mythemeshop

WEB SERVER SECURITY

Team

k. durga prasad
B. upendra
J. ganesh
M. kanvith
P. charan

1. INTRODUCTION

(a) Overview

Web server security is the security of any server that is deployed on a worldwide web domain over the Internet. It is implemented through several methods and the layers typically, including the Base operating System (OS) security layer, hosted application security layer and network security layer. OS security, which ensures access to authorized users only, operates a web server's critical components and services. Application layer security ensures control over the content and services hosted on the web server.

Network Security provides protection against Internet Based security exploits, viruses and attacks. The web server security service Module (SSM) provides an environmental Binding between the web logic enterprise security Infrastructure and IIS and apache web servers, The web logic enterprise Infrastructure Provides six distinct services: Registry authentication, authorization auditing, Role Mapping, and credential Mapping each of these services is expressed in a way that is understandable to application Running within a web server that is protected by the web logic enterprise security Infrastructure.

The web server SSM makes access control decisions for the web server to which it is Bound. The security configuration on which the access control decisions are Based is defined and deployed by the administration and resources

(b) purpose

→ The purpose of web server security is to protect the server and the data it hosts from various threats, such as unauthorized access, data breaches, malware injections, and denial-of service attacks. This is achieved through measures like encryption, firewalls, access controls, regular updates, and security audits.

Ultimately, it ensures the confidentiality, integrity and availability of the web server and it's resources.

By using denial service attack in a web server security project can serve several purposes.

1) Testing Resilience :-

It allows you to test how resilient your web server is against such attacks.

2) Identifying weaknesses :-

Dos attack can help you identify weaknesses in your server configuration, networks infrastructure.

3) Tuning security controls :-

conducting controlled DoS attacks as part of a security project can raise awareness among shake holders's about the importance of web server security.

(e) LITERATURE SURVEY

Existing approaches and methods to solve this problem.

web servers security concerns, including denial of service attacks, several approaches and methods can be employed.

1) Firewalls :-

Implementing firewalls can help filter incoming and outgoing traffic. preventing unauthorized access and mitigating Dos attack by Blocking malicious traffic

2) Intrusion Detection System (IDS)

IDS tools can monitor network traffic for suspicious activities and patterns, alerting administrators to potential Dos attacks in real time.

3) Load Balancers :

Load Balancers distribute incoming traffic across multiple servers, preventing any single server from becoming overwhelmed by a Dos attack

4) Rate Limiting :-

Implementing Rate limiting mechanisms can restrict the number of requesting from individual IP addresses, preventing attackers, from overwhelming the server with excessive requests.

(b) proposed solution:-

In This project web have to suggest the Dos attacks on the one educational websites. considering proposed solution comprising methods and suggestions:.

1) Traffic analysis and Monitoring:

Deploy tools for continous monitoring and analysis of incoming traffic to detect unusual of incoming traffic to detect unusual patterns indicative of Dos attacks.

2) Rate limiting and Requesting filtering:-

Implement Rate limiting Mechanisms to restrict the number of requests from individual ip addresses or Blocks requests that exceed certain thresholds. use requests filtering techniques to identify and block suspicious.

3) Load Balancing and scalability:-

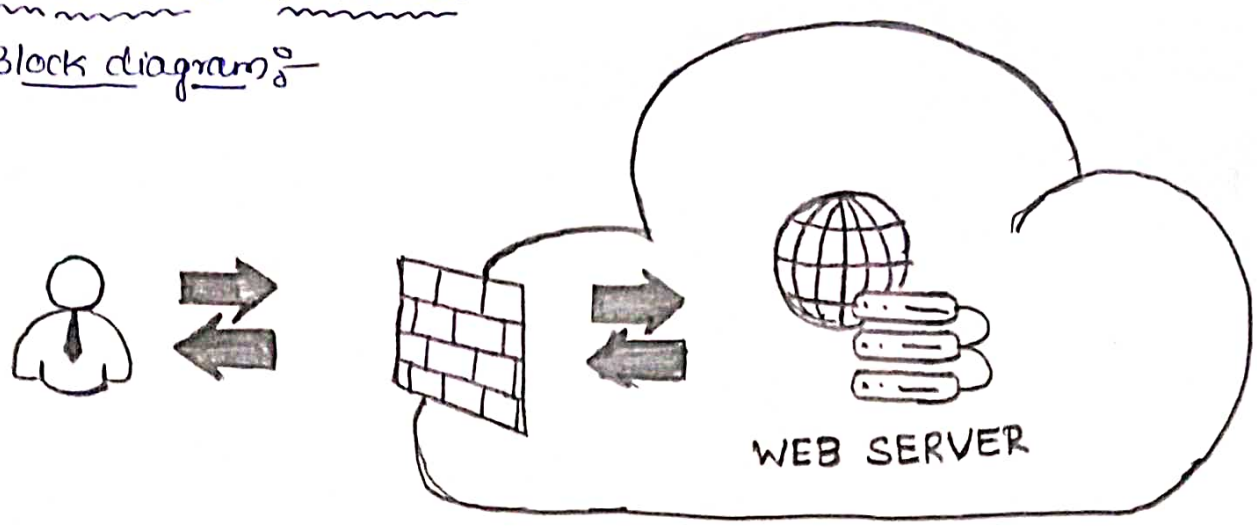
Employ load Balancers to distribute incoming traffic across multiple servers, ensures no single server is overwhelmed by an influx of requests, Implement scalable Infrastructure that can dynamically allocate resources to handle increased traffic during potential Dos attacks.

4) Content Delivery Networks (CDN):-

utilize CDN Services to cache and distribute content across geographically dispersed servers, Reducing the impact of Dos attacks by absorbing and mitigating malicious traffic closer to the source.

(3) THEORITICAL ANALYSIS

(a) Block diagram :-



(1) Network layer :

⇒ Firewall : Controls incoming and outgoing traffic Based on predetermined security Rules.

⇒ Intrusion Detection system IDS/intrusion prerention System (IPS) : monitors network traffic for malicious activity and can take action to prerent it.

(2) web server :-

⇒ Application layer firewall : filters and monitors HTTP / HTTPS requests and responses

⇒ Secure configeration :

(3) Operating System :

⇒ patch management : Regular updates and patches to address known Vulnerabilities

(4) Database Server :-

⇒ Data Base firewalls : Monitors and filters database traffic to prurent unauthorized access or SQL injection attacks.

(b) Hardware and Software designing:

⇒ Hardware Requirements:

(1) Network Hardware:-

⇒ High-performance routers and switches capable of handling large volumes of traffic and implementing access control lists.

⇒ Load Balancers to distribute incoming traffic across multiple servers preventing a single point of failure.

(2) Server Hardware:

⇒ Robust servers with sufficient CPU, memory and disk space to handle normal traffic and potential DOS attack spikes.

⇒ Redundant power supplies and RAID configurations for fault tolerance and data integrity.

⇒ Distributed denial of service (DDOS) mitigation appliances or services capable of handling massive volumes of traffic.

⇒ Software Requirements:-

(1) Operating System:

⇒ Securely configured operating system with the latest security patches and updates applied.

⇒ Properly configured firewall software to filter incoming traffic and block known attack patterns.

(2) Web Server Software:

⇒ Securely configured web server software with appropriate settings to limit resource consumption and prevent abuse.

(3) Security Software:-

⇒ Intrusion detection and prevention system software to detect and mitigate DOS attacks in real-time.

⇒ Logging and monitoring software to track and analyze server and network activity, including signs of DOS attacks.

4) Results :-

→ In this project web server security, we can performing the DOS attack on the attacking web site is the xampp which is used when even if it is refreshed we don't get the site. DOS attack is the type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device normal functioning. As we get into the xampp there we appear the search engines we have in our system. As we enter into the all controls of the xampp we appear the anaconda prompt then we need to make it as the pin as administrator then we can perform the dos attack the anaconda prompt is nothing But the slowris tool. Local host ip address is : 127.0.0.1.

→ finally after complition of the dos attack on the xampp through local host ip address and then "The site can't be reached as we request so many times even after refresh mutiple times.

localhost/dashboard/

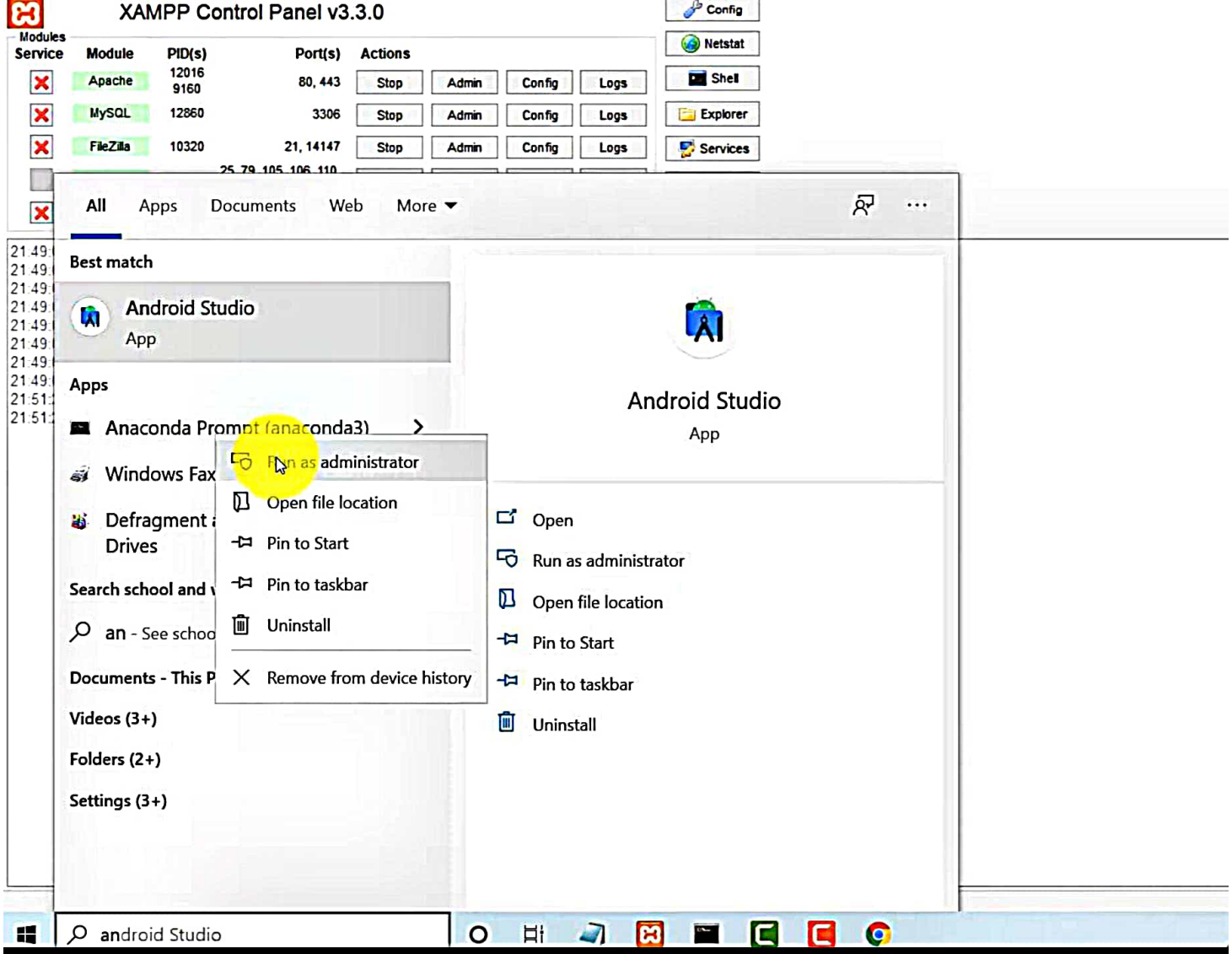
Apache Friends | Applications | FAQs | HOW-TO Guides | PHPInfo | phpMyAdmin

XAMPP Apache + MariaDB + PHP + Perl

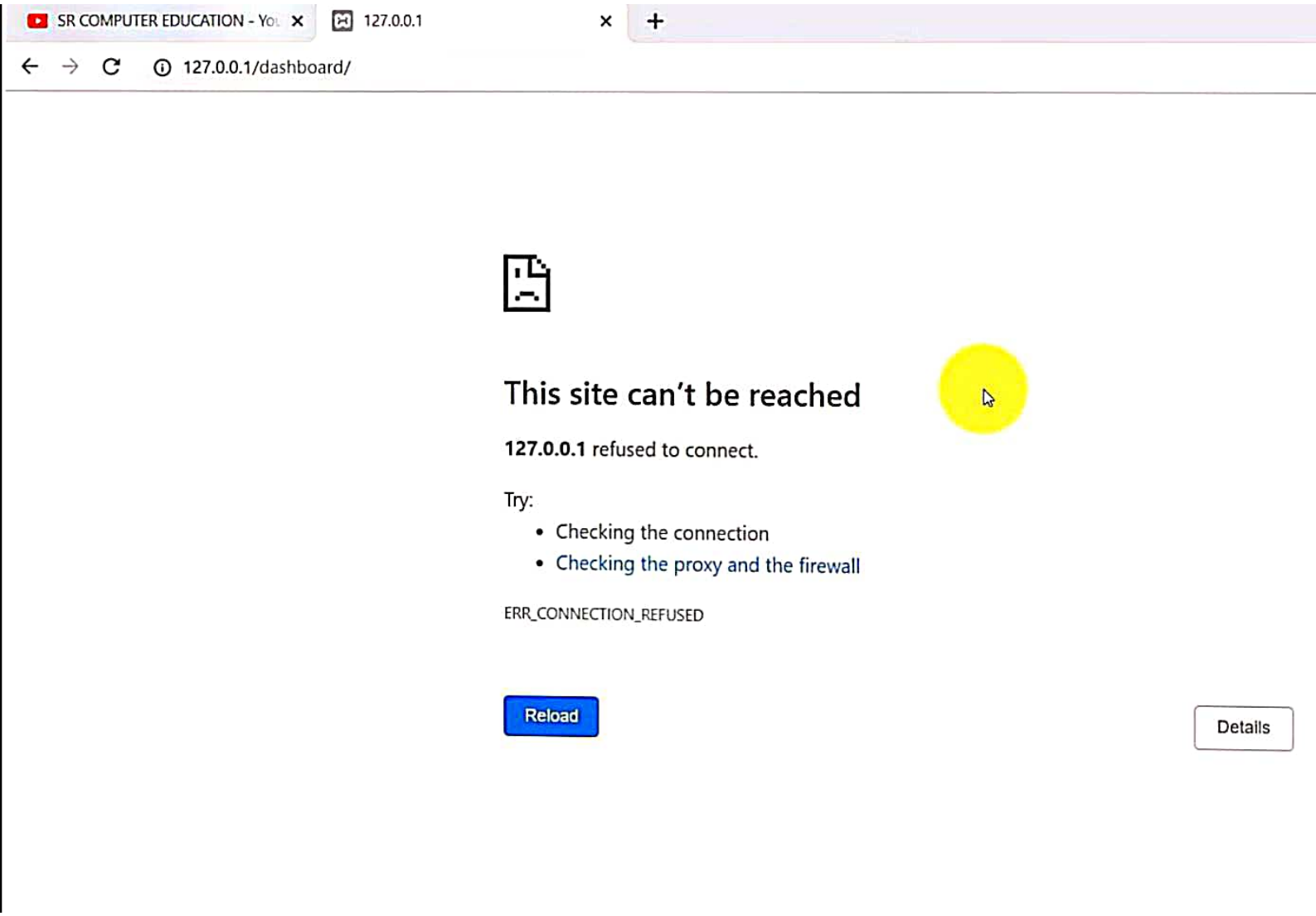
Welcome to XAMPP for OS X 5.6.19

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

Start the XAMPP Control Panel to check the server status.




```
(base) C:\Users\91990>slowloris -s 500 -p 80 127.0.0.1
[28-10-2021 22:07:01] Attacking 127.0.0.1 with 500 sockets.
[28-10-2021 22:07:01] Creating sockets...
[28-10-2021 22:07:07] Sending keep-alive headers... Socket count: 350
[28-10-2021 22:07:24] Sending keep-alive headers... Socket count: 350
[28-10-2021 22:07:41] Sending keep-alive headers... Socket count: 350
```


SR COMPUTER EDUCATION - Yo
127.0.0.1
127.0.0.1/dashboard/
This site can't be reached
127.0.0.1 refused to connect.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
Reload
Details

(5) ADVANTAGES & DISAVANTAGES :-

⇒ Advantages & disadvantages of the enhancing web server security specifically against Dos attack:

Advantages of web server security :-

(i) Improved availability :-

By mitigating Dos attacks, web server security measures ensure that online services remain accessible to legitimate users, enhancing overall availability.

(ii) Enhanced Reliability :-

Strengthening web server security against Dos attacks increases the reliability of web services by reducing the likelihood of disruptions caused by malicious traffic.

(iii) protection of Reputation :-

preventing successful Dos attacks helps safeguard the reputation of the organization by maintaining uninterrupted access to online resources and preserving user trust.

(iv) cost saving :-

Avoiding downtime and service interruptions due to Dos attacks, helps organizations meet compliance requirements mandated by industry regulations & standards.

Disadvantages of the web server Security :—

(1) Resource intensive :

Implementing and Maintaining effective security Measures against Dos attacks can be resource intensive, requiring investments in hardware, software and personnel.

(2) False positives :

Overly aggressive security measures may lead to false positives, Blocking legitimate traffic and impacting the user experience. Fine-tuning security controls is necessary to minimize false positives while effectively mitigating Dos attack.

(3) Complexity :

Maraging a comprehensive web server security strategy, including protection against Dos attack, adds complexity to it infrastructure and operations, potentially increasing the likelihood of misconfigurations and vulnerabilities.

(4) Potential performance Impact :

Some security measures, such as Rate limiting and request filtering, may introduce overhead and impact the performance of web servers, particularly during peak traffic periods.

(6) Applications :-

web server security measures aimed at mitigating Denial of Service attacks have various applications across different sectors and industries.

(1) E-commerce platforms :-

Online retailers heavily rely on web servers to conduct transactions and provide services to customers. Implementing robust security measures against DOS attacks ensures continuous availability of e-commerce websites, preventing revenue loss due to downtime and maintaining customer trust

(2) financial Institutions :

Banks, payments processors, and other financial institutions utilize web servers to offer online banking services and process transactions.

Protecting these systems from DOS attacks is critical to safeguarding sensitive financial data, preventing service disruptions, and maintaining regulatory compliance.

(3) Government websites :-

Government agencies and public sector organizations host websites to provide information services, and resources to citizens.

(4) Media, entertainment websites :-

Streaming platforms, news websites and online entertainment services depend on web servers to deliver content to users worldwide.

(7) CONCLUSION :-

As we have seen, distributed DoS attack are genuine threat that cause serious damage to many Internet users. The losses being suffered have escalated from being merely annoying to actually being debilitating from and disastrous for some users there is every reason to believe that the rate and seriousness of DDoS attacks will increase. The current limited level of losses caused by DDoS is probably not due to success in defending against them, difficulties in perpetrating the attacks, or lack of attractive targets to attack. Rather, the level of loss is related more to the motivations and desires of those who are perpetrating the attacks.

As more unprincipal and dissatisfied users of the Internet observe the success of vulnerabilities in web application can allow attackers to exhaust available resources and thereby deny access to legitimate users. companies that rely on web application to provide critical business functions core increasible at risk from attackers wishing to disrupt these functions by exploiting application-level vulnerabilities.

The possibility of a denial of service attack should be considered when designing, implementing and providing applications, and appropriate strategies and mitigation techniques put in place within the application.

8)

Future Scope :-

In the ever-changing digital Battlefield, Distributed Denial of Service (DDoS) attacks continue to be a formidable weapon for cybercriminals and disruptors. As technology advances, so do the tactics employed in DDoS attacks, necessitating organizations to stay one step ahead with adaptive prevention strategies. Let's take a peek into the future of DDoS threats and explore how organizations can prepare for what lies ahead.

Emerging Trends in DDoS attacks :-

(1) Increased Complexity and Sophistication :-

Future DDoS attackers are likely to become more complex by employing multi-vector approaches. attackers may combine different techniques to overload both network and application layers simultaneously, making mitigation more challenging.

(2) Rise of IoT-Based Botnets :-

The proliferation of vulnerable internet of things devices creates a vast potential for Botnets. future attacks might leverage these compromised devices, amplifying the scale and impact of DDoS Incidents.

(3) Weaponised AI and Machine Learning :-

Attackers are expected to leverage artificial intelligence and Machine learning to develop adaptive attack schemes. This could bypass traditional signature-based detection methods requiring more sophisticated defense mechanisms.