ДОДАТОК А ЛАБОРАТОРНА РОБОТА №2 «КОНФІГУРАЦІЯ ПАРАМЕТРІВЗАХИСТУВЕБ-СЕРВЕРУ»

Метою лабораторної роботи є оволодіння практичними навичками налаштування базових параметрів захисту веб-сторінок за допомогою стандартних засобів веб-сервераApache.

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитись із розділами навчального посібника, що присвячені засобам налаштування базових параметрів захисту веб-серверу Apache.

Завдання на лабораторну роботу:

1. Заборонити перегляд структури всіх веб-документів.
2. Заборонити доступ до всіх ресурсів.
3. Заборонити перехід веб-сервера по символьним посиланням.
4. Обмежити параметрTimeout величиною45 секунд.
5. Мінімізувати службову інформацію.
6. Обмежити обсяг файлів, які можливо завантажити на веб-сервер величиною1 МБ.
7. Встановити,що час очікування наступного запиту перед розривом з’єднання дорівнює 15 секунд.
8. Встановити,що максимальна кількість одночасно підтримуваних запитів наодне з'єднаннядорівнює200.
9. Заборонити запуск програм в теці з веб-документами .10. Заборонити підтримку директив в файлах. htaccess.

11. Заборонити доступ до кореневої теки веб-документів з доменного імені www.rrr.ua таIP-адрес172.16.16.0 і172.16.16.8.

12. Дозволити доступ до теки АААзIP-адреси127.0.01 тільки користувачеві use raaa. Пароль – 1111.

13. Використати базовий тип перевірки парольних даних.

14. Дозволити доступ до текиBBBзIP-адреси127.0.01 тільки користувачеві userbbb.Пароль – 2222. Використати цифровий тип перевірки парольних даних.

15. Зняти всі обмеження доступу до теки CCC.

16. Встановити файл *q.html*в якості головного файлу директорії CCC.16.Заборонити доступ до файлу CCC методом POST.

17. Заборонити доступ всіх користувачів веб-серверу до файлу *myf.html*, розміщеному в теці AAA.

18. Заборонити доступ всіх користувачів веб-серверу дотеки DDD.

19. Дозволити доступ всіх користувачів до файлу *rrr.htm*, розміщеному в теці DDD.

20. Визначити файлу. *Html* в якості відповіді веб-серверу при виникненні помилки(зверненні до неіснуючого файлу).

21. Використовуючи метод підбору паролю пословнику спробувавти підібрати пароль до текиAAA. Визначити термін підбору.

22. Використовуючи метод підбору паролю пословнику спробувати підібрати пароль до теки BBB. Визначити термін підбору.

23. Використовуючи метод повного перебору підібрати пароль до текиAAA. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки. Визначити термін підбору для кількості потоків 1,5,20,50.

24. Використовуючи метод повного перебору підібрати пароль до теки BBB. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки.

25. Визначити термін підбору для кількості потоків 1,5,20,50.

Хід виконання роботи

1. Підготовчі роботи:

Перед виконанням лабораторної роботи слід ознайомитись із матеріалами лабораторного практикуму, що присвячені засобам безпеки та засобам перевірки стійкості парольного захисту веб-серверу Apache.

– В теці F:\int\home\localhost\www створює всі теки і файли потрібні для виконання лабораторних завдань. Це теки AAA,BBB,CCC,DDDтафайли*q.html*,*rrr.html* та*y.html*.

– В теках AAA, BBB, CCC, DDD створити файли *index.html* зміст яких відповідає назві теки та назві файлу. Наприклад, на (рис.А.1) показано змістфайлу*index.html*,щорозміщений втеціAAA.

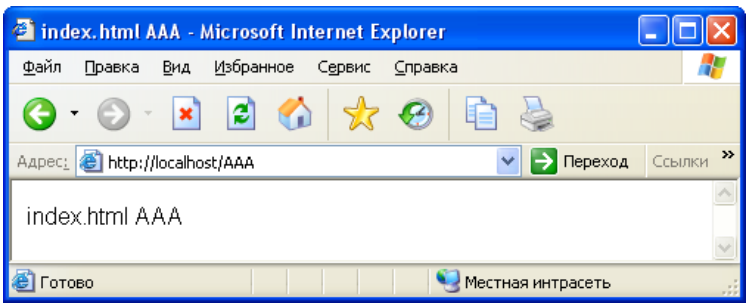


Рисунок А.1 – Відображення файлу index.html,розміщеного в теці AAA

– Записати в файл *q.html*(розміщенийвтеціCCC) текст "q.htmlCCC".

– Записати в файл *rrr.html* (розміщений в теці DDD) текст " rrr.html DDD".

– Записати в файл *myf.htm* (розміщений в теці AAA) текст " myf.htmlAAA".

– Записати в файл *y.html*(розміщенийвтеціAAA) текст" Поганий запит".

2. Виконання кожного наступного пункту завдання лабораторної роботи містить однотипні етапи:

– Параметри записуються в конфігураційний файл веб-серверу– *http.conf*.

– Після запису файл *http.conf* слід зберегти *http.conf*,веб-сервер перезапустити та перевірити коректність виконання пункту завдання.

3. Для заборони перегляду структури всіх веб-документів в секції

<Directory"F:/int/home/localhost/www">слід записати

Options–Indexes

4. Для демонстрації заборони перегляду структури необхідно:

– Знищити файл *index.html*,

– В адресному рядку браузера набрати http://localhost/.

Очікувана відповідь веб-сервера показанана (рис.А.2)

5. Для заборони доступу до всіх ресурсів за межами теми з веб-документами слід виправити параметри секції <Directory/>:

<Directory

/>AllowOverr

ide

NoneOrder

deny,allowDeny

fromall

</Directory>

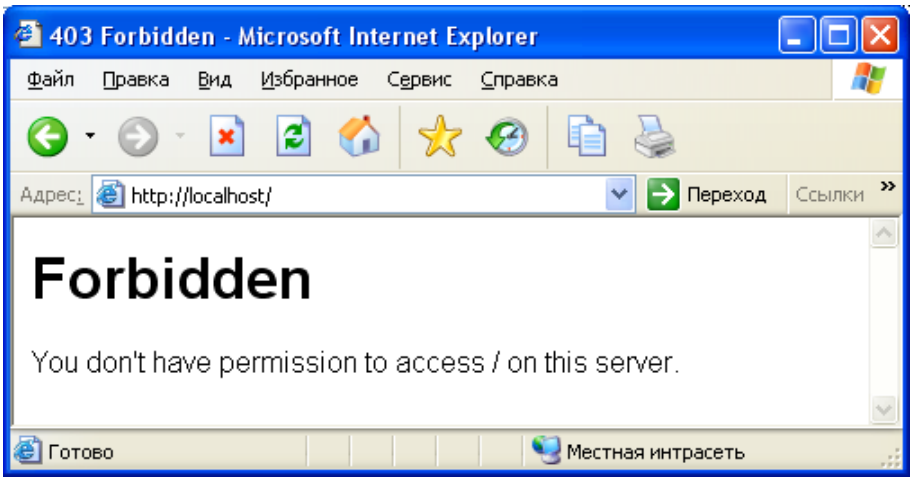


Рисунок А.2 – Заборона перегляду структури веб-сайту

6. Для заборони переходу по символьним посиланням слід в секції <Directory"F:/int/home/localhost/www">знищити рядок

OptionsIndexesFollowSymLinks

7. Для виконання послідовного виконання завдань 4–8 слід в кінці файлу *httpd.conf* слід записати:

Timeout45 Server

Signature Off Server

Tokens Prod Limit

Request Body

1048576

KeepAliveTimeout15

MaxKeep Alive Requests 200

8. Для заборони запуску програм в теці звеб-документами та заборони підтримки директив в файлах. *htaccess* необхідно пересвідчитись , що в секції <Directory" F:/int/home/localhost/www"> є наступні рядки:

Options

IncludesNOEXECAl

lowOverridesNone

9. Для заборони доступу до кореневої теки веб-документів здоменного імені www.rrr.uataIP-адрес 172.16.16.0i172.16.16.8 в секції <Directory "F:/int/home/localhost/www"> після рядка:

Allowfromall

Слід записати:

Denyfromwww.rrr.ua,172.16.16.0,172.16.16.8

10. Після тегу кінця секції <Directory "F:/int/home/localhost/www">

</Directory>записати:

<Directory

"F:/int/home/localhost/www/aaa">Or

derdeny,allow

Deny fromall

Allowfrom127.0.0.1

AuthUserFile

"C:/Program Files/Apache SoftwareFoundation/Apache2.2/bin/pfile"

AuthName

"useraaa"Auth

Type

Basicrequireva

lid-user

</Directory>

11.За допомогою команд"Пуск□Выполнить□cmd"операційної системи Windows відкрити вікно командного рядка та послідовно виконати інструкції показані на (рис.А.3) При цьому пароль – 1111, а парольні дані записуються в файл– *pfile*.

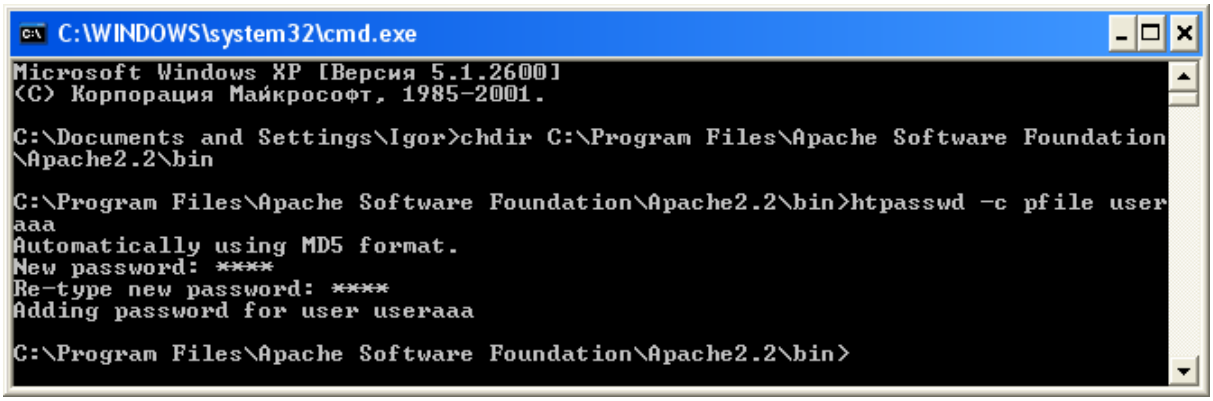


Рисунок А.3– Створення файлу з парольними даними

Зазначимо, що при спробі доступу з IP-адреси 127.0.0.1 до текиhttp://localhost/aaa/перед користувачем повинно з’явитись показане на (рис.А.4) вікно вводу парольних даних. Тека стане доступною тільки після вводу вполе"Пользователь"–useraaa,авполе"Пароль"–1111.Таким чином реалізація пп.10,11 відповідає за виконання дванадцятого завдання роботи.

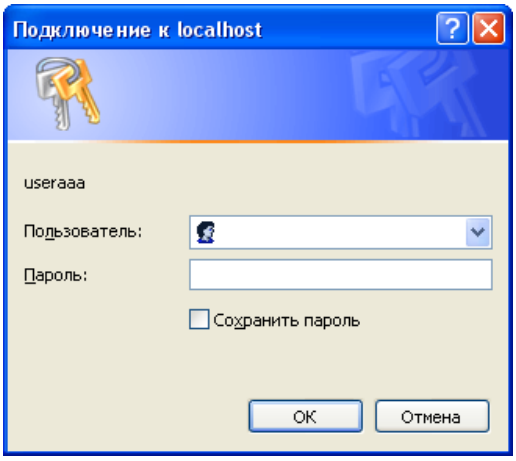


Рисунок А.4 – Вікно вводу парольних даних при базовій авторизації

12. Для підключення модулю підтримки цифрової авторизації в файлі

httpd.conf слід замінити

на

#LoadModuleauth_digest_modulemodules/mod_auth_digest.so

на

LoadModuleauth_digest_modulemodules/mod_auth_digest.so

13. Після тегу кінця секції <Directory "F:/int/home/localhost/www/bbb">

</Directory>записати:

<Location
/bbb/>Ord
er

ny,allowDeny fromall

Allow from
127.0.0.1

AuthType
DigestAuthNa
me"bbb"

AuthDigestDomain /bbb/ http://
127.0.0.1/bbb/AuthDigestProvider file

AuthUserFile "C:/Program Files/Apache SoftwareFoundation/Apache2.2/bin/.hhh"

Requirevalid-user

</Location>

14. За допомогою команд "Пуск□Выполнить□cmd"операційної системи Windows відкрити вікно командного рядка та послідовно виконати інструкції показані на (рис.А.5) При цьому, пароль – 2222 а парольні дані записуються в файл– *.hhh*.

Зазначимо, що при спробі доступу з IP-адреси 127.0.0.1 до текиhttp://localhost/bbb/ перед користувачем повинно з’явитись показане на (рис.А.6) вікно вводу парольних даних. Тека стане доступною тільки після вводу вполе "Пользователь"–userbbb,авполе"Пароль"–2222.Таким чином реалізація пп.12–14 відповідає за виконання завдання№13.

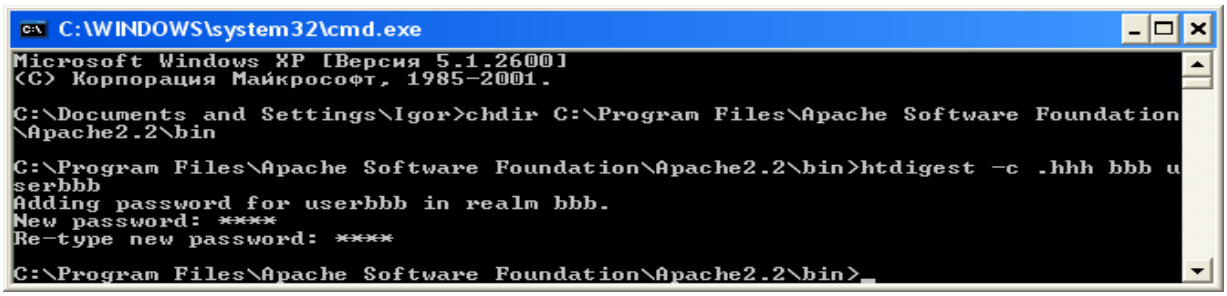


Рисунок.А.5 – Створення файлу з парольними даними для цифрової авторизації

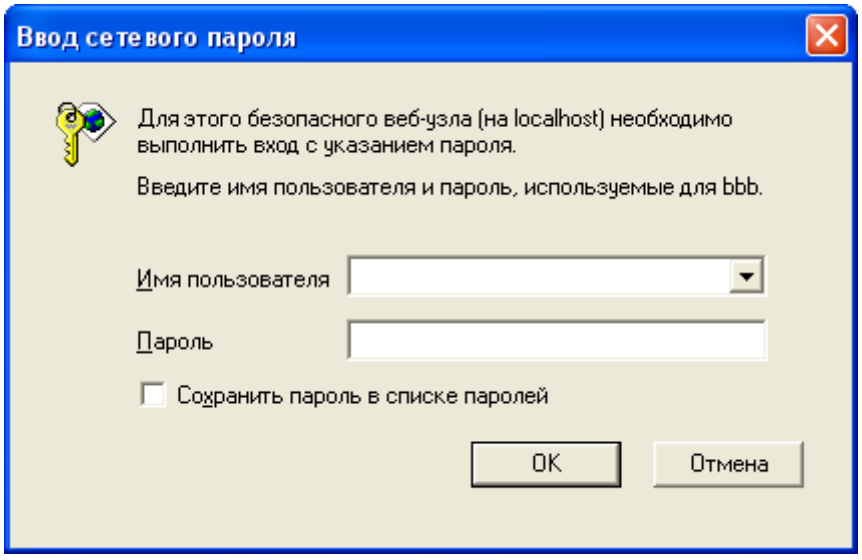


Рисунок А.6 – Вікно вводу парольних даних при цифровій авторизації

15. Для того,щоб зняти всі обмеження доступу до теки CCC після тегу кінця секції *<Location/bbb/></Location>* слід записати:

<Directory"F:/int/home/localhost/www/ccc">

Order

deny,allow

allowfroma

ll

</Directory>

Зазначимо,що таким чином були перевизначені обмеження доступу задані для корневої текивеб-документів.

Пересвідчимось,що при доступі до теки *CCC* відкривається файл *index.html*(див.рис.А.7).

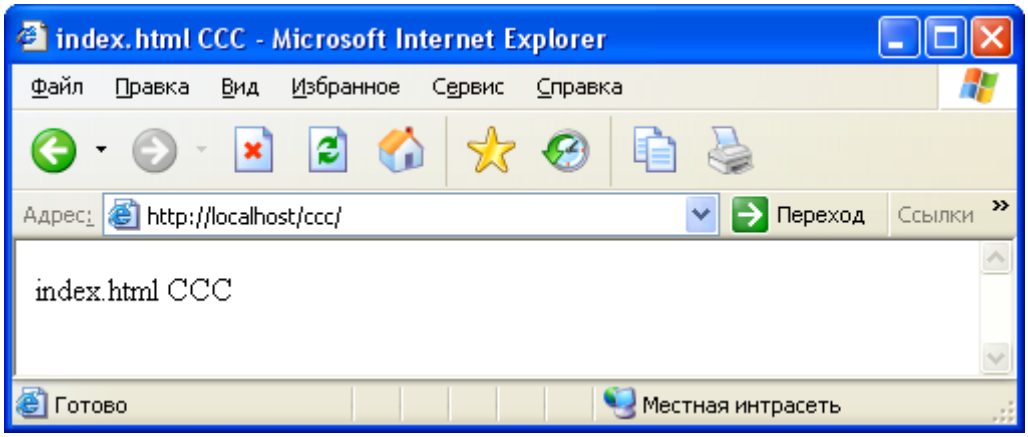


Рис.А.7– Звернення до теки CCC при стандартному налаштуванні

16. Всекцію<Directory"F:/int/home/localhost/www/ccc">слід дописати рядок:

DirectoryIndexq.html

Пересвідчимось,що при доступі до теки *CCC* відкривається файл *q .html*.

Реалізація пп.16–18 дозволяє встановити файлq.html в якості головного файлу директорії CCC.

17. Для заборони доступу до теки CCC методом POST в секцію (рис.А.8)

<Directory"F:/int/home/localhost/www/ccc">слід дописати:

<Limit

POST>or

der

deny,allow

denyfroma

ll

</Limit>

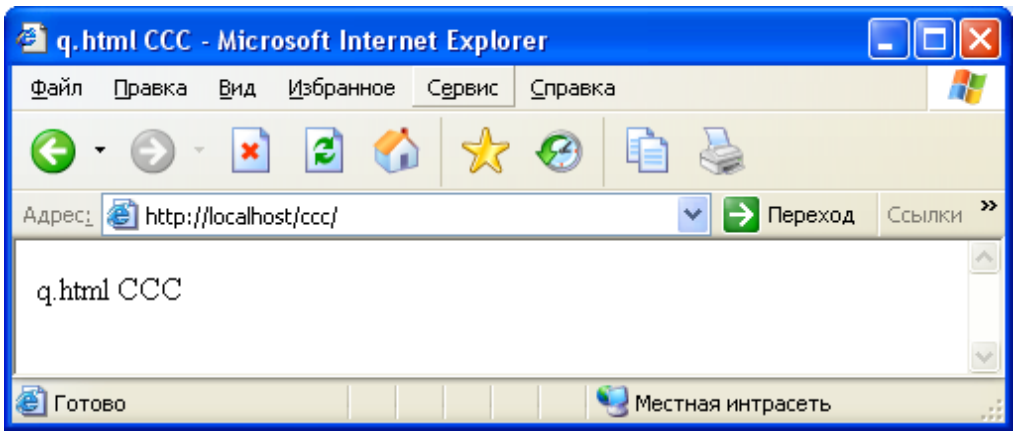


Рисунок.А.8– Звернення до теки CCC при заміні головного файлу на q.html

18.Для заборони доступу всіх користувачі ввеб-серверу до файлу *myf.html*,розміщеному в теці AAA слід в секції <Directory "F:/int/home/ localhost/www /aaa"> дописати:

<Files

myf.html

>order

deny,allowd

enyfromall

</Files>

19. Для заборони доступу всіх користувачі в веб-серверу до теки DDD слід після кінця секції <Directory "F:/int/home/localhost/www/ccc"> </Directory> записати:

<Directory
"F:/int/home/localhost/www/ddd">Or
derdeny,allow

Deny fromall

</Directory>

20. Відповідно (рис.А.9) пересвідчимось в недоступності всіх файлі в текиDDD.

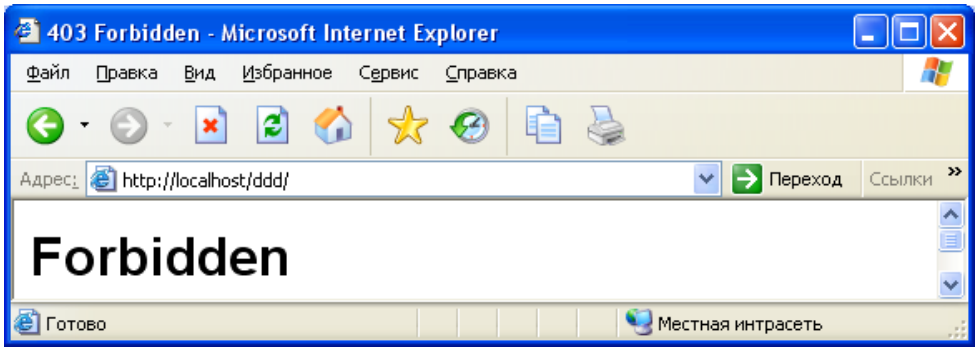


Рисунок.А.9 – Доступ до теки DDD заборонено

21. Для відкриття доступу всіх користувачів до файлу rrr.htm,розміщеному втеці DDD слід в кінці секції <Directory F:/int/home/localhost/www/ddd"> дописати:

<Filesrrr.html>

order

deny,allow

allowfrom

all

</Files>

22. Відповідно (рис.1.10.А) пересвідчимось у відкритті доступу до файлу rrr.htm, розміщеному в теці DDD.

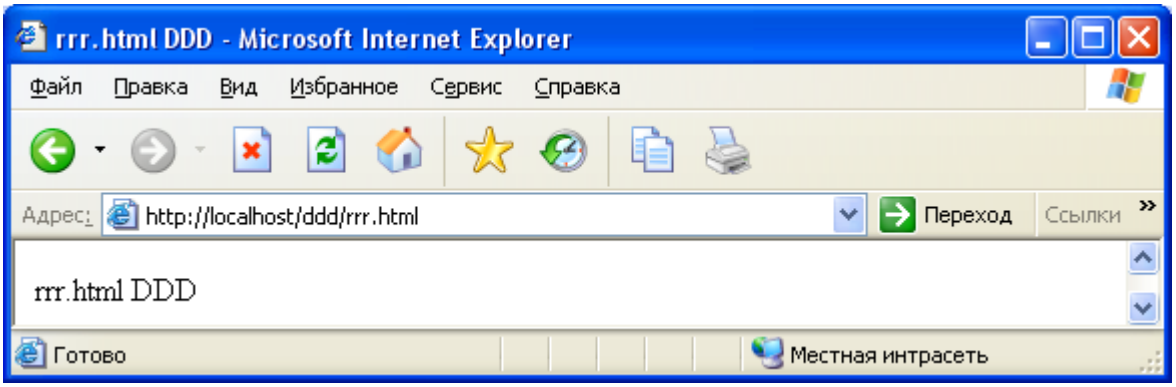


Рисунок.А.10– Доступ до файлу rrr.htm теки DDD відкрито

23. Для визначення файлу *y.html* в якості відповіді веб-серверу при виникненні помилки типу404- «Ресурсне знайдено»слід:

– Після рядка

#ErrorDocument402http://localhost/subscription_info.html

записати

ErrorDocument404http://localhosty.html

– в теці F:\int\home\localhost\www\ створити файл *y.html* та записати в нього потрібну інформацію

24. Для перевірки зміни відповіді слід звернутись до неіснуючого ресурсу веб-серверу, наприклад http://localhost/ccc/1.htm. У відповідь, к цепоказано на (рис.А.11)повинен відкритись файл *y.html*.

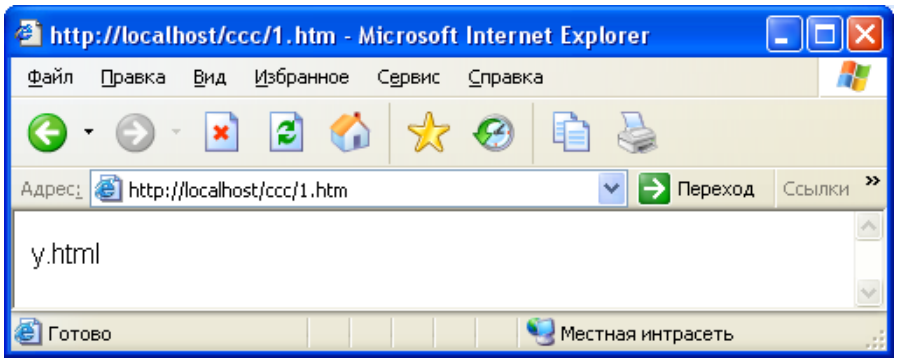


Рисунок А.11 – Зміна файлу повідомлення про помилку

ДОДАТОК Б

СЛАЙДИ ПРЕЗЕНТАЦІЇ

Дослідження методів захисту веб-сервісів від кібератак

Виконав: Студент 2курсу,групи ІМІзм-20-1 Коваленко О.Г.

Керівник: к.т.н., доцент Золотарьов В.А.

Мета кваліфікаційної роботи

- Дослідити найактуальніші вразливості веб-застосунків, які можуть бути використані при кібератаках
- Запропонувати шляхи обмеження вразливостей веб-застосунків
- Дослідити найнебезпечніші кібератаки на веб-застосунки
- Запропонувати методи захисту від кібератак
- Розробити лабораторну роботу «Конфігурація веб-сервісів»

Таблиця 1.1 - A0h1:2021-Broken Access Control (Порушений контроль доступу)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник який є авторизованим користувачем, просто змінює URL або параметри привілейованої функції.	Додатки не завжди належним чином захищають свої функції. Інколи захист на функціональному рівні здійснюється за рахунок конфігурації ,а система налаштовується невірно.		Такі недоліки дають зловмисникам можливість отримати доступ до незахищеної функції.	Зважайте на значення функції та даних, що ними оброблюються для діяльності.

Таблиця 1.2 A02:2021-Cryptographic Failures (Криптографічні збої)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати слабкий або застарілий алгоритм та фреймворків додатку.	Слабкі криптографічні алгоритми, недостатня ентропія, застарілі протоколи, використання власних алгоритмів.		Такі недоліки дають зловмисникам можливість отримати доступ до данних.	Зважайте на значення функції та даних, що ними оброблюються для діяльності.

Таблиця 1.3-A03:2021-Injection (Ін'єкція)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може впровадити дані в веб-додаток і змусити виконати дії які не були розроблені для програми.	Відсутність перевірки та очищення данних, використання коду через SQL-запит що використовує ненадійні дані.		Такі недоліки дають зловмисникам можливість крадіжки конфіденційної інформації та данних.	Зважайте на значення функції та даних, що ними оброблюються для діяльності.

Таблиця 1.4 - A04:2021-Insecure Design (Небезпечний дизайн)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Використовуючи підроблений дизайн для обману користувача.	Слабкі шаблони безпеки, ,використання власних алгоритмів.		Такі недоліки дають зловмисникам можливість отримати доступ до данних.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Таблиця 1.5 - A05:2021-Security Misconfiguration (Помилка конфігурації безпеки)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки тяжкі	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати застаріле або вразливе програмне забезпечення в системі.	Без параметру безпеки в серверах, програмах, базах данних що встановленні в безпечні значення.		Такі недоліки дають зловмисникам можливість використати для доступу до сервера, крадіжку данних, знаходження вразливостей контролю доступу.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Табличка 1.6 - A06:2021-Vulnerable and Outdated Components (Уразливі та застарілі компоненти)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати не обновлені або застарілі компоненти.	Не обновленні компоненти що використовуються, програмне забезпечення що є вразливим і не підтримується розробником, не виконується сканування на пошук вразливостей.		Такі недоліки дають зловмисникам Скористуватися вразливостями для доступу до програми.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Таблиця 1.7 - A09:2021-Security Logging and Monitoring Failures (Помилки ідентифікації та аутентифікації)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку/ діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник має список дійсних імен користувачів і паролів які дійсні.	Використання слабких процесів відновлення данних, слабкі паролі доступу,		Такі недоліки дають зловмисникам можливість отримати доступ до данних користувача.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Таблиця 1.8 - A08:2021-Software and Data Integrity Failures
(Помилки програмного забезпечення та цілісності даних)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Спешифічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати недоліки програмного забезпечення для зміни.	Порушення цілісності програмного забезпечення які не мають захист, слабке кодування данних.		Зловмисник потенційно може завантажувати власні оновлення для розповсюдження та запуску на всіх установках	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Таблиця 1.9 - A09:2021-Software and Data Integrity Failures
(Помилки програмного забезпечення та цілісності даних)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку/діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати порушення через відсутність моніторингу та реєстрації	Порушення через відсутність моніторингу та реєстрації, порушення данних.		Зловмисник може отримати доступ до інформації або крадіжку конференційної інформації користувача.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Таблиця 1.10 - A10:2021-Server-Side Request Forgery (Підробка запиту на стороні сервера)

Чинники Загрози	Вектори атаки	Слабкі місця безпеки		Технічні наслідки	Наслідки для діяльності
Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність Звичайна	Можливість виявлення СЕРЕДНЯ	Наслідки помірні	Специфічні для додатку /діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатку.	Зловмисник може використати порушення через відсутність моніторингу та реєстрації	Порушення через відсутність URL-адреси.		Зловмисник може отримати доступ до інформації або крадіжку конференційної інформації користувача.	Зважайте на значення функції та даних, що ними обробляються для діяльності.

Рисунок 2.1 - Введення SQL-коду

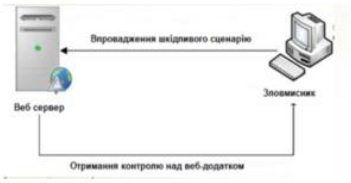


Рисунок 2.2 - PNP - ін'єкція

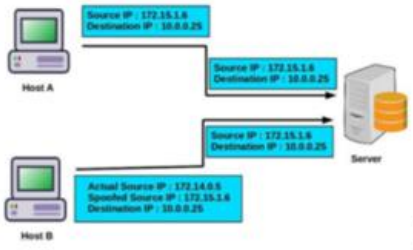


Рисунок 2.3 - Атака з заміною IP-адреси

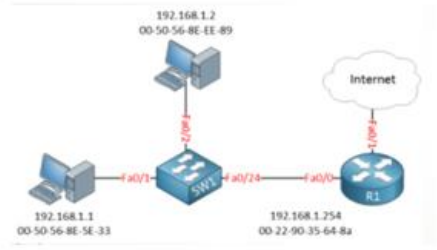


Рисунок 2.4 Заміна ARP

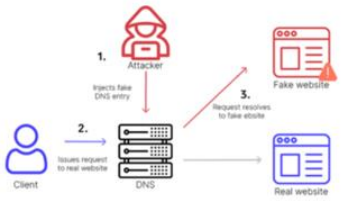


Рисунок 2.5 - Спуфінг DNS-сервера

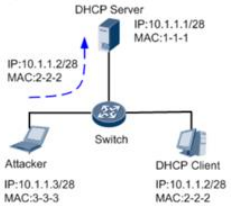
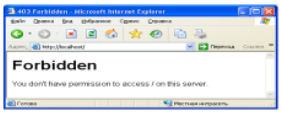
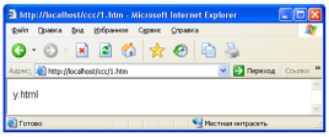


Рисунок 2.6 - Спуфінг MAC-адрес

РОЗРОБКА ЛАБОРАТОРНОЇ РОБОТИ «КОНФІГУРАЦІЯ ПАРАМЕТРІВ ЗАХИСТУ ВЕБ-СЕРВЕРУ»

- *Метою* лабораторної роботи є оволодіння практичними навичками налаштування базових параметрів захисту веб-сторінок за допомогою стандартних засобів веб-серверу Apache.





Позначення	*Найменування*	
	Текстові документи	
1.	Пояснювальна записка	93
	Графічні документи	
2.	Слайди презентації	13

Змін.	Арк.	Номер докум.	Підпис	Дата	Дослідження методів захисту веб-сервісів від кібератак	Літ.	Аркуш	Аркушів
Розроб.		Коваленко				У	1	1
Перевір.		Золотарьов				**ХНУРЕ** кафедра ІМІ		
Н. контр.		Золотарьов						
Затв.		Безрук						