

Insecure

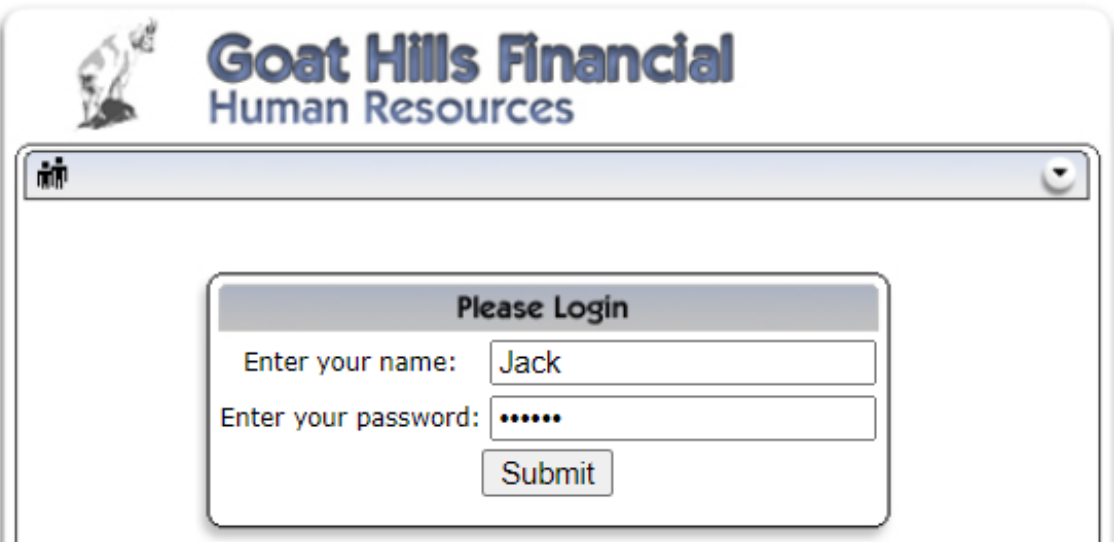
1. Insecure Communication

Dữ liệu nhạy cảm không nên được gửi ở dạng bản rõ! Thông thường, các ứng dụng chuyển sang kết nối an toàn sau khi đã cấp quyền cho người dùng. Kẻ tấn công chỉ có thể đánh hơi thông tin đăng nhập và sử dụng thông tin thu thập được để đột nhập vào tài khoản. Một ứng dụng web tốt luôn chú ý đến việc mã hóa các dữ liệu nhạy cảm.

Bài này mục đích cho ta biết, lý do tại sao nên mã hóa các dữ liệu nhạy cảm trong quá trình lưu chuyển nó trên không gian mạng.

For this lesson you need to have a server client setup. Please refer to the Tomcat Configuration in the Introduction section.

Stage1: In this stage you have to sniff the password. And answer the question after the login.



Goat Hills Financial
Human Resources

Please Login

Enter your name: Jack

Enter your password:

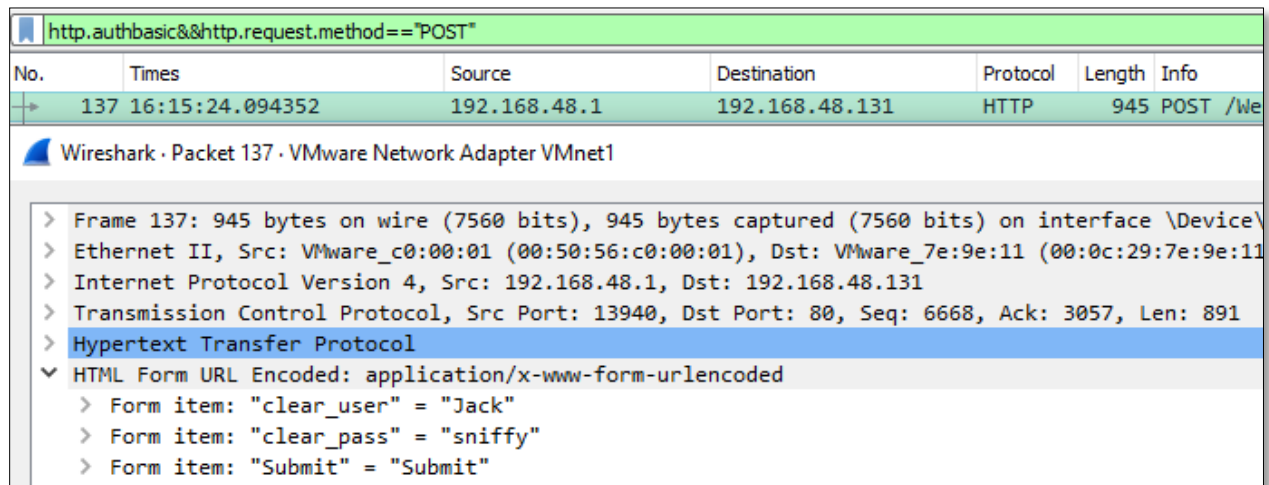
Submit

Bài yêu cầu ta đánh hơi mật khẩu được sử dụng trong quá trình đăng nhập của người dùng, và trả lời chúng sau khi login. Thông tin đăng nhập được website cho trước rồi nhé, ta chỉ việc submit. Vấn đề là làm sao để đánh hơi nó đây ?

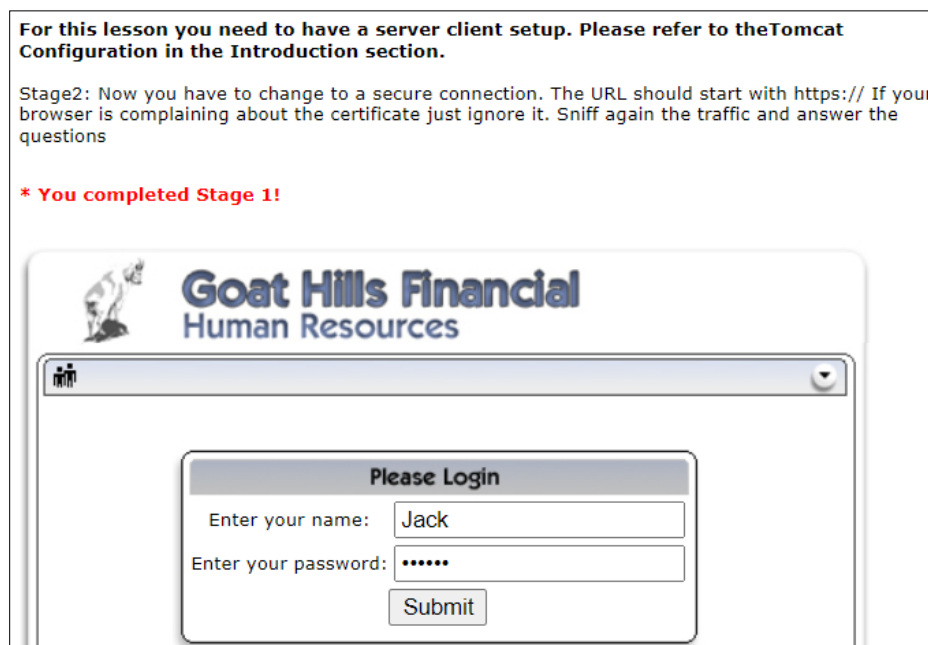
Thật ra nếu bạn đã hiểu về HTML, thì bạn có thể xem hẳn giá trị của nó thông qua thẻ HTML luôn, hoặc dùng Proxy chặn request lại xem giá trị là sẽ thấy.

Nhưng để đúng với mục tiêu là "sniffing password", thì ta nên dùng WireShark, bắt toàn bộ các gói tin trên lưu lượng mạng rồi lọc các gói tin Authentication ra.

Vì mình biết bài này không có mã hóa dữ liệu khi gửi, nên chắc chắn nó dùng HTTP rồi.

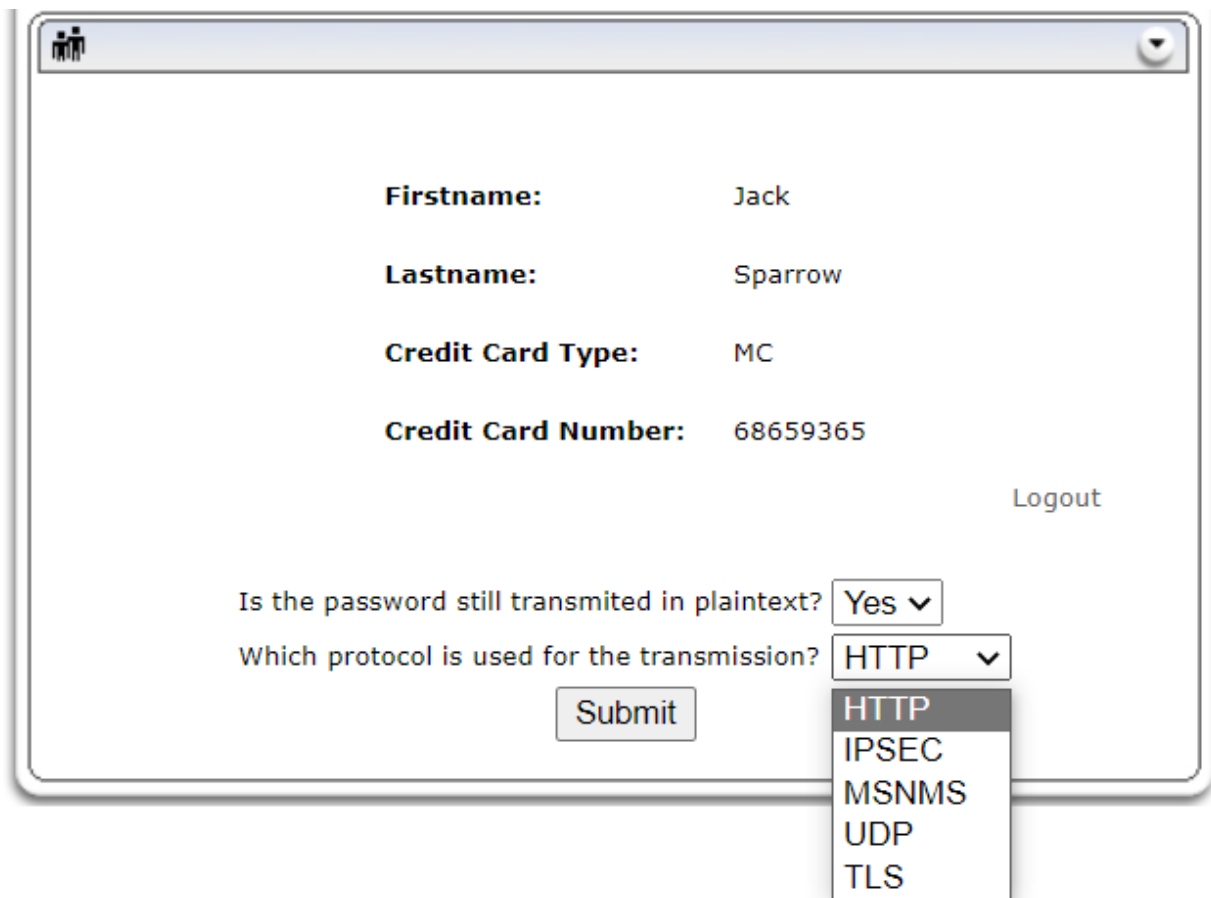


Nó đây, vì Login thì sẽ POST thông tin lên Server, và kiểu chứng thực, theo như mình nghĩ đầu tiên thì là Basic Authen, lọc 1 phát ra luôn, nếu k ra thì lọc phương thức Authen khác là đc nhé.



STAGE 2: Bây giờ ta phải thay đổi sang một kết nối bảo mật hơn để tránh việc hacker dễ dàng lấy được password như Stage 1. URL hiện nay nên bắt đầu bằng **https** (cổng 443, sử dụng mã hóa TLS hoặc SSL), gia tăng tính bảo mật.

Bài này bạn có thể dùng TOMCAT để cấu hình cho website sử dụng **https** rồi làm. Vì mình không biết cấu hình nên STAGE 2 hiện bỏ qua. Nhưng cũng bật mí luôn, khi đã sử dụng HTTPS rồi thì chụp lại mọi lưu lượng chúng đều sẽ bị mã hóa hết.



The screenshot shows a web application window with a header bar containing a user icon and a close button. The main content area displays the following information:

- Firstname:** Jack
- Lastname:** Sparrow
- Credit Card Type:** MC
- Credit Card Number:** 68659365

On the right side, there is a **Logout** link. Below the user details, there are two questions with dropdown menus:

- Is the password still transmitted in plaintext? **Yes** ▾
- Which protocol is used for the transmission? **HTTP** ▾

A **Submit** button is located below the second dropdown. The dropdown menu for the second question is open, showing the following options:

- HTTP** (highlighted)
- IPSEC
- MSNMS
- UDP
- TLS

Okay, login thử vào xem còn gì không. Nó cho ta vài tùy chọn, ở đây chắc là để củng cố kiến thức của ta về HTTPS thôi. Chọn cho đúng các thông số vốn có của 1 giao thức HTTPS là xong bài (TLS + Encode).



Goat Hills Financial Human Resources



Firstname: Jack
Lastname: Sparrow
Credit Card Type: MC
Credit Card Number: 68659365

[Logout](#)

Is the password still transmitted in plaintext?

Which protocol is used for the transmission?

*** Congratulations. You have successfully completed this lesson.**



Goat Hills Financial Human Resources



Please Login

Enter your name:

Enter your password:

2. Insecure Configuration

Nội dung bài này để ta biết khai thác Forced Browsing như thế nào.

Forced Browsing là một cuộc tấn công với mục đích là liệt kê và truy cập các tài nguyên không được ứng dụng tham chiếu nhưng vẫn có thể truy cập được.

Hacker có thể sử dụng các kỹ thuật Brute Force để tìm kiếm các nội dung chưa được liên kết trong thư mục miền, chẳng hạn như các thư mục và tệp tạm thời cũng như các tệp cấu hình và sao lưu cũ. Các tài nguyên này có thể lưu trữ thông tin nhạy cảm về các ứng dụng web và hệ điều hành, chẳng hạn như mã nguồn, thông tin đăng nhập, địa chỉ mạng nội bộ, v.v., đó được coi là tài nguyên có giá trị đối với những kẻ xâm nhập.

* Your goal should be to try to guess the URL for the "config" interface.
* The "config" URL is only available to the maintenance personnel.
* The application doesn't check for horizontal privileges.

Can you try to force browse to the config page which should only be accessed by maintenance personnel.

Mục tiêu bài này là đoán URL của trang config, trang này chỉ dành cho nhân viên bảo trì. Thêm vào đó trang này không kiểm tra đặc quyền theo chiều ngang, tức là ta có thể leo thang đặc quyền theo chiều ngang.

Hiểu 1 chút về 2 kiểu leo thang đặc quyền này thì:

- Nâng cấp đặc quyền theo chiều ngang: Trong hình thức tấn công này, tin tặc vẫn ở cùng mức đặc quyền của người dùng; tuy nhiên, họ có thể truy cập dữ liệu và chức năng của các tài khoản khác không có sẵn với tài khoản hiện có. Nói về các ứng dụng web, một ví dụ về leo thang đặc quyền theo chiều ngang có thể có nghĩa là giành được quyền truy cập vào hồ sơ của người dùng khác có sẵn bằng kỹ thuật số.

- **Nâng cấp đặc quyền theo chiều dọc:** Việc leo thang đặc quyền theo chiều dọc được coi là nguy hiểm hơn leo thang đặc quyền theo chiều ngang. Nâng cấp đặc quyền thường được gọi là nâng cao đặc quyền. Trong hình thức tấn công này, kẻ tấn công bắt đầu từ tài khoản có đặc quyền thấp hơn bằng cách lấy quyền của người dùng cao hơn và mạnh mẽ hơn, như quản trị viên hệ thống. Theo cuộc tấn công leo thang đặc quyền này, kẻ tấn công có thể phá vỡ hệ thống và ứng dụng của những người khác bằng cách lấy đi thông tin đăng nhập và dữ liệu quan trọng khác.

Okay, làm bài thôi. Các bạn có thể sử dụng ZAP, Burp hay Acunetix để quét thử các đường dẫn. Mình thì ngồi mò tay, biết đâu lại ăn may.

Đường dẫn là `*/WebGoat/conf` nhé.

*** Congratulations. You have successfully completed this lesson.**

Welcome to WebGoat Configuration Page

Set Admin Privileges for:

Set Admin Password:

Submit

Created by Sherif Koussa **SoftwareSecured**

OWASP Foundation | Project WebGoat | Report Bug

3. Insecure Storage

Các sơ đồ mã hóa khác nhau có thể được sử dụng trong các ứng dụng web với những lý do khác nhau.

Bài học này chỉ đơn giản là giúp user làm quen với các sơ đồ mã hóa đó.

Enter a string:

Enter a password (optional):

Go!

Description	Encoded	Decoded
Base64 encoding is a simple reversible encoding used to encode bytes into ASCII characters. Useful for making bytes into a printable string, but provides no security.		
Entity encoding uses special sequences like & for special characters. This prevents these characters from being interpreted by most interpreters.		
Password based encryption (PBE) is strong encryption with a text password. Cannot be decrypted without the password	/MI6QLf8NMA=	
MD5 hash is a checksum that can be used to validate a string or byte array, but cannot be reversed to find the original string or bytes. For obscure cryptographic reasons, it is better to use SHA-256 if you have a choice.	1B2M2Y8AsgTpgAmY7PhCfG==	Cannot reverse a hash
SHA-256 hash is a checksum that can be used to validate a string or byte array, but cannot be reversed to find the original string or bytes.	47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=	N/A
Unicode encoding is...	Not Implemented	Not Implemented

Nó cho chúng ta nhập tài khoản và mật khẩu, sau đó sẽ mã hóa dưới nhiều dạng cho chúng ta. Nhập đại 1 giá trị nào đó và xem kết quả mã hóa sẽ ra sao dưới nhiều thuật toán mã hóa.

*** Congratulations. You have successfully completed this lesson.**

Enter a string:

Enter a password (optional):

Description	Encoded	Decoded
Base64 encoding is a simple reversible encoding used to encode bytes into ASCII characters. Useful for making bytes into a printable string, but provides no security.	aGVsbG8=	??
Entity encoding uses special sequences like & for special characters. This prevents these characters from being interpreted by most interpreters.	hello	hello
Password based encryption (PBE) is strong encryption with a text password. Cannot be decrypted without the password	f+S6YA8b0ow=	This is not an encrypted string
MD5 hash is a checksum that can be used to validate a string or byte array, but cannot be reversed to find the original string or bytes. For obscure cryptographic reasons, it is better to use SHA-256 if you have a choice.	XUFAKrxLKna5cZ2REBfFkg=	Cannot reverse a hash
SHA-256 hash is a checksum that can be used to validate a string or byte array, but cannot be reversed to find the original string or bytes.	LPJNul+wow4m6DsqxbninhsWHLwfp0JecwQzYpOLmCQ=	N/A
Unicode encoding is	Not Implemented	Not Implemented