

Authentication

Authentication Technologies

- Có nhiều kỹ thuật chứng thực:
 - HTML forms-based authentication
 - Multifactor mechanisms, Ví dụ: kết hợp passwords và physical tokens
 - Client SSL certificates and/or smartcards
 - HTTP basic and digest authentication
 - Windows-integrated authentication using NTLM or Kerberos
 - Authentication services

Design Flaws in Authentication Mechanisms

- Bad Passwords

- Ngắn hoặc trống
- Dùng các từ thông dụng
- Giống tên đăng nhập
- Dùng mật khẩu mặc định

Design Flaws in Authentication Mechanisms

Hack Steps

Tìm các mô tả về quy tắc đặt mật khẩu có thể có trên Website

Tự đăng ký một số tài khoản để đoán quy tắc đặt mật khẩu

Đổi mật khẩu sang các giá trị có độ dễ khác nhau.

Design Flaws in Authentication Mechanisms

What are the WaveMail password requirements?

Password Rules

- The password is case-sensitive.
- The password can contain uppercase letters and lowercase letters.
- The password can contain numbers.
- The password can contain the following ASCII text characters:
` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /
- The minimum password length is 6 characters.
- The maximum password length is 16 characters.

Password Restrictions The password can't contain any of the following items:

- Spaces.
- Non-English characters.
- The account name part of the e-mail address. For example, if the email address is riptide@tulane.edu, the password can't contain "tide." This restriction isn't case-sensitive. Therefore, "TIDE" or "Tide" can't be used in the password for riptide@tulane.edu.
- The password can't contain the same word that is the answer to the Windows Live ID secret question

Brute-Forcible Login

- Sử dụng hàng loạt các cặp Username, password để đăng nhập thử vào ứng dụng web.
- Có thể dùng các phần mềm để tự động hóa quá trình này: Burpsuite,

Brute-Forcible Login

Hack Steps

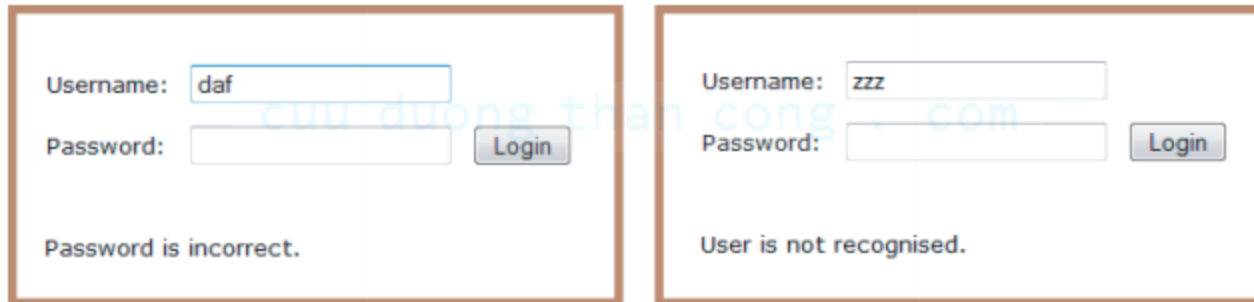
Tiến hành đăng nhập thử và theo dõi thông báo lỗi

Nếu không có thông báo lỗi, chứng tỏ đăng nhập thành công và không có lockout policy

Nếu có lockout policy, dùng tài khoản khác, nên dùng mỗi cookie cho mỗi lần đăng nhập

Đoán các tên đăng nhập khác nhau

Verbose Failure Messages



The image displays two side-by-side login forms, each enclosed in a brown rectangular border. Both forms have a light gray background and a blue watermark reading 'cuu duong than cong . com' across the center.

Left Form: The 'Username:' field contains the text 'daf'. The 'Password:' field is empty. A gray 'Login' button is positioned to the right of the password field. Below the fields, the message 'Password is incorrect.' is displayed in a dark gray font.

Right Form: The 'Username:' field contains the text 'zzz'. The 'Password:' field is empty. A gray 'Login' button is positioned to the right of the password field. Below the fields, the message 'User is not recognised.' is displayed in a dark gray font.

Vulnerable Transmission of Credentials

- Nếu một ứng dụng dùng unencrypted HTTP connection để truyền thông tin đăng nhập, kẻ nghe trộm có thể thu thập các thông tin này tùy vào vị trí khác nhau: [cuu duong than cong . com](http://cuuduongthancong.com)
 - user's local network
 - user's IT department
 - user's ISP
 - Internet backbone
 - ISP hosting the application
 - IT department managing the application

Vulnerable Transmission of Credentials (2)

- Thậm chí thông tin đăng nhập cũng có thể bị phơi bày khi dùng HTTPS mà không có cơ chế quản lý an toàn:
 - Gửi các thông tin đăng nhập qua string parameter, lưu ở webbrowser history, log của webserver.
 - Lưu thông tin đăng nhập trong cookie, “Remember me.”, nguy cơ cho tấn công replay
- Chuyển sang HTTPs cho các khu vực đăng nhập => Attacker có thể chặn và chỉnh sửa các form đăng nhập để chuyển URL sang HTTP thay vì HTTPs trước khi nghe lén thông tin đăng nhập.

Password Change Functionality

- Ưu điểm
 - Cho phép thay đổi mật khẩu thường xuyên hơn, đảm bảo tính mới của mật khẩu.
 - Cho phép thay đổi mật khẩu nhanh khi xảy ra việc bị lộ mật khẩu.
- Tuy nhiên:
 - Mật khẩu mới và xác nhận mật khẩu mới chỉ diễn ra nếu như mật khẩu cũ đúng => ?

Forgotten Password Functionality

Forgot Your Password or User ID?

User Id: **Tim**

When you registered your User Id, you provided a secret question.

Your secret question, provided during registration, is:

what street did you live on in sierra vista

Enter the answer to your secret question:

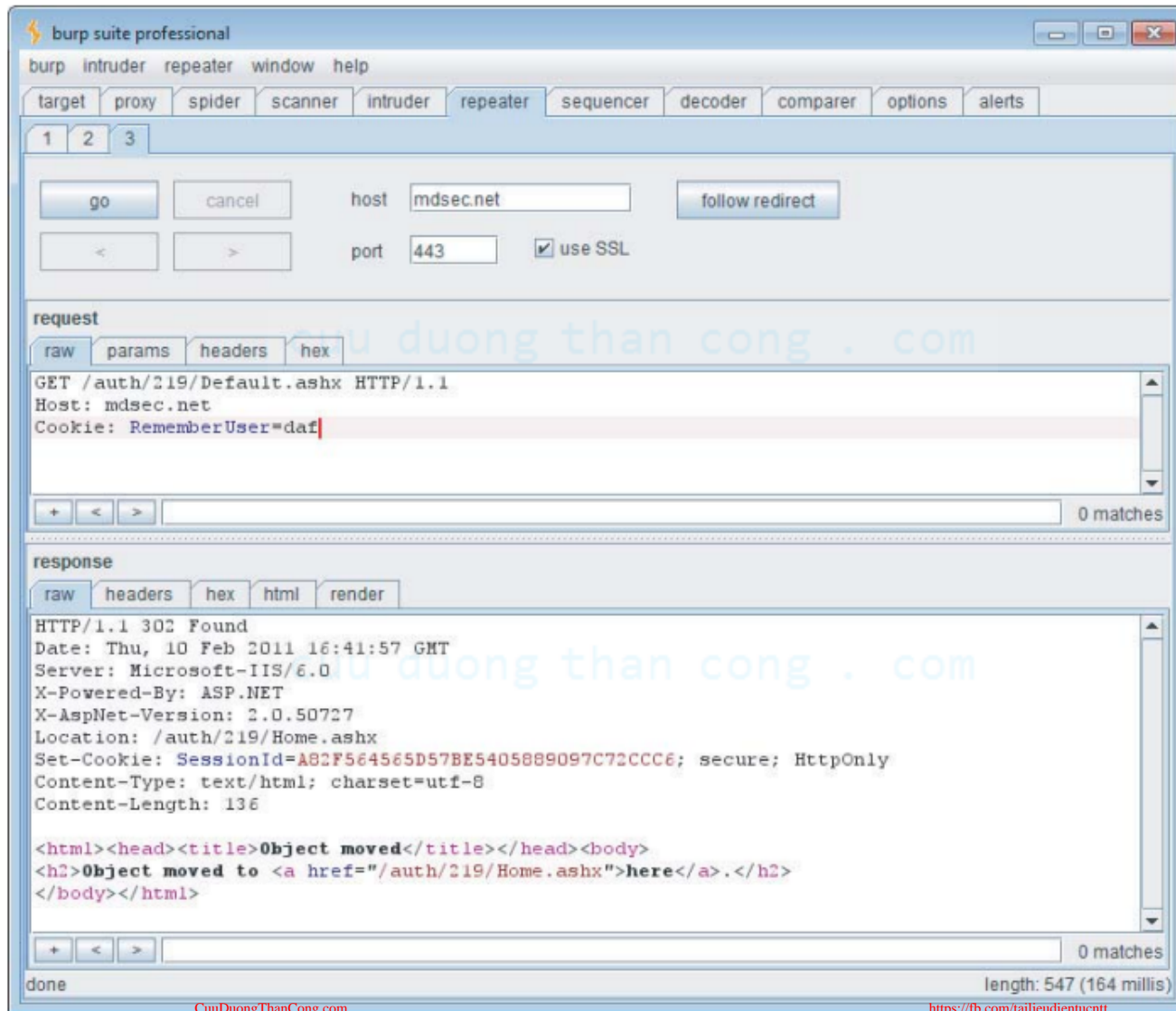
 CONTINUE

Forgotten Password Functionality (2)

HACK STEPS

1. Identify any forgotten password functionality within the application. If this is not explicitly linked from published content, it may still be implemented (see Chapter 4).
2. Understand how the forgotten password function works by doing a complete walk-through using an account you control.
3. If the mechanism uses a challenge, determine whether users can set or select their own challenge and response. If so, use a list of enumerated or common usernames to harvest a list of challenges, and review this for any that appear easily guessable.
4. If the mechanism uses a password “hint,” do the same exercise to harvest a list of password hints, and target any that are easily guessable.
5. Try to identify any behavior in the forgotten password mechanism that can be exploited as the basis for username enumeration or brute-force attacks (see the previous details).
6. If the application generates an e-mail containing a recovery URL in response to a forgotten password request, obtain a number of these URLs, and attempt to identify any patterns that may enable you to predict the URLs issued to other users. Employ the same techniques as are relevant to analyzing session tokens for predictability (see Chapter 7).

“Remember Me” Functionality



“Remember Me” Functionality

HACK STEPS

1. **Activate any “remember me” functionality, and determine whether the functionality indeed does fully “remember” the user or whether it remembers only his username and still requires him to enter a password on subsequent visits. If the latter is the case, the functionality is much less likely to expose any security flaw.**
2. **Closely inspect all persistent cookies that are set, and also any data that is persisted in other local storage mechanisms, such as Internet Explorer’s userData, Silverlight isolated storage, or Flash local shared objects. Look for any saved data that identifies the user explicitly or appears to contain some predictable identifier of the user.**
3. **Even where stored data appears to be heavily encoded or obfuscated, review this closely. Compare the results of “remembering” several very similar usernames and/or passwords to identify any opportunities to reverse-engineer the original data. Here, use the same techniques that are described in Chapter 7 to detect meaning and patterns in session tokens.**
4. **Attempt to modify the contents of the persistent cookie to try to convince the application that another user has saved his details on your computer.**

Incomplete Validation of Credentials

HACK STEPS

1. Using an account you control, attempt to log in with variations on your own password: removing the last character, changing the case of a character, and removing any special typographical characters. If any of these attempts is successful, continue experimenting to try to understand what validation is actually occurring.
2. Feed any results back into your automated password-guessing attacks to remove superfluous test cases and improve the chances of success.

cuu duong than cong . com

Nonunique Usernames

HACK STEPS

1. If self-registration is possible, attempt to register the same username twice with different passwords.
2. If the application blocks the second registration attempt, you can exploit this behavior to enumerate existing usernames even if this is not possible on the main login page or elsewhere. Make multiple registration attempts with a list of common usernames to identify the already registered names that the application blocks.
3. If the registration of duplicate usernames succeeds, attempt to register the same username twice with the same password, and determine the application's behavior:
 - a. If an error message results, you can exploit this behavior to carry out a brute-force attack, even if this is not possible on the main login page. Target an enumerated or guessed username, and attempt to register this username multiple times with a list of common passwords. When the application rejects a specific password, you have probably found the existing password for the targeted account.
 - b. If no error message results, log in using the credentials you specified, and see what happens. You may need to register several users, and modify different data held within each account, to understand whether this behavior can be used to gain unauthorized access to other users' accounts.

Predictable Usernames

HACK STEPS

1. If the application generates usernames, try to obtain several in quick succession, and determine whether any sequence or pattern can be discerned.
2. If it can, extrapolate backwards to obtain a list of possible valid usernames. This can be used as the basis for a brute-force attack against the login and other attacks where valid usernames are required, such as the exploitation of access control flaws (see Chapter 8).

cuu duong than cong . com

Predictable Initial Passwords

HACK STEPS

1. If the application generates passwords, try to obtain several in quick succession, and determine whether any sequence or pattern can be discerned.
2. If it can, extrapolate the pattern to obtain a list of passwords for other application users.
3. If passwords demonstrate a pattern that can be correlated with usernames, you can try to log in using known or guessed usernames and the corresponding inferred passwords.
4. Otherwise, you can use the list of inferred passwords as the basis for a brute-force attack with a list of enumerated or common usernames.

Nhóm	Tên đề tài
1	OWASP
2	OpenVAS
3	Accunetix
4	Nikto – Web Server Scanner
5	NMAP – Network Mapper
6	VEGA – Vulnerability Scanner
7	SearchSploit – Exploit Database
8	ARACHNI – Web application audit framework
9	sqlmap
10	www.sonarqube.org
11	Burpsuit
12	metasploit
13	W3afis - Web Application Attack and Audit Framework
14	Dradis: an open source framework (a web application) that helps with maintaining the information that can be shared among the participants of a pen-test

BeEF is short for The Browser Exploitation Framework

Luật an toàn thông tin mạng áp dụng từ ngày nào?



Full Screen

Next



Show media

End Game



01/08/2017



01/07/2016



01/08/2016



01/08/2015

cuu duong than cong . com

cuu duong than cong . com

cuu duong than cong . com

cuu duong than cong . com