**Міністерство освіти і науки України  
Дніпровський національний університет   
імені Олеся Гончара**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Кафедра компʼютерних технологій**

Лабораторна робота №1

«**Захист інформації**»

Укладачі:

канд. техн. наук, доц. К.Є. Золотько,

ст. викл. Д.В. Красношапка,

асист. С.Ф. Сірик.

*Ухвалено на вченій раді ФПМ*

*протокол № 6*

*від 22 травня 2022 р.*

**Дніпро**

**ДНУ**

**2023**

Зміст

[Політика безпеки Web-сайту 3](#_Toc148557819)

## Політика безпеки Web-сайту

***Модель зловмисника***

Людина або кампанія, яка здійснює різноманітні атаки з метою отримання особистих даних, поширення монетизованої реклами, збільшення пропускної здатності бот-мереж за допомогою пропускної датності власника сайту.

***Цілі зловмисника***

Зловмисник може атакувати, якщо йому цікава інформація користувачів системи. Він може мати такі цілі:

* бажання отримувати гроші за переходи користувачів на певні посилання, що закодовані у коді сайту;
* бажання спаплюжити думку про власника сайту;
* бажання отримати грошову винагороду за повернення «чистої» резервної копії сайту.

***Цілі захисту***

Основною метою цієї Політики є захист конфіденційної інформації користувачів від несанкціонованого доступу та від можливого нанесення їм моральної, матеріальної чи будь-якої іншої шкоди.

***Можливі атаки на систему***

***SQL-ін’єкція*** – це вид атаки на веб-додатки, при якій зловмисник впроваджує шкідливі SQL-запити у вхідні дані, що передаються до бази даних. Це відбувається тоді, коли веб-додаток належним чином не перевіряє або не екранує вхідні дані, дозволяючи зловмиснику впровадити додатковий SQL-код у запити до бази даних.

***XSS-атака*** - це вид атаки на веб-додатки, при якій зловмисник вставляє шкідливий код на веб-сторінку, який потім виконується у браузері користувача.

***Brute-Force атака*** - це метод зламу, при якому зловмисник систематично намагається перебрати всі можливі комбінації паролів, доки не знайде правильний пароль або не отримає несанкціонований доступ до облікового запису чи системи. У цьому методі атаки використовується автоматизований скрипт або програма, яка послідовно перебирає можливі комбінації паролів шляхом спроб входу.

***Атака типу «відмова в обслуговуванні» (DDoS)*** - це спроба завдати шкоди, зробивши недоступною цільову систему, наприклад веб-сайт або додаток, для звичайних кінцевих користувачів. Зазвичай зловмисники генерують велику кількість пакетів або запитів, які в кінцевому рахунку перевантажують роботу цільової системи. Для здійснення атаки типу «розподілена відмова в обслуговуванні» (DDoS) зловмисник використовує безліч зламаних або контрольованих джерел.

***Реалізація атаки. Програмне забезпечення***

***Реалізація атаки SQL-ін’єкція***. На жаль, CMS системи мають широку популярність серед non-code спільноти, що не вимагає великих зусиль від х . Хакер використовує шкідливий код шляхом надсилання його у вразливе поле або параметр URL-адреси. Успіх шкідливого коду полягає у низькій програмі безпеки обробки та перевірки даних базою даних.

***Програмне забезпечення для атаки*** ***«підслуховування (sniffing)».***

***Wireshark:***

Захоплення і аналізатор пакетів з відкритим вихідним кодом. Він підтримує Windows, Linux і т. Д. І є інструментом на основі графічного інтерфейсу (альтернатива Tcpdump). Він використовував pcap для відстеження та захоплення пакетів з мережевого інтерфейсу. Пакети можна фільтрувати по IP, протоколу та багатьма іншими параметрами. Пакети можуть бути згруповані або позначені на основі релевантності. Кожен пакет можна вибрати і проаналізувати відповідно до потреб.

***Debookee:***

Це платний інструмент, який можна використовувати для моніторингу та аналізу мережі. Він може перехоплювати і аналізувати трафік від пристроїв, що знаходяться в цій підмережі, незалежно від типу пристрою (ноутбук, пристрої, телевізор і т. Д). Він пропонує різні модулі:

* Модуль мережевого аналізу: сканування підключених пристроїв, перехоплення трафіку в підмережі, сканер TCP-портів, мережевий аналіз та моніторинг протоколів HTTP, DNS, TCP, DHCP, аналіз викликів VoIP і т. Д.
* Модуль моніторингу Wi-Fi: відомості про точках доступу в радіодіапазоні, відомості про бездротові клієнтів, статистика Wi-Fi і т. Д.
* Модуль дешифрування SSL / TLS: підтримка моніторингу та аналізу захищених протоколів.

***Реалізація XSS-атаки.***  Голосовий фішинг (voice phishing) реалізується за допомогою дзвінка через телефон або будь-яку систему голосового спілкування. Вішинг зазвичай передає автоматичне голосове повідомлення нібито від легітимного осередку (наприклад, ваш банк або державна установа).

Зловмисники можуть заявити, що ви заборгували велику суму грошей, термін дії вашої автостраховки Текст ваша кредитна карта має підозрілу активність, яку необхідно негайно виправити. У цей момент жертві зазвичай говорять, що вона повинна надати особисту інформацію, таку як облікові дані кредитної картки або номер соціального страхування, щоб підтвердити свою особу, перш ніж отримати додаткову інформацію і вжити будь-які дії.

***Програмне забезпечення для вішингу.***

Вішинг являє собою різновид фішингу та реалізується з використанням war diallers (автонабірателей), а також інтернет-телефонії (VoIP).

***Реалізація атаки розпорошення паролів.*** Метод атаки приймає велику кількість імен користувачів і зациклює їх за допомогою одного пароля. Можна використовувати декілька ітерацій, використовуючи кілька різних паролів. Але кількість спроб введення пароля зазвичай невелика в порівнянні з кількістю спроб користувача. Цей метод дозволяє уникнути блокувань паролем. І він часто більш ефективний для виявлення слабких паролів, ніж для конкретних користувачів.

Для успіху атаки паролем необхідний гарний список паролів. Можна використовувати певні інструменти, такі як CEWL. Для створення списків конкретних цілей відповідно, використовуючи слова з веб-сайтів або придумати свій власний метод. У минулому був великий успіх, використовуючи MonthYear, welcome1 і organization1, а також прості паролі, такі як qwerty12345 та інші.

Зловмисники зазвичай, після успішного отримання списку дійсних користувачів від дійсних контролерів домену, використовують свої знання загальних паролів і пробують ОДИН ретельно продуманий пароль проти ВСІХ відомих облікових записів користувачів. (Один пароль для багатьох облікових записів). Якщо атака не вдалася з першої спроби, то зловмисники спробують знову використовувати інший пароль. Як правило, чекаючи близько декількох хвилин або близько того між спробами, щоб не викликати будь-які пороги блокування облікового запису на основі часу.

***Програмне забезпечення для*** ***атаки розпорошення паролів***

Існує безліч програмних інструментів для злому паролів, але найпопулярнішими є Aircrack, Cain and Abel, John the Ripper, Hashcat, Hydra, DaveGrohl і ElcomSoft. Багато пакетів програмного забезпечення для підтримки судових розглядів також включають функцію злому паролів. Більшість з цих пакетів використовують поєднання стратегій злому, алгоритмів з використанням грубої сили і словникових атак, що виявляється найбільш продуктивним.

Aircrack-ng - це набір мережевого програмного забезпечення, що складається з детектора, аналізатора пакетів, зломщика WEP і WPA / WPA2-PSK і інструменту аналізу для бездротових локальних мереж стандарту 802.11. Він працює з будь-яким контролером бездротового мережевого інтерфейсу, драйвер якого підтримує режим прямого моніторингу і може прослуховувати трафік 802.11a, 802.11b і 802.11g. Програма працює під Linux, FreeBSD, macOS, OpenBSD і Windows.

John the Ripper - це безкоштовний програмний інструмент для злому паролів. Спочатку розроблений для операційної системи Unix, він може працювати на п'ятнадцяти різних платформах (одинадцять з яких є архітектурно-залежними версіями Unix, DOS, Win32, BeOS та OpenVMS). Це одна з найбільш часто використовуваних програм перевірки і злому паролів, оскільки вона об'єднує декілька зломщиків паролів в один пакет, автоматично визначає типи хеш паролів і включає свій програмний зломщик, який можна настроїти.

CeWL (Custom Word List generator, тобто генератор призначеного для списку слів) - це додаток на основі Ruby, яке переглядає вказану URL-адресу до зазначеної глибини і повертає список слів, який потім може використовуватися для зломщиків паролів. При бажанні CeWL може переходити за зовнішніми посиланнями.

***Реалізація атаки «людина посередині».*** В даному прикладі ми розглянемо атаку на SSL через HTTP, також відомого як HTTPS, оскільки це найпоширеніша модель реалізації протоколу SSL і використовується практичних у всіх системах банківських мережевих додатків, службах електронної пошти для забезпечення шифрування каналу зв'язку. Ця технологія покликана забезпечити збереження даних від перехоплення третіми особами за допомогою простого аналізатора пакетів.

Розглянемо процес комунікації по HTTPS на прикладі підключення користувача до облікового запису на Google. Цей процес включає в себе кілька окремих операцій:

* Клієнтський браузер звертається до http://mail.google.com на порт 80 за допомогою HTTP.
* Сервер перенаправляє клієнтську HTTPS-версію цього сайту, використовуючи HTTP code 302 перенаправлення.
* Клієнт підключається до https://mail.google.com на порт 443.
* Сервер пред'являє клієнту свій сертифікат відкритих ключів для перевірки автентичності сайту.
* Клієнт звіряє даний сертифікат зі своїм списком довірених центрів сертифікації.
* Створюється зашифроване з'єднання.

З усіх цих дій найбільш вразливою бачиться операція перенаправлення на HTTPS через код відповіді HTTP 302. Для здійснення атаки на точку переходу від незахищеного до захищеного каналу був створений спеціальний інструмент SSLStrip. З використанням даного інструменту процес атаки виглядає наступним чином:

* Перехоплення трафіку між клієнтом і веб сервером.
* У момент виявлення HTTPS URL адреси інструмент SSLstrip підміняє його HTTP-посиланням, зіставляючи всі зміни.
* Атакуюча машина надає сертифікати веб-сервера і уособлює клієнта.
* Трафік приймається з захищеного веб-сайту і надається клієнтові.

В результаті чого атакуючий отримує доступ до даних, які клієнт відправляє на сервер. Ними можуть бути паролі від облікових записів, номери банківських карт або будь-яка інша інформація, яка зазвичай передається в прихованому вигляді. Потенційним сигналом проведення даної атаки для клієнта може стати відсутність позначення захищеного HTTPS-трафіку в браузері. Для сервера же така підміна залишиться зовсім непоміченою, тому що немає ніяких змін в SSL-трафіку.

***Програмне забезпечення для*** ***атаки «людина посередині»***

***Принцип атаки «відмова в обслуговуванні»***.

***Програмне забезпечення для атаки «відмова в обслуговуванні»***

Найпоширенішою програмою є LOIC. Цей є у відкритому доступі і будь-який бажаючий може його скачати і використовувати.

Ця програма розрахована для Ddos-атак, коли вам заздалегідь відомий IP і URL атакується ресурсу. Щоб скористатися даною програмою, потрібно:

* Знайти та завантажити її з інтернету, вона там є у відкритому доступі.
* Активувати цей додаток за допомогою файлу «loic.exe».
* Ввести в відкритих полях IP і URL ресурсу, який потрібно атакувати.
* Відрегулювати рівень передачі запитів.
* Натиснути для старту кнопку «imma chargin mah lazer».

Звичайно, запуском однієї такої програми з одного комп'ютера ви, швидше за все, не зможете нашкодити ресурсу, тому що у нього спрацює його система безпеки. Але якщо буде багато запущених програм на один ресурс, наприклад 10, 100, то цілком можливо вивести ресурс зі строю.

***Захист від атак***

***Захист від SQL-ін’єкції***. Необхідно дотримуватись наступних правил:

* ліміт на надання прав доступу до бази даних;
* своєчасне оновлення ядра WordPress, та її додатків(плагінів, теми, ПХП версії і тд);
* використання перевірених, а також плагінів безпеки (Wordfence, Sucuri Security);
* вимкнення відображення «дебаг» опції;
* вимкнення лістінгу директорій/файлів інсталяції;
* застосування коректних прав доступу до файлів/директорій;
* регулярне оновлення та використання лише надійних паролей;
* підключення фаєрволу (за можливості).

***Захист від XSS-атаки.*** Основний способи захисту є наступними:

* встановлення фаєрволу з серверної сторони (CSF, IPTables, Mod Security);
* встановлення фаєрволу на рівні додатку (Wordfence, Sucuri Security);
* використання Cloudflare;
* фільтрація HTTP запитів;
* створення чорного списку для певних типів запитів;
* створення двофакторної аутентифікації для доступу до файлів сайту;
* регулярно перегляди логи доступу на сервер.

***Захист від атаки «людина посередині» (Man-in-the-Middle).***

***Захист від атаки типу «відмова в обслуговуванні» (DDoS)***

***Захист від атаки розпорошення паролів***.