Report 03

URL: datacamp.com

Password Transmitted over HTTP

HIGH

The vulnerability of transmitting password data over HTTP arises due to the lack of encryption in the communication channel. When a user enters their password on a website or any other online service, and that data is transmitted over an HTTP connection, it is sent in plain text format. This means that the password is not encrypted or protected in any way during transmission. The impact of this vulnerability is significant. If an attacker can intercept the network traffic between the user and the server, they can easily capture the password in clear text. This can be achieved through various means, such as eavesdropping on unsecured Wi-Fi networks, using network sniffing tools, or compromising network infrastructure.

Once an attacker obtains a user's password, they can potentially gain unauthorized access to the user's account. This can lead to various malicious activities, including identity theft, unauthorized transactions, unauthorized access to sensitive information, and even impersonation of the user. Transmitting password data over HTTP is highly insecure because any party with access to the network traffic can read and potentially abuse the information. It is important to note that even if the website or application hashes or encrypts the passwords when storing them, transmitting them over HTTP in plain text format exposes them to interception before they are protected.

URL : http://www.datacamp.com/

Input Name : `user[password]`

Form target action : `http://www.datacamp.com/users`

Affected Components

- Network Communication: The vulnerability lies in the communication between the user's device (client) and the server hosting the website or application. Specifically, it affects the transmission of password data over the network.

- Web Application or Website: The vulnerability is relevant to any web application or website that transmits password data over HTTP. This includes login forms, registration forms, password change forms, and any other components where users enter their passwords.

- Authentication Process: The vulnerability affects the authentication process of the web application or website. Since the passwords are transmitted in plain text, an attacker can potentially obtain them and compromise user accounts.

- Data Privacy and Security: The overall data privacy and security of the system are affected. The transmission of passwords over HTTP undermines the confidentiality and integrity of sensitive user information.

Impact Assessment

The vulnerability of transmitting password data over HTTP has a significant impact on the security and privacy of user information.

- Confidentiality Impact: The confidentiality of password data is compromised as it is transmitted in plain text over the network. Any attacker with access to the network traffic can easily intercept and read the passwords, exposing sensitive user credentials.

- Account Compromise: If an attacker successfully intercepts and obtains user passwords, they can gain unauthorized access to user accounts. This can lead to various malicious activities, such as unauthorized transactions, data manipulation, or even complete account takeover.

- Data Breach Risk: Transmitting passwords over HTTP increases the risk of a data breach. If an attacker gains access to the network or compromises the server, they can retrieve a vast amount of unencrypted password data, potentially affecting multiple users.

- User Privacy Violation: Users' privacy is violated as their sensitive information is exposed to unauthorized parties. This can erode user trust and confidence in the affected system or service.

- Regulatory Compliance: Depending on the nature of the data and applicable regulations (such as GDPR, HIPAA, or PCI DSS), the vulnerability of transmitting passwords over HTTP may result in non-compliance with data protection and privacy requirements.

Steps to Reproduce

- Identify the target web application or website that transmits password data over HTTP.

- Set up a network monitoring tool or use network sniffing techniques to intercept network traffic between the user's device and the server.

- Begin capturing network packets to capture the HTTP requests and responses exchanged during the login process or any other instance where passwords are entered.

- Locate the specific HTTP request that contains the password data. This can usually be identified by looking for form submissions or POST requests that include parameters related to password fields.

- Extract and analyze the captured network packet to obtain the plaintext password data.

- If necessary, decode or decrypt any encoding applied to the password data (e.g., URL encoding) to obtain the original password value.

- Document the successful interception and extraction of the password data, noting the method used and any additional relevant information.

- Repeat the process multiple times to ensure consistency and verify that the vulnerability exists consistently.

Proposed Mitigation or Fix

✓ Adopt HTTPS (HTTP Secure): Upgrade the web application or website to use HTTPS for transmitting sensitive data, including passwords. HTTPS encrypts the communication between the user's device and the server, ensuring that the data is

protected from interception and unauthorized access. Obtain an SSL/TLS certificate and configure the server to enforce HTTPS connections.

- ✓ Implement HSTS (HTTP Strict Transport Security): Enable HSTS on the server to instruct the user's browser to only connect to the website using HTTPS. This prevents users from inadvertently accessing the site over insecure HTTP connections and helps enforce secure communication consistently.

- ✓ Use Secure Password Storage: Implement strong password hashing algorithms, such as bcrypt or Argon2, along with a unique salt for each user. Hash the passwords before storing them in the database to protect against unauthorized retrieval in case of a data breach.

- ✓ Implement Two-Factor Authentication (2FA): Enable and encourage users to set up two-factor authentication for their accounts. This adds an extra layer of security by requiring a second form of verification, such as a code sent to a mobile device, in addition to the password.

- ✓ Conduct Security Testing and Auditing: Regularly perform security testing, such as vulnerability scanning and penetration testing, to identify and address any security weaknesses, including the transmission of passwords over HTTP.

- ✓ Implement Intrusion Detection and Prevention Systems: Deploy intrusion detection and prevention systems to monitor network traffic and detect any attempts to intercept or manipulate password data in transit