality

24. Як захистити веб-портал від інформаційних атак [Электронный ресурс] – режим доступа : <https://www.dialognauka.ru/press-center/article/4764/>

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

25. Що таке WAF, або захищаєм сайти і веб-додатки від DDoS-атак
[Електронний ресурс] –

<https://channel4it.com/publications/CHto-takoe-WAF-ili-zashchishchaem-sayty-i-prilozheniya-ot-DDoS-atak-33271.html>

		Кулик Д.А.			КІ.КР.Б – 123 -21 - ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		100