LONG PASSWORD DOS ATTACK

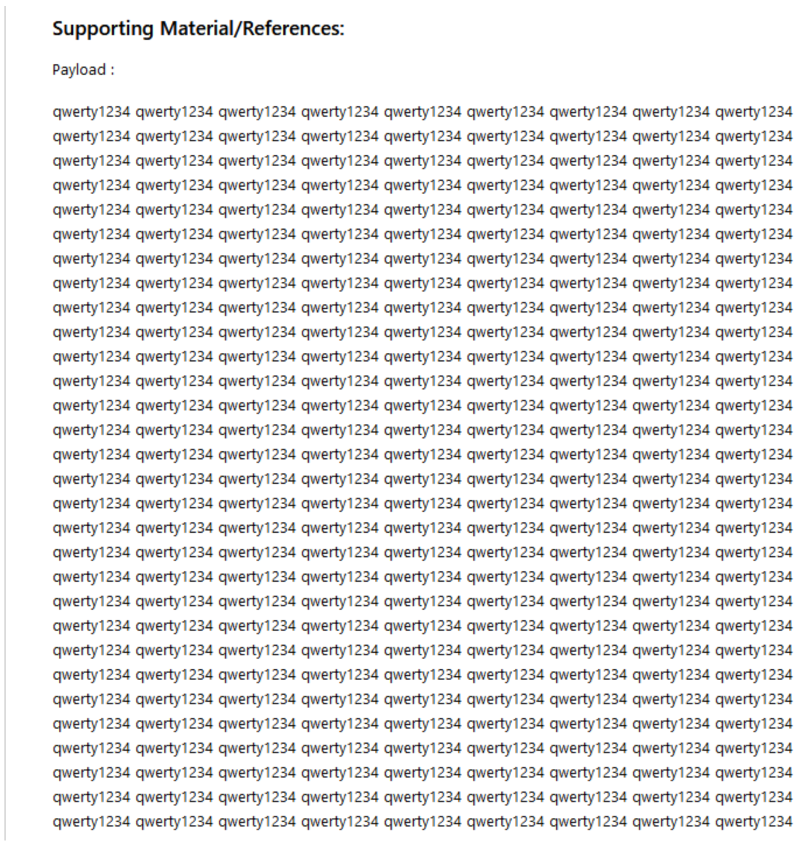
What is Long Password DoS attack?

A denial-of-service (DoS) attack aims to disrupt the normal functioning of a system, service, or network, making it temporarily or indefinitely unavailable to users. These attacks can take various forms, including overwhelming a system with a flood of traffic, exploiting vulnerabilities, or exhausting system resources.

A Long Password DoS (Denial-of-Service) attack occurs when an adversary exploits a vulnerability in the string hashing implementation of a system by sending an excessively long string, typically around 100,000 characters. This malicious act aims to overwhelm the server's resources, leading to CPU and memory exhaustion during the string hashing process. As a consequence, the targeted website may become unavailable or unresponsive, compromising its normal functioning. This attack underscores the importance of robust string hashing mechanisms and the need for effective countermeasures to prevent resource exhaustion due to excessively long inputs.

Steps

1. Open the login page of a website
2. Now interrupt the request in the burp and send it to repeater
3. In the password field enter the very long string of password around 500 characters

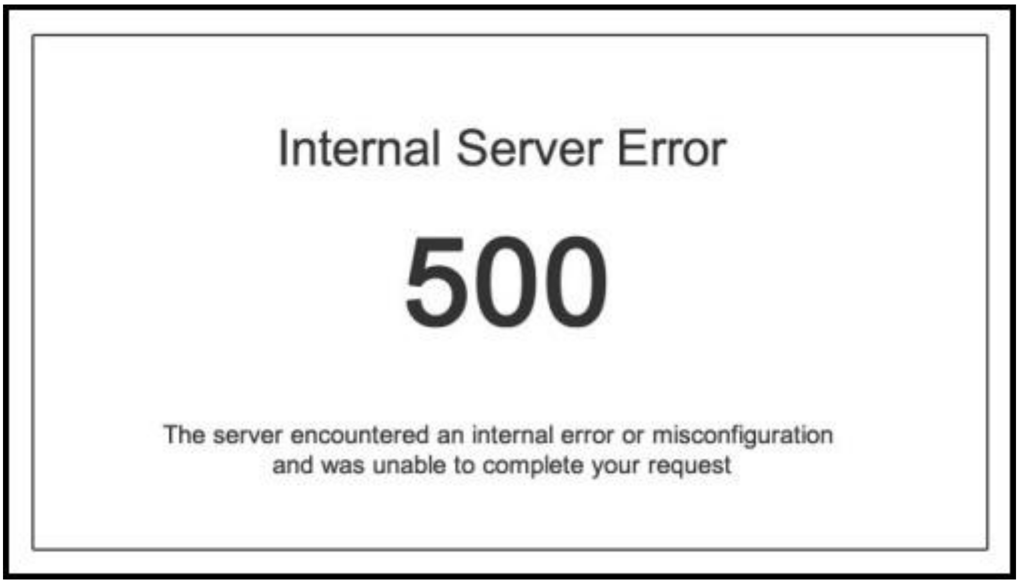


Supporting Material/References:

Payload :

```
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234 qwerty1234
```

4. Send the request
5. If response receive is 503 internal server error then it is vulnerable



Internal Server Error

500

The server encountered an internal error or misconfiguration
and was unable to complete your request

Impact

The impact of a Long Password DoS (Denial-of-Service) attack can be significant, affecting both the targeted system and its users. Here are potential impacts associated with this type of attack:

1. **Service Unavailability:**
    - The primary impact is the disruption of normal services. The targeted website or system may become temporarily or even permanently unavailable, preventing legitimate users from accessing the services.
2. **Website Unresponsiveness:**
    - The server's resources, particularly CPU and memory, may be exhausted during the string hashing process. As a result, the server becomes unresponsive to legitimate user requests, leading to degraded performance or complete unresponsiveness.
3. **User Frustration:**
    - Legitimate users attempting to access the affected website or service may experience frustration and inconvenience due to the prolonged unavailability. This can impact user satisfaction and trust.
4. **Financial Loss:**
    - Businesses relying on the affected system for online services may suffer financial losses, especially if the disruption leads to a loss of customers or impacts e-commerce transactions.
5. **Reputation Damage:**
    - Persistent or recurrent denial-of-service incidents can harm the reputation of the targeted organization or service provider. Users may lose trust in the reliability and security of the affected platform.
6. **Operational Downtime:**
    - The organization may incur operational downtime as IT teams work to identify and mitigate the attack. This could result in additional costs and delays in providing services.
7. **Resource Overhead:**
    - The server's resources, such as CPU and memory, may remain under heavy load even after the attack has ceased, affecting the overall performance and responsiveness of the system.

Mitigations

Mitigating the risk of a Long Password DoS (Denial-of-Service) attack involves implementing several measures to enhance the resilience of the system. Here are key mitigations:

1. **Input Validation:**
    - Implement stringent input validation mechanisms to ensure that user inputs, including passwords, adhere to defined length limits. Reject excessively long inputs to prevent resource exhaustion during string hashing.
2. **Define Password Length Limits:**
    - Establish reasonable password length limits based on the system's capacity and hashing algorithm requirements. This helps prevent abuse and ensures that the hashing process remains efficient.
3. **Hashing Algorithm Selection:**
    - Choose robust and efficient hashing algorithms that can handle a wide range of input lengths without causing undue strain on system resources. Stay informed about best practices in cryptographic algorithms.
4. **Rate Limiting:**
    - Implement rate-limiting mechanisms to restrict the number of authentication attempts within a specific time frame. This helps protect against brute-force attacks and mitigates the impact of a potential Long Password DoS attack.
5. **Monitoring and Anomaly Detection:**
    - Deploy monitoring tools to detect unusual patterns of behavior, including a sudden influx of exceptionally long password strings. Implement anomaly detection mechanisms to identify potential attacks and trigger alerts.
6. **Resource Management:**

- Optimize resource management on the server to handle authentication processes efficiently. This may involve load balancing, optimizing code, and ensuring that adequate resources are allocated to handle authentication requests.

7. **Incident Response Plan:**
   - Develop and regularly test an incident response plan specific to denial-of-service attacks. This plan should include steps for quickly identifying, mitigating, and recovering from a Long Password DoS attack.
8. **Regular Security Audits:**
   - Conduct regular security audits to identify vulnerabilities in password handling mechanisms and overall system security. Stay proactive in addressing potential weaknesses before they can be exploited.
9. **User Education:**
   - Educate users about the importance of creating passwords within defined length limits and the potential risks associated with using extremely long passwords. Encourage the adoption of strong, yet practical, password practices.
10. **Implementing CAPTCHA or Challenge-Response Mechanisms:**
    - Introduce CAPTCHA or challenge-response mechanisms during authentication to ensure that requests are coming from legitimate users and not automated scripts.
11. **Web Application Firewall (WAF):**
    - Deploy a Web Application Firewall that can help detect and block malicious traffic, providing an additional layer of defense against denial-of-service attacks.

References

- https://acunetix.com/vulnerabilities/web/long-password-denial-of-service/#:~:text=By%20sending%20a%20very%20long,a%20vulnerable%20password%20hashing%20implementation.
- https://shahjerry33.medium.com/long-string-dos-6ba8ceab3aa0