Лабораторная 10: Взлом вебсайта и его защита

Поднимите веб-сервер Apache с СУБД MySQL (или MariaDB). Можно использовать XAMPP или LAMPP пакеты.

Создайте базу данных website и добавьте таблицу. Дамп БД приведен ниже:

CREATE TABLE `guestbook` (

  `id` int(11) NOT NULL,

  `author` varchar(255) NOT NULL,

  `post` text NOT NULL,

  `created` datetime NOT NULL DEFAULT current\_timestamp()

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

ALTER TABLE `guestbook`

  ADD PRIMARY KEY (`id`);

ALTER TABLE `guestbook`

  MODIFY `id` int(11) NOT NULL AUTO\_INCREMENT;

На веб сервере, в папке для хранения веб скриптов (обычно httpd), создайте папку website, и в ней добавьте PHP скрипт гостевой книги index.php:

<!DOCTYPE html>

<html>

<head>

    <meta charset="utf-8">

    <title>Гостевая книга</title>

    <style>

        .message {border: 1px solid #000000; margin: 1em;}

        .author { padding: 1em; font-weight: bold; border-bottom: 1px dashed #333333; }

        .post { padding: 1em; }

        .date { padding: 1em; border-top: 1px dashed #333333; font-style: italic; }

    </style>

</head>

<body>

    <h1>Гостевая книга</h1>

    <!-- Форма для отправки сообщения в гостевую книгу -->

    <h3>Добавить сообщение</h3>

    <form action="index.php" method="POST">

        <label>Автор</label>

        <div><input type="text" name="author" style="width:100%"></div>

        <label>Сообщение</label>

        <div><textarea name="message" rows="10" style="width:100%"></textarea></div>

        <div><input type="submit" value="Отправить"></div>

    </form>

</body>

<h3>Сообщения</h3>

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "website";

// Подключение к и выбор БД

$conn = new mysqli($servername, $username, $password, $dbname);

if ($conn -> connect\_errno) {

    echo "Failed to connect to MySQL: " . $conn -> connect\_error;

    exit();

}

// Добавление сообщения в БД, если есть POST данные

if(isset($\_POST['author']) && isset($\_POST['message']))

{

    $sql = 'INSERT INTO guestbook (author, post) VALUES("' . $\_POST['author'] . '", "' . $\_POST['message'] . '")';

    $result = $conn -> query($sql);

}

// Выборка сообщений из БД

$sql = 'SELECT id, author, post, created FROM guestbook ORDER BY id DESC';

$result = $conn -> query($sql);

while($row = mysqli\_fetch\_assoc($result)) {

   echo "<div class='message'><div class='author'>{$row['author']}</div><div class='post'>{$row['post']}</div><div class='date'>{$row['created']}</div></div>";

}

?>

</html>

Теперь, доступ к гостевой книге доступен по ссылке <http://localhost/website>

Задача:

* Провести QoS атаку на вебсайт в любой форме
* Дать рекомендацию по защите веб сайта от QoS атаки
* Провести необходимые изменения в скрипте по рекомендации