



Bảo mật ứng dụng web

WWW.UIT.EDU.VN



TS. Nguyễn Tấn Cầm



Nội dung



- Giới thiệu ứng dụng web
- Kiến trúc ứng dụng web
- Các nguy cơ bảo mật ứng dụng web phổ biến
- Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web
- Kiểm thử an toàn ứng dụng web
- Câu hỏi ôn tập



Giới thiệu ứng dụng web



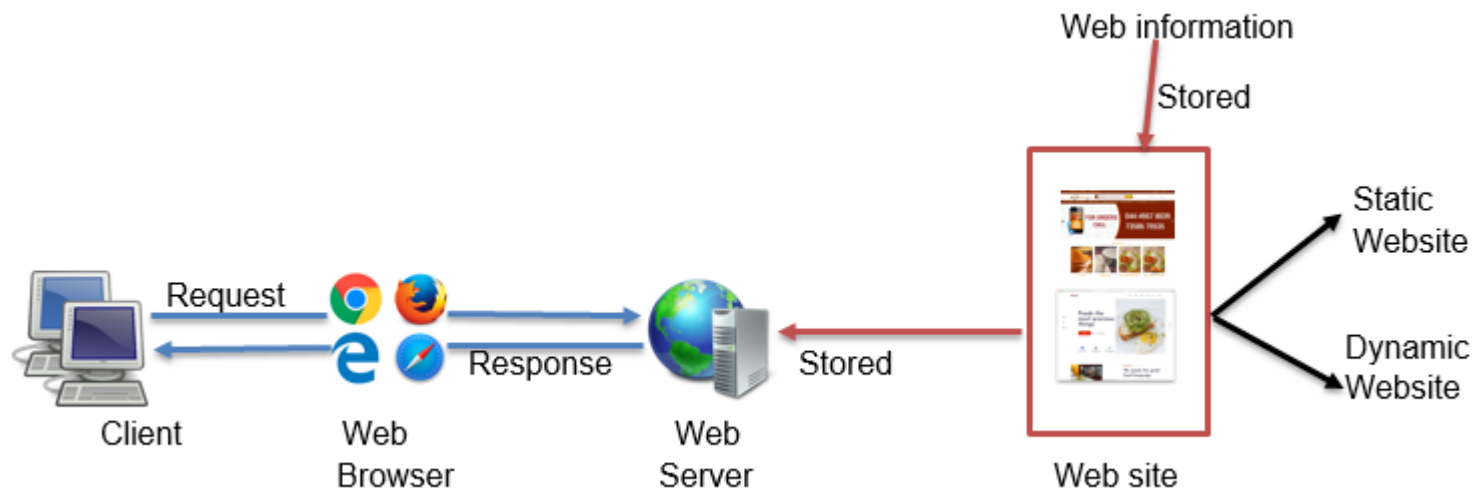
Giới thiệu ứng dụng web



- Ứng dụng web là phần mềm chạy trên trình duyệt web và đóng vai trò như một cầu nối giữa người dùng và máy chủ thông qua các trang web.
- Chúng giúp người dùng truy vấn, gửi và nhận dữ liệu từ cơ sở dữ liệu trên Internet thông qua các tương tác với giao diện đồ họa (graphical user interface).
- Ứng dụng web giúp tạo các trang web linh hoạt hơn.
- Chúng cho phép người dùng thực hiện các tác vụ như tìm kiếm, gửi mail, kết nối với bạn bè, mua sắm trực tuyến, ...
- Có rất nhiều các dịch vụ được xây dựng trên nền tảng web app và mỗi khi người dùng cần sử dụng các dịch vụ này, họ chỉ cần gửi các URI hay URL trên trình duyệt web.
- Trình duyệt sau đó sẽ chuyển yêu cầu này đến máy chủ nơi chứa dữ liệu của các ứng dụng web này để chúng xử lý.
- Một vài máy chủ web phổ biến có thể kể như: Microsoft IIS, Apache,...

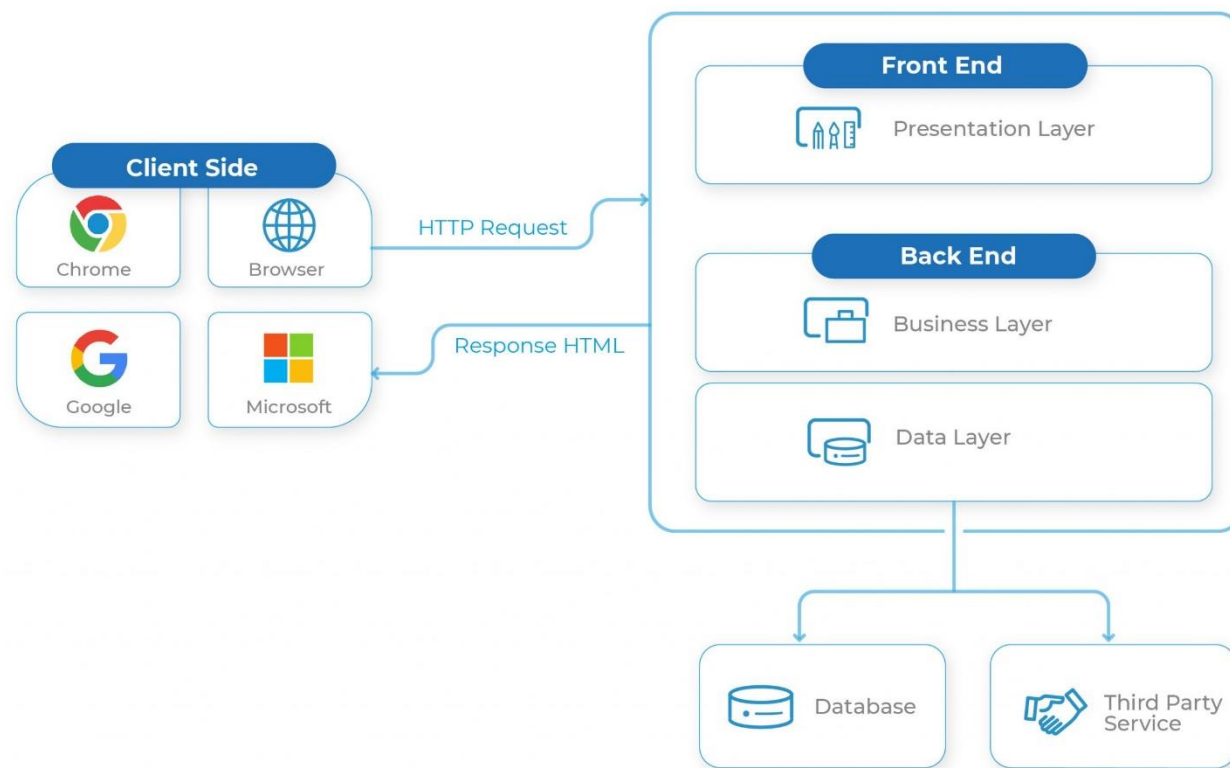


Giới thiệu ứng dụng web





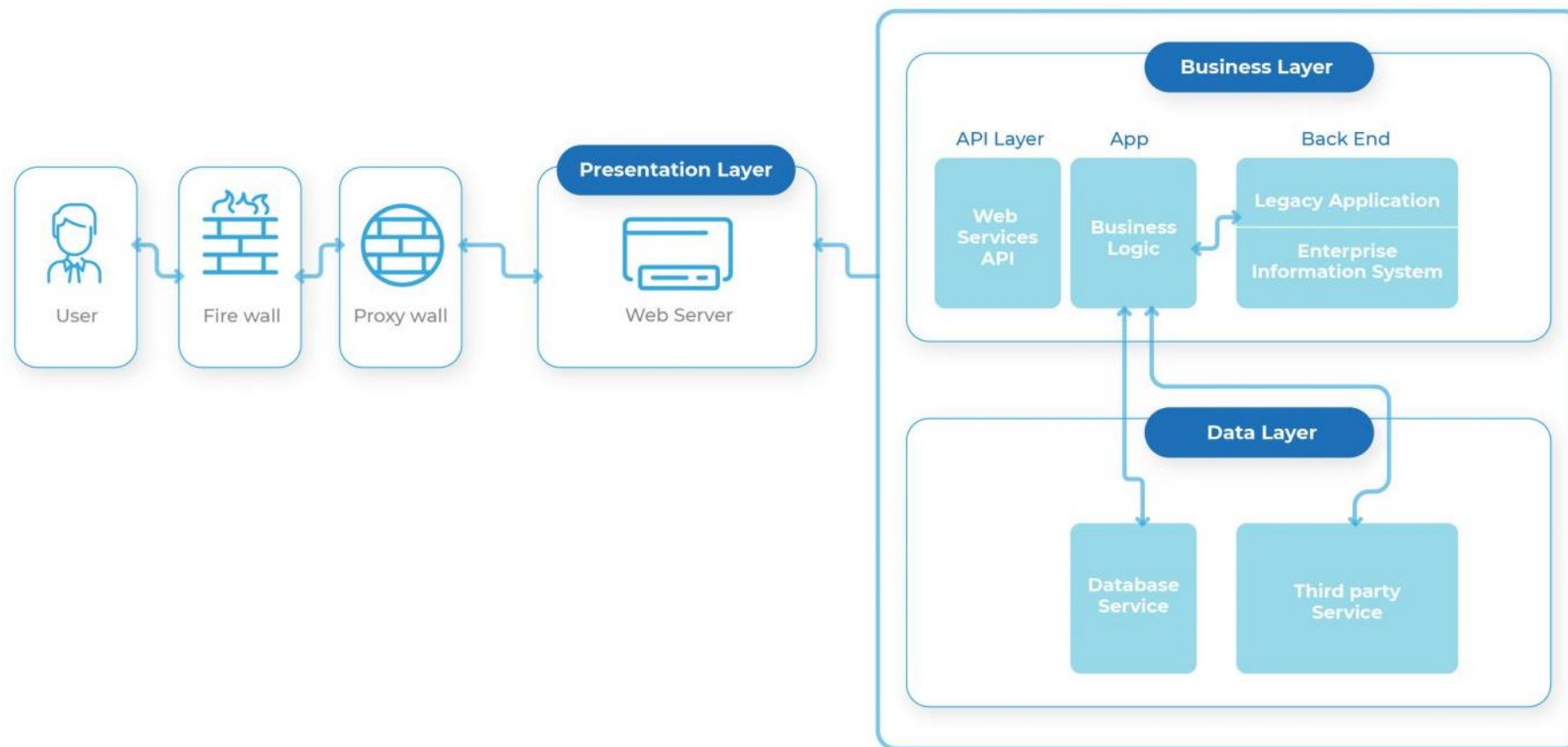
Kiến trúc ứng dụng web



Kiến trúc hai tầng của ứng dụng web



Kiến trúc ứng dụng web



Kiến trúc ba tầng của ứng dụng web



Kiến trúc ứng dụng web



- Ưu điểm của các ứng dụng web
 - Hoạt động được trên nhiều hệ điều hành khác nhau.
 - Truy cập mọi lúc mọi nơi với một máy tính có kết nối Internet
 - Người dùng có thể truy cập thông qua bất kì thiết bị nào có trình duyệt web và được kết nối Internet.
 - Ứng dụng có thể được đặt trên nhiều máy chủ giúp tăng bảo mật vật lý, giảm nguy cơ bị theo dõi.
 - Sử dụng các công nghệ lõi như JSP, Servlets, SQL Server,... và ngôn ngữ kịch bản (scripting language) như .NET giúp dễ mở rộng và hỗ trợ cả các nền tảng di động.



Kiến trúc ứng dụng web



- Mặc dù ứng dụng web sẽ có các chính sách về an toàn thông tin nhưng chúng cũng dễ bị tấn công bởi SQL injection, cross-site scripting, session hijacking,... trong quá trình vận hành.
- Việc bảo trì và truy cập các ứng dụng web trải qua rất nhiều lớp bao gồm các ứng dụng chuyên biệt cho web, thành phần bên thứ ba, cơ sở dữ liệu, máy chủ, hệ điều hành, mạng và bảo mật.
- Tất cả những cơ chế và dịch vụ được sử dụng ở mỗi lớp đều giúp người dùng truy cập đến trang web một cách an toàn hơn.
- Danh sách các lớp dưới đây thể hiện các phân tầng và các cơ chế, yếu tố hoặc dịch vụ ở mỗi lớp khiến cho trang web dễ bị tấn công



Kiến trúc ứng dụng web



- Danh sách các lớp dưới đây thể hiện các phân tầng và các cơ chế, yếu tố hoặc dịch vụ ở mỗi lớp khiến cho trang web dễ bị tấn công

Lớp 7	• Mức logic và ứng dụng web
Lớp 6	• Mức thư viện của bên thứ ba
Lớp 5	• Mức cơ sở dữ liệu
Lớp 4	• Mức hệ điều hành máy chủ web
Lớp 3	• Mức các dịch vụ
Lớp 2	• Mức thiết bị mạng
Lớp 1	• Mức máy chủ web



Các nguy cơ bảo mật ứng dụng web phổ biến

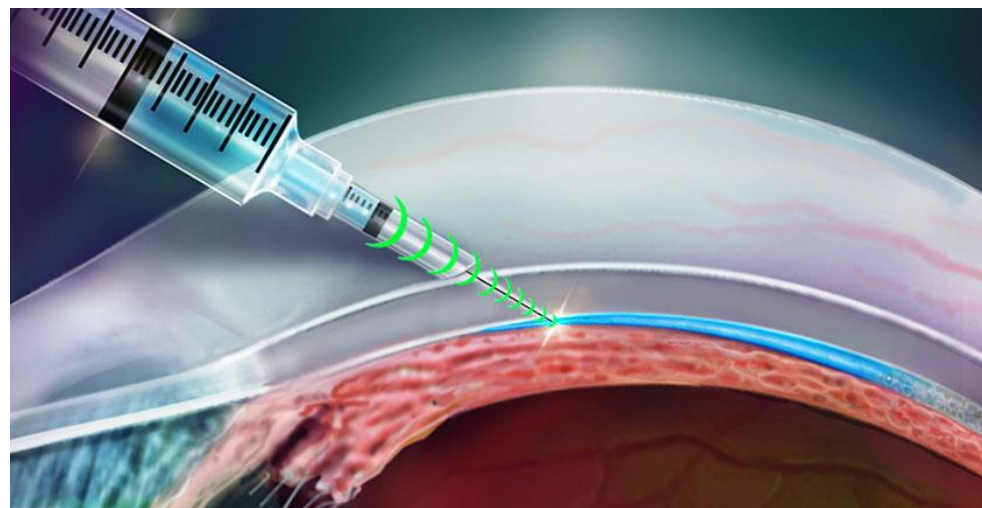


Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi injection

- Là lỗi hỏng ứng dụng web cho phép dữ liệu không đáng tin được diễn giải và thực thi như một phần của câu lệnh hoặc truy vấn.
- Những kẻ tấn công khai thác các lỗi này bằng cách sử dụng các lệnh hoặc truy vấn độc hại dẫn đến mất mát hoặc hỏng dữ liệu.
- Từ đó, những kẻ tấn công có thể dễ dàng đọc, ghi, xóa và cập nhật dữ liệu liên quan.
- Các lỗi injection phổ biến trong mã kế thừa, thường được tìm thấy trong các truy vấn SQL, LDAP và XPath, v.v. và có thể dễ dàng được phát hiện bởi các công cụ quét lỗi hỏng ứng dụng.





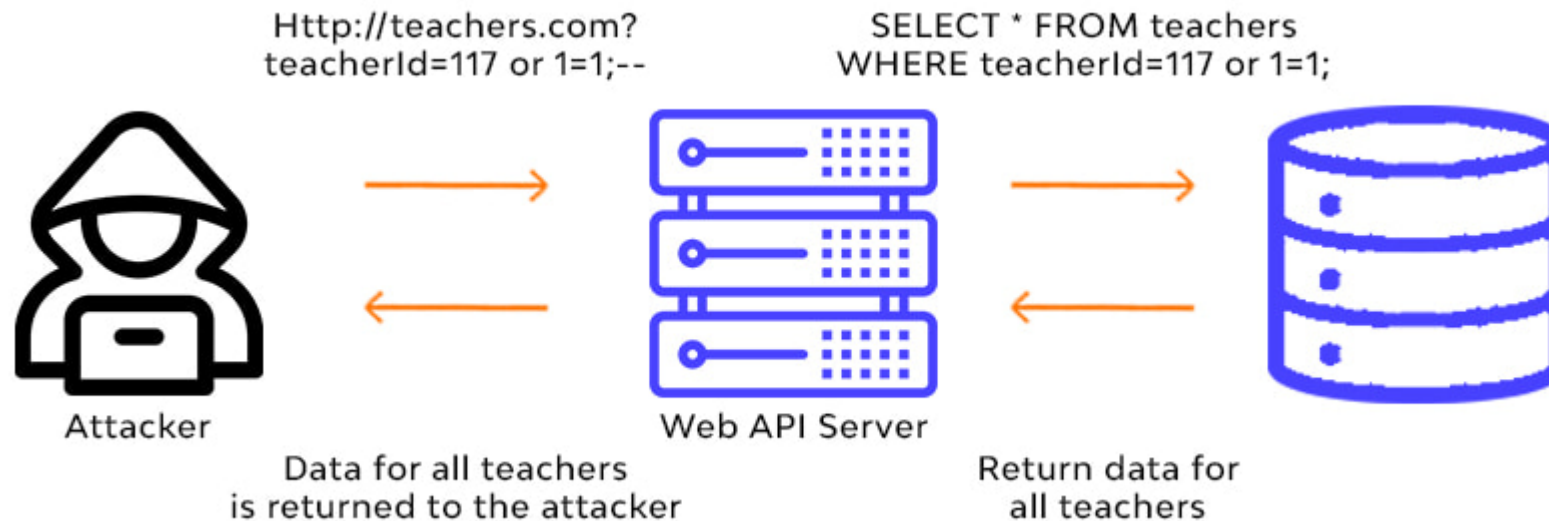
Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi injection

- SQL Injection

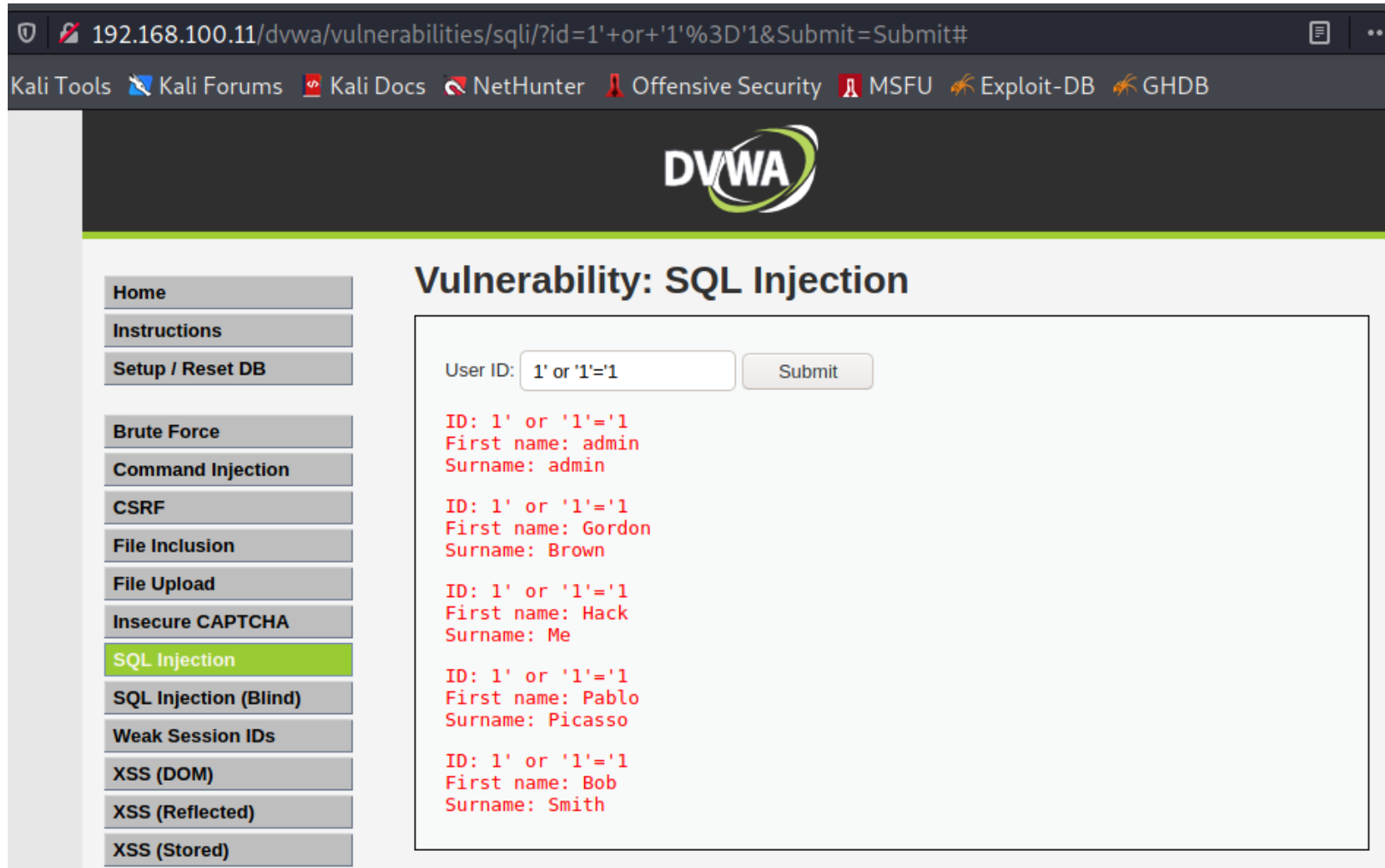
- Lỗi hỏng trang web phổ biến nhất trên Internet và được sử dụng để tận dụng các lỗ hổng đầu vào không được xác thực.
 - Trong kỹ thuật này, kẻ tấn công đưa các truy vấn SQL độc hại vào biểu mẫu đầu vào của người dùng để truy cập trái phép vào cơ sở dữ liệu hoặc để lấy thông tin trực tiếp từ cơ sở dữ liệu.





Các nguy cơ bảo mật ứng dụng web phổ biến

- Lỗi injection
 - SQL Injection



192.168.100.11/dvwa/vulnerabilities/sqli/?id=1'+or+'1'%3D'1&Submit=Submit#

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

DVWA

Vulnerability: SQL Injection

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)

User ID: Submit

ID: 1' or '1'='1
First name: admin
Surname: admin

ID: 1' or '1'='1
First name: Gordon
Surname: Brown

ID: 1' or '1'='1
First name: Hack
Surname: Me

ID: 1' or '1'='1
First name: Pablo
Surname: Picasso

ID: 1' or '1'='1
First name: Bob
Surname: Smith



Các nguy cơ bảo mật ứng dụng web phổ biến

- Lỗi injection

- Command Injection:

- Những kẻ tấn công khai thác lỗ hổng bằng cách đưa vào ứng dụng một lệnh độc hại để thực thi các lệnh tùy ý được cung cấp trên hệ điều hành máy chủ.





Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi injection

- LDAP Injection:

- LDAP injection là một phương pháp tấn công trong đó các trang web xây dựng các câu lệnh LDAP từ đầu vào do người dùng cung cấp bị khai thác để khởi chạy các cuộc tấn công.
 - Khi một ứng dụng không thể “làm sạch” đầu vào của người dùng, thì kẻ tấn công sẽ sửa đổi câu lệnh LDAP.
 - Điều này dẫn đến việc thực thi các lệnh tùy ý như cấp quyền truy cập vào các truy vấn trái phép và thay đổi nội dung bên trong kho dữ liệu LDAP.

Example 1: Data leakage

Original Query	http://ribadeohacklab.com.ar/people_search.aspx?name=John)(zone=public)
Malformed Query	http://ribadeohacklab.com.ar/people_search.aspx?name=John)(zone=*)
Result	By default the application is meant to give person details only from the 'public' zone. The hacker can bypass this limit by using wildcard.

Example 2: Data Integrity

Code	<?php \$attr["cn"] = "ToModify"; \$dn = "uid=Ribadeo,ou=People,dc=foo"; \$result = ldap_modify(\$ldapconn,\$dn, \$attr); if (TRUE === \$result) { echo "Entry was modified."; } else { echo "Entry could not be modified."; } ?>
Malformed Query	\$dn = "uid=Ribadeo,ou=People,dc=*"
Result	All CN entries under the branch will be modified with the "ToModify" value.



Các nguy cơ bảo mật ứng dụng web phổ biến

WWW.UIT.EDU.VN



- Lỗi injection

- File Injection:

- Đây là loại tấn công mà kẻ tấn công lợi dụng cơ chế chèn tập tin tự động vào ứng dụng web. Khi đó, nếu chúng ta không kiểm tra kỹ đường dẫn và tên tập tin trước khi thực thi yêu cầu sẽ gây nên các nguy cơ bảo mật.
 - Ví dụ:
 - <http://trangweb.com/chenganh.php?PIC=http://webdochai.com/exploit>



Các nguy cơ bảo mật ứng dụng web phổ biến

WWW.UIT.EDU.VN



- Lỗi injection

- Chúng ta có thể sử dụng các cách sau để hạn chế lỗ hổng bảo mật liên quan đến Injection:
 - Tùy chọn ưu tiên là sử dụng API an toàn, tránh sử dụng hoàn toàn trình thông dịch hoặc cung cấp giao diện được tham số hóa.
 - Sử dụng xác thực đầu vào phía máy chủ.
 - Đối với bất kỳ truy vấn động nào còn lại, hãy lọc các ký tự đặc biệt bằng cách sử dụng cú pháp lọc cụ thể cho trình thông dịch đó.
 - Sử dụng LIMIT và các điều khiển SQL khác trong các truy vấn để ngăn tiết lộ hàng loạt các bản ghi trong trường hợp chèn SQL



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi xác thực
 - Các chức năng của ứng dụng Web liên quan đến quá trình chứng thực và quản lý phiên có thể được triển khai không đúng cách.
 - Kẻ tấn công có thể sử dụng các lỗ hổng trong chức năng xác thực hoặc quản lý phiên để thực hiện việc đánh cắp thông tin tài khoản, mã phiên đăng nhập, quản lý mật khẩu, và những thứ khác để mạo danh người dùng



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi xác thực
 - Đánh cắp thông tin phiên đăng nhập
 - Ứng dụng web tạo mã cho phiên đăng nhập tương ứng khi người dùng đăng nhập vào trang web.
 - Kẻ tấn công sử dụng công cụ khác nhau để đánh cắp cookie có chứa thông tin phiên đăng nhập hoặc đánh lừa người dùng để lấy thông tin phiên đăng nhập.
 - Kẻ tấn công sẽ sử dụng thông tin này để chuyển hướng đến trang đã đăng nhập của nạn nhân.
 - Khai thác mật khẩu
 - Những kẻ tấn công có thể xác định mật khẩu được lưu trữ trong cơ sở dữ liệu vì thuật toán băm yếu.
 - Những kẻ tấn công có thể truy cập vào cơ sở dữ liệu mật khẩu của ứng dụng web nếu mật khẩu của người dùng không được mã hóa, điều này cho phép kẻ tấn công khai thác mật khẩu của mọi người dùng.
 - Khai thác thời gian chờ
 - Nếu thời gian chờ phiên của ứng dụng được đặt trong thời gian dài hơn, thì khi người dùng chỉ cần đóng trình duyệt mà không đăng xuất khỏi các trang web được truy cập thông qua máy tính công cộng, kẻ tấn công có thể sử dụng cùng một trình duyệt sau đó để tiến hành cuộc tấn công, vì ID phiên có thể vẫn còn hiệu lực và khai thác các đặc quyền của người dùng.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi xác thực

- Chúng ta có thể sử dụng các phương thức sau đây để hạn chế lỗi xác thực của ứng dụng web [34]
 - Nếu có thể, hãy triển khai xác thực đa yếu tố để ngăn chặn các cuộc tấn công tự động, nhồi nhét thông tin xác thực và các cuộc tấn công tái sử dụng thông tin xác thực bị đánh cắp.
 - Không gửi hoặc sử dụng với bất kỳ thông tin đăng nhập mặc định nào, đặc biệt là đối với người dùng quản trị.
 - Thực hiện kiểm tra mật khẩu yếu, chẳng hạn như kiểm tra mật khẩu mới hoặc đã thay đổi dựa trên danh sách mật khẩu kém nhất, phổ biến nhất.
 - Điều chỉnh độ dài, độ phức tạp và các chính sách xoay vòng của mật khẩu.
 - Đảm bảo các đường dẫn đăng ký, khôi phục thông tin xác thực và API được tăng cường chống lại các cuộc tấn công liệt kê tài khoản bằng cách sử dụng các thông báo giống nhau cho tất cả các kết quả.
 - Hạn chế hoặc ngày càng trì hoãn các lần đăng nhập không thành công.
 - Ghi nhật ký tất cả các lỗi và cảnh báo cho quản trị viên khi phát hiện thấy hành vi nhồi nhét thông tin xác thực, tấn công vét cạn, tấn công theo từ điển hoặc các cuộc tấn công khác.
 - Sử dụng trình quản lý phiên tích hợp, an toàn, phía máy chủ tạo mã phiên ngẫu nhiên mới với entropy cao sau khi đăng nhập.
 - Mã phiên không được có trong URL, được lưu trữ an toàn và bị vô hiệu hóa sau khi đăng xuất, không hoạt động và hết thời gian chờ tuyệt đối.



Các nguy cơ bảo mật ứng dụng web phổ biến



- **Lộ thông tin nhạy cảm**
 - Ứng dụng web cần lưu trữ thông tin nhạy cảm như mật khẩu, số thẻ tín dụng, hồ sơ tài khoản hoặc thông tin xác thực khác trong cơ sở dữ liệu hoặc trên hệ thống.
 - Nếu người dùng không duy trì sự bảo mật thích hợp cho các vị trí lưu trữ này của họ, thì ứng dụng có thể gặp rủi ro, vì những kẻ tấn công có thể truy cập vào cơ sở dữ liệu thông qua các lỗ hổng có thể có và sử dụng chúng.
 - Mặc dù dữ liệu được mã hóa, tuy nhiên, một số phương pháp mã hóa mật mã có điểm yếu cố hữu cho phép kẻ tấn công khai thác và đánh cắp dữ liệu.
 - Khi một ứng dụng sử dụng các công cụ mã hóa yếu, kẻ tấn công có thể dễ dàng khai thác lỗ hổng này và đánh cắp hoặc sửa đổi dữ liệu nhạy cảm.
 - Các nhà phát triển có thể tránh các cuộc tấn công như vậy bằng cách sử dụng các thuật toán mã hóa thích hợp để mã hóa dữ liệu này. Đồng thời, phải quan tâm đến việc lưu trữ các khóa mật mã một cách an toàn.
 - Nếu những khóa này được lưu trữ ở những nơi không an toàn, thì những kẻ tấn công có thể lấy chúng dễ dàng và giải mã dữ liệu. Việc lưu trữ khóa, chứng chỉ và mật khẩu không an toàn cũng cho phép kẻ tấn công có quyền truy cập vào ứng dụng web với tư cách là người dùng hợp pháp



Các nguy cơ bảo mật ứng dụng web phổ biến



- Sử dụng các đối tượng tham chiếu từ bên ngoài
 - Tấn công XML là một cuộc tấn công truy vấn yêu cầu phía máy chủ (SSRF) trong đó ứng dụng có thể phân tích cú pháp đầu vào XML từ một nguồn không đáng tin cậy do trình phân tích cú pháp XML được cấu hình sai.
 - Trong cuộc tấn công này, kẻ tấn công sẽ gửi một đầu vào XML độc hại chứa tham chiếu đến một thực thể bên ngoài tới ứng dụng web nạn nhân.
 - Khi đầu vào độc hại này được xử lý bởi trình phân tích cú pháp XML được cấu hình yếu của ứng dụng web mục tiêu, nó cho phép kẻ tấn công truy cập các tập tin và dịch vụ được bảo vệ từ máy chủ hoặc mạng được kết nối.
 - Vì các tính năng XML có sẵn và được sử dụng rộng rãi, kẻ tấn công lợi dụng các tính năng này để tạo tài liệu hoặc tập tin động tại thời điểm xử lý.
 - Những kẻ tấn công sẽ tận dụng tối đa cuộc tấn công này vì nó giúp việc truy xuất dữ liệu bí mật, tấn công DoS, tiết lộ thông tin nhạy cảm qua giao thức http và trong một số trường hợp xấu nhất, chúng có thể dẫn đến việc thực thi mã từ xa hoặc khởi chạy cuộc tấn công CSRF [35] trên bất kỳ dịch vụ dễ bị tấn công nào.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Sử dụng các đối tượng tham chiếu từ bên ngoài
 - Để giảm thiểu nguy cơ bảo mật khi sử dụng các đối tượng bên ngoài, chúng ta có thể sử dụng các phương thức sau:
 - Bất cứ khi nào có thể, hãy sử dụng các định dạng dữ liệu ít phức tạp hơn như JSON.
 - Vá hoặc nâng cấp tất cả các bộ xử lý và thư viện XML đang được ứng dụng hoặc trên hệ điều hành đang sử dụng. Sử dụng bộ kiểm tra phụ thuộc.
 - Tắt thực thể bên ngoài XML trong tất cả các trình phân tích cú pháp XML trong ứng dụng.
 - Triển khai xác thực, lọc hoặc kiểm tra đầu vào phía máy chủ để ngăn chặn dữ liệu độc hại trong các tài liệu, tiêu đề hoặc nút XML.
 - Sử dụng các công cụ kiểm tra tự động như SCAT [36] để kiểm tra các bất thường trong mã nguồn, mặc dù xem xét mã thủ công là giải pháp thay thế tốt nhất trong các ứng dụng lớn, phức tạp với nhiều tích hợp. Nếu các biện pháp kiểm soát này không thể thực hiện được, hãy xem xét sử dụng cổng bảo mật API hoặc Tường lửa ứng dụng web (WAF) để phát hiện, giám sát và chặn các cuộc tấn công sử dụng đối tượng ngoài



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi kiểm soát truy cập
 - Kiểm soát truy cập là việc một ứng dụng web cấp quyền truy cập để tạo, cập nhật và xóa các bản ghi và nội dung.
 - Nó cũng bao gồm các kỹ thuật phân quyền sử dụng chức năng của ứng dụng web cho một số người dùng có đặc quyền và hạn chế những người dùng khác.
 - Lỗi kiểm soát truy cập là một phương pháp trong đó kẻ tấn công xác định một lỗ hổng liên quan đến kiểm soát truy cập và bỏ qua việc xác thực, sau đó xâm nhập vào hệ thống.
 - Các điểm yếu của kiểm soát truy cập khá phổ biến do thiếu sự phát hiện tự động và thiếu kiểm tra tính hiệu quả các chức năng bởi các nhà phát triển ứng dụng.
 - Nó cho phép kẻ tấn công hoạt động như người dùng hoặc quản trị viên với các chức năng đặc quyền và tạo, truy cập, cập nhật hoặc xóa các bản ghi.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi kiểm soát truy cập
 - Lỗi kiểm soát truy cập là sự kết hợp của tham chiếu đối tượng trực tiếp không an toàn và kiểm soát truy cập cấp chức năng bị thiếu.
 - Tham chiếu đối tượng trực tiếp không an toàn:
 - Khi các nhà phát triển để lộ các đối tượng triển khai nội bộ khác nhau như tập tin, thư mục, bản ghi cơ sở dữ liệu, kết quả là tham chiếu đối tượng trực tiếp không an toàn. Ví dụ: nếu số tài khoản ngân hàng là khóa chính, có khả năng ứng dụng bị xâm nhập bởi những kẻ tấn công lợi dụng các tham chiếu đó.
 - Thiếu kiểm soát truy cập mức chức năng:
 - Trong một số ứng dụng web, bảo vệ mức chức năng được quản lý thông qua cấu hình và những kẻ tấn công khai thác các lỗ hổng kiểm soát truy cập mức chức năng này để truy cập chức năng trái phép. Mục tiêu chính của những kẻ tấn công trong kịch bản này sẽ là các chức năng quản trị. Các nhà phát triển phải kiểm tra các mã thích hợp để ngăn chặn các cuộc tấn công vì kẻ tấn công dễ dàng phát hiện ra những sai sót như vậy. Tuy nhiên, việc xác định các chức năng dễ bị tấn công hoặc các trang web dễ tấn công là rất khó và cần có thời gian



Các nguy cơ bảo mật ứng dụng web phổ biến



- Lỗi kiểm soát truy cập

- Kiểm soát truy cập chỉ hiệu quả nếu được thực thi trong mã phía máy chủ đáng tin cậy hoặc API phía máy chủ, nơi kẻ tấn công không thể sửa đổi kiểm tra kiểm soát truy cập hoặc siêu dữ liệu.
- Chúng ta có thể thực hiện các phương thức sau để giảm thiểu ảnh hưởng của lỗi kiểm soát truy cập:
 - Ngoại trừ các tài nguyên công cộng, hãy từ chối theo mặc định.
 - Thực hiện các cơ chế kiểm soát truy cập một lần và sử dụng lại chúng trong toàn bộ ứng dụng.
 - Kiểm soát truy cập phải thực thi quyền sở hữu bản ghi, thay vì chấp nhận rằng người dùng có thể tạo, đọc, cập nhật hoặc xóa bất kỳ bản ghi nào.
 - Vô hiệu hóa danh sách thư mục máy chủ web và đảm bảo các tập tin siêu dữ liệu (ví dụ: .git) và tập tin sao lưu không có trong thư mục gốc của trang web.
 - Ghi nhật ký các lỗi kiểm soát truy cập, cảnh báo cho quản trị viên khi thích hợp (ví dụ: các lỗi lặp lại).
 - Quyền truy cập API giới hạn tỷ lệ với bộ điều khiển để giảm thiểu tác hại từ công cụ tấn công tự động.
 - Các nhà phát triển và nhân viên kiểm thử nên tích hợp quy trình kiểm soát truy cập chức năng và các bài kiểm tra tích hợp



Các nguy cơ bảo mật ứng dụng web phổ biến



- Thiếu cấu hình bảo mật
 - Các nhà phát triển và quản trị viên mạng nên đảm bảo rằng toàn bộ ứng dụng được cấu hình đúng cách, nếu không, cấu hình bảo mật sai có thể xảy ra ở bất kỳ thành phần nào liên quan đến ứng dụng web.
 - Ví dụ: nếu nhà phát triển không cấu hình máy chủ đúng cách, điều này có thể dẫn đến các vấn đề khác nhau dẫn đến lỗi bảo mật trang web.
 - Các vấn đề dẫn đến các trường hợp như vậy bao gồm dữ liệu đầu vào chưa được xác thực, giả mạo tham số, biểu mẫu, xử lý lỗi không đúng, dữ liệu không được mã hóa khi truyền thông,...



Các nguy cơ bảo mật ứng dụng web phổ biến



- Thiếu cấu hình bảo mật
 - Đầu vào chưa được kiểm chứng
 - Giả mạo tham số, biểu mẫu
 - Xử lý lỗi không phù hợp
 - Bảo vệ lớp truyền tải không đủ



Các nguy cơ bảo mật ứng dụng web phổ biến



- Thiếu cấu hình bảo mật

- Chúng ta có thể sử dụng các cách sau để giảm thiểu nguy cơ tấn công ứng dụng web do thiếu cấu hình bảo mật:
 - Tất cả các môi trường phát triển, kiểm thử và sản xuất phải được cấu hình giống nhau, với các thông tin xác thực khác nhau được sử dụng trong mỗi môi trường. Quá trình này phải được tự động hóa để giảm thiểu nỗ lực cần thiết để thiết lập một môi trường an toàn mới.
 - Một nền tảng tối thiểu không có bất kỳ tính năng, thành phần, tài liệu và mẫu không cần thiết nào. Loại bỏ hoặc không cài đặt các tính năng và thư viện không sử dụng.
 - Nhiệm vụ xem xét và cập nhật các cấu hình phù hợp với tất cả các ghi chú bảo mật, bản cập nhật và bản vá như một phần của quy trình quản lý bản vá Đặc biệt, hãy xem xét các quyền lưu trữ đám mây.
 - Triển khai quy trình tự động để xác minh tính hiệu quả của các cấu hình và cài đặt trong mọi môi trường.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Cross-Site Scripting (XSS)

- Các cuộc tấn công XSS khai thác các lỗ hổng trong các trang web được tạo động, cho phép những kẻ tấn công đưa tập lệnh độc hại phía máy khách vào các trang web được người dùng khác xem.
- Nó xảy ra khi dữ liệu đầu vào không hợp lệ được trong nội dung động được gửi đến trình duyệt web của người dùng để hiển thị.
- Những kẻ tấn công đưa JavaScript, VBScript, ActiveX, HTML hoặc Flash độc hại để thực thi trên hệ thống của nạn nhân bằng cách ẩn nó trong các yêu cầu hợp pháp.
- Lúc đó kẻ tấn công vượt qua cơ chế bảo mật phía máy khách và có được đặc quyền truy cập, sau đó đưa các tập lệnh độc hại vào các trang web cụ thể.
- Những đoạn mã độc hại này thậm chí có thể viết lại nội dung trang web HTML

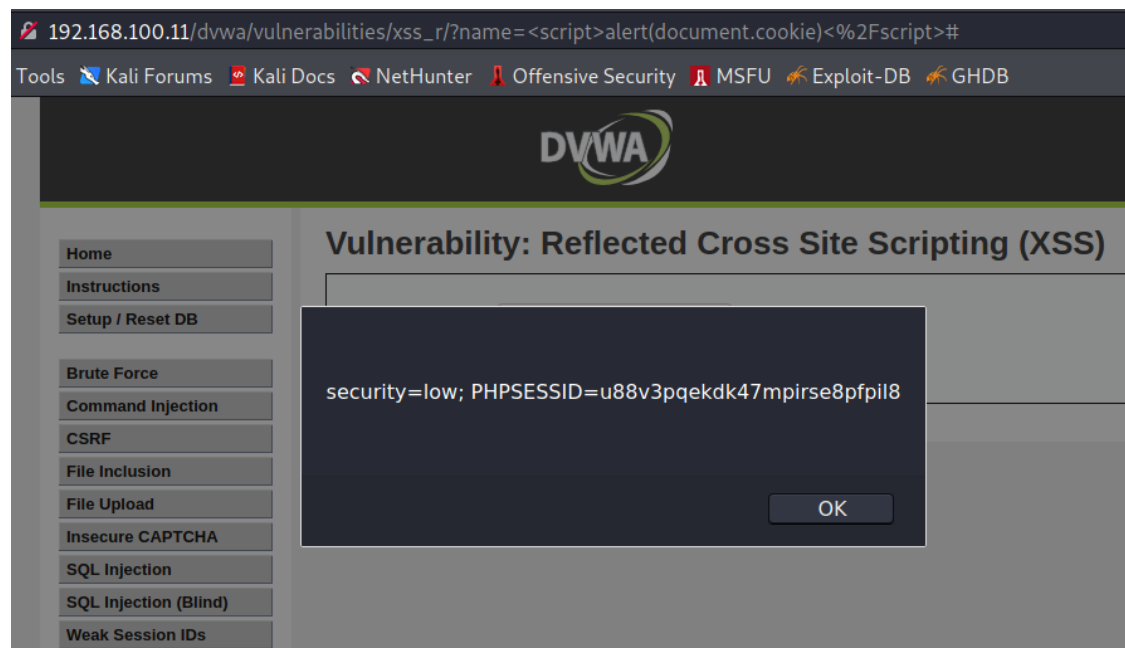


Các nguy cơ bảo mật ứng dụng web phổ biến

WWW.UIT.EDU.VN



- Cross-Site Scripting (XSS)





Các nguy cơ bảo mật ứng dụng web phổ biến



- Cross-Site Scripting (XSS)

- Chúng ta có thể sử dụng các phương thức sau đây để giảm thiểu các lỗi liên quan đến lỗ hổng này:
 - Sử dụng các framework có khả năng tự động loại bỏ XSS theo thiết kế, chẳng hạn như Ruby on Rails mới nhất, React JS. Tìm hiểu các hạn chế của từng giải pháp bảo vệ ứng dụng web khỏi tấn công XSS và xử lý thích hợp các trường hợp sử dụng không được đề cập.
 - Loại bỏ dữ liệu yêu cầu HTTP không đáng tin cậy dựa trên ngữ cảnh trong đầu ra HTML (nội dung, thuộc tính, JavaScript, CSS hoặc URL) sẽ giải quyết các lỗ hổng XSS.
 - Bộ Chính sách bảo mật nội dung (CSP) như một biện pháp kiểm soát giảm thiểu chuyên sâu về phòng thủ chống lại XSS. Sẽ có hiệu quả nếu không có lỗ hổng nào khác cho phép đặt mã độc hại qua tập tin cục bộ (ví dụ: ghi đè đường dẫn hoặc thư viện dễ bị tấn công từ các mạng phân phối nội dung được phép).



Các nguy cơ bảo mật ứng dụng web phổ biến



- Xử lý các đối tượng không an toàn
 - Xử lý các đối tượng không an toàn xảy ra khi một ứng dụng nhận và xử lý các đối tượng không an toàn.
 - Do quá trình xử lý không đúng cách này, mã độc hại được đưa vào sẽ không bị phát hiện và sẽ hiện diện trong quá trình thực thi cuối cùng. Nó có thể có tác động nghiêm trọng đến hệ thống, vì nó sẽ cho phép kẻ tấn công thực thi mã từ xa, nghe lén, giả mạo, tấn công leo thang quyền hạn.
 - Thực hiện kiểm tra tính toàn vẹn chẳng hạn như chữ ký điện tử trên bất kỳ đối tượng được xử lý để ngăn chặn việc tạo đối tượng độc hại hoặc giả mạo dữ liệu.
 - Thực thi các ràng buộc nghiêm ngặt cho các kiểu đối tượng trong quá trình xử lý.
 - Xử lý các đối tượng dùng chung trong quyền hạn thấp nhất có thể.
 - Ghi nhật ký quá trình xử lý các đối tượng, đặc biệt trong các trường hợp có lỗi bất thường diễn ra.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Sử dụng các thành phần chứa lỗ hổng đã được biết
 - Các thành phần như thư viện, frameworks, và các thành phần ứng dụng khác được khởi chạy với cùng quyền hạn với ứng dụng web chứa nó.
 - Nếu một thành phần có lỗ hổng và được khai thác kẻ tấn công có thể gây phương hại không những đến ứng dụng web này mà còn máy chủ web.
 - Những kẻ tấn công có thể xác định các thành phần yếu hoặc phụ thuộc bằng cách quét hoặc thực hiện phân tích thủ công.
 - Những kẻ tấn công tìm kiếm bất kỳ lỗ hổng nào trên các trang web khai thác như Cơ sở dữ liệu khai thác (<https://www.exploit-db.com>), v.v ...
 - Nếu một thành phần dễ bị tấn công được xác định, kẻ tấn công sẽ khai thác và thực hiện cuộc tấn công.
 - Việc này cho phép kẻ tấn công gây mất dữ liệu nghiêm trọng hoặc chiếm quyền kiểm soát các máy chủ



Các nguy cơ bảo mật ứng dụng web phổ biến



- Sử dụng các thành phần chứa lỗ hổng đã được biết
 - Các phương pháp nhằm loại bỏ lỗ hổng này bao gồm:
 - Loại bỏ các thành phần không sử dụng, các tính năng, thành phần, tệp và tài liệu không cần thiết.
 - Liên tục kiểm kê các phiên bản của cả thành phần phía máy khách và phía máy chủ (ví dụ: framework, thư viện) và các phụ thuộc của chúng bằng cách sử dụng các công cụ như DependencyCheck [39], reti.js [40], v.v.
 - Liên tục theo dõi các nguồn như CVE [41] và NVD [42] để tìm lỗ hổng trong các thành phần.
 - Sử dụng các công cụ phân tích thành phần phần mềm để tự động hóa quy trình. Đăng ký nhận thông báo qua email về các lỗ hổng bảo mật liên quan đến các thành phần bạn sử dụng.
 - Chỉ lấy các thành phần từ các nguồn chính thức qua các liên kết an toàn. Ưu tiên các gói đã ký để giảm nguy cơ bao gồm một thành phần độc hại đã được sửa đổi.
 - Giám sát các thư viện và thành phần không bị lỗi hoặc không tạo các bản vá bảo mật cho các phiên bản cũ hơn. Nếu không thể vá, hãy xem xét triển khai một bản vá ảo để theo dõi, phát hiện hoặc bảo vệ chống lại sự cố đã phát hiện.
 - Mọi tổ chức phải đảm bảo rằng có một kế hoạch liên tục để giám sát, phân loại và áp dụng các bản cập nhật hoặc thay đổi cấu hình trong suốt thời gian tồn tại của ứng dụng hoặc danh mục đầu tư



Các nguy cơ bảo mật ứng dụng web phổ biến



- Thiếu nhật ký và giám sát
 - Các ứng dụng web duy trì nhật ký để theo dõi hoạt động của ứng dụng web.
 - Ghi nhật ký và giám sát không đầy đủ đề cập đến tình huống phần mềm phát hiện không ghi lại sự kiện độc hại hoặc bỏ qua các chi tiết quan trọng về sự kiện này.
 - Những kẻ tấn công thường chen, xóa hoặc giả mạo nhật ký ứng dụng web để tham gia vào các hoạt động độc hại hoặc che giấu danh tính của họ.
 - Lỗi hỏng theo dõi và ghi nhật ký không đầy đủ làm cho việc phát hiện các sự kiện độc hại của kẻ tấn công trở nên khó khăn hơn và cho phép kẻ tấn công thực hiện các cuộc tấn công độc hại tương tự trong tương lai.
 - Do đó, chúng ta cần cấu hình các phương thức ghi nhật ký và giám sát phù hợp.



Các nguy cơ bảo mật ứng dụng web phổ biến



- Thiếu nhật ký và giám sát
 - Các phương pháp nhằm loại bỏ lỗ hổng này bao gồm:
 - Đảm bảo tất cả các lỗi đăng nhập, kiểm soát truy cập và lỗi xác thực đầu vào phía máy chủ có thể được ghi lại với ngữ cảnh người dùng đủ để xác định các tài khoản đáng ngờ hoặc độc hại và được lưu giữ đủ thời gian để cho phép phân tích pháp y bị trì hoãn.
 - Đảm bảo rằng nhật ký được tạo ở định dạng có thể dễ dàng sử dụng bằng giải pháp quản lý nhật ký tập trung.
 - Đảm bảo các giao dịch có giá trị cao có lộ trình kiểm tra với các biện pháp kiểm soát tính toàn vẹn để ngăn chặn việc giả mạo hoặc xóa, chẳng hạn như các bảng cơ sở dữ liệu chỉ thêm vào hoặc tương tự.
 - Thiết lập giám sát và cảnh báo hiệu quả để các hoạt động đáng ngờ được phát hiện và phản ứng kịp thời.
 - Thiết lập hoặc áp dụng kế hoạch phục hồi và ứng phó sự cố, chẳng hạn như NIST 800-61 phiên bản 2 trở lên [43].
 - Có các khung bảo vệ ứng dụng mã nguồn mở và thương mại như OWASP AppSensor [44], tường lửa ứng dụng web như ModSecurity với Bộ quy tắc cốt lõi OWASP ModSecurity [45] và phần mềm tương quan nhật ký với bảng điều khiển tùy chỉnh và cảnh báo.



Các nguy cơ bảo mật ứng dụng web phổ biến

WWW.UIT.EDU.VN



- Một số nguy cơ bảo mật ứng dụng web khác
 - Dò tìm thư mục (Directory Traversal):
 - Đây là loại tấn công cho phép kẻ tấn công truy cập vào các tập tin tại các thư mục bị giới hạn. Kẻ tấn công có thể thực thi các câu lệnh bên ngoài thư mục gốc của ứng dụng web.
 - Không kiểm soát việc điều hướng:
 - Kẻ tấn công lôi kéo người dùng thực hiện việc nhấp chuột vào các đường dẫn độc hại. Điều này có thể giúp kẻ tấn công cài mã độc hoặc đánh cắp thông tin này cảm.
 - Giả mạo thông tin Cookie:
 - Kẻ tấn công có thể thay đổi thông tin trong Cookie để vượt qua các hệ thống chứng thực.
 - Tấn công từ chối dịch vụ:
 - Kẻ tấn công có thể làm ảnh hưởng đến tính sẵn sàng của ứng dụng web. Họ có thể làm cho lưu lượng mạng tăng dẫn đến các yêu cầu từ khách hàng bị chậm. Thậm chí, họ có thể thực hiện tấn công từ chối dịch vụ mức ứng dụng.
 - Ví dụ, kẻ tấn công đăng ký hết tất cả các tài khoản có thể có, điều này làm cho người dùng không thể đăng ký tài khoản bình thường được



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Do thám thông tin dịch vụ web
 - Việc do thám cơ sở hạ tầng web cho phép kẻ tấn công thực hiện các tác vụ sau:
 - **Khám phá máy chủ:** Những kẻ tấn công có thể khám phá các máy chủ vật lý lưu trữ ứng dụng web, sử dụng các kỹ thuật như Whois Lookup, thăm vấn DNS (DNSstuff Toolbox) [46], Port Scanning,... Chúng ta có thể đọc nội dung chi tiết trong Chương 3.
 - **Khám phá dịch vụ:** Những kẻ tấn công có thể khám phá các dịch vụ đang chạy trên máy chủ web để xác định xem họ có thể sử dụng một số dịch vụ trong số chúng làm đường dẫn tấn công ứng dụng web hay không.
 - Quy trình này cũng cung cấp thông tin ứng dụng web như vị trí lưu trữ, thông tin về các máy chạy dịch vụ, sử dụng mạng và các giao thức liên quan. Những kẻ tấn công có thể sử dụng các công cụ như Nmap [31], NetScan Tools Pro [47] và các công cụ khác để tìm các dịch vụ chạy trên các cổng mở và khai thác chúng.
 - **Nhận dạng máy chủ:** Những kẻ tấn công sử dụng tính năng lấy thông tin máy chủ giúp xác định kiến trúc và phiên bản của phần mềm máy chủ web. Thông tin khác mà kỹ thuật này cung cấp bao gồm: vị trí máy chủ, địa chỉ cục bộ, tên máy chủ,...
 - **Khám phá nội dung ẩn:** Việc do thám cũng cho phép kẻ tấn công trích xuất nội dung và chức năng không được liên kết trực tiếp đến hoặc có thể truy cập được từ nội dung hiển thị chính.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công máy chủ web

- **Quét lỗ hổng** trên máy chủ web giúp kẻ tấn công khởi động các cuộc tấn công một cách dễ dàng bằng cách xác định các lỗ hổng có thể khai thác hiện trên máy chủ web.
 - Những kẻ tấn công sử dụng các công cụ như Metasploit [29], UrlScan (<https://urlscan.io/>), Nikto [48], v.v. để quét các lỗ hổng của máy chủ web.
- Để ngăn máy chủ web phục vụ người dùng hoặc máy khách hợp pháp, những kẻ tấn công **khởi chạy một cuộc tấn công DoS/DDoS** chống lại nó, sử dụng các công cụ như DoSHTTP [49] và Hping [5] để thực hiện một cuộc tấn công DoS.
 - Để thực hiện một cuộc tấn công DDoS, họ có thể sử dụng các công cụ như HOIC [50] và LOIC [50], hoặc SYN Flooding, Slowloris và DRDoS [50].
- Kẻ tấn công có thể dùng các **công cụ tấn công máy chủ web** như WebInspect [51].
 - Đây Là một công cụ kiểm tra thâm nhập và bảo mật ứng dụng web tự động và có thể định cấu hình, bắt chước các kỹ thuật tấn công và tấn công trong thế giới thực. Nó cho phép những kẻ tấn công phân tích các ứng dụng web và dịch vụ phức tạp để tìm các lỗ hổng bảo mật.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Phân tích ứng dụng web

- Kẻ tấn công cần phân tích các ứng dụng web mục tiêu để xác định các lỗ hổng của chúng.
- Điều này giúp họ tiết kiệm thời gian trong quá trình tấn công.
- Để phân tích ứng dụng web, những kẻ tấn công có được kiến thức cơ bản về ứng dụng web và sau đó phân tích chức năng và công nghệ của ứng dụng đang hoạt động để xác định bất kỳ lỗ hổng nào có thể bị khai thác.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Phân tích ứng dụng web

- Xác định khu vực cho phép nhận dữ liệu từ người dùng
- Xác định công nghệ được sử dụng phía máy chủ
- Xác định chức năng phía máy chủ
- Lập bản đồ khả năng tấn công



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Bỏ qua kiểm soát phía máy khách
 - Một ứng dụng web yêu cầu các kiểm soát phía máy khách để hạn chế đầu vào của người dùng trong việc truyền dữ liệu qua các thành phần máy khách và triển khai các biện pháp kiểm soát tương tác của người dùng.
 - Một nhà phát triển sử dụng các kỹ thuật như thẻ HTML ẩn, tiện ích mở rộng trình duyệt,... để cho phép truyền dữ liệu đến máy chủ thông qua máy khách.
 - Thông thường các nhà phát triển web nghĩ rằng dữ liệu được truyền từ máy khách đến máy chủ nằm trong tầm kiểm soát của người dùng và giả định này có thể khiến ứng dụng dễ bị tấn công bởi các cuộc tấn công khác nhau.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Bỏ qua kiểm soát phía máy khách
 - Tấn công các trường biểu mẫu ẩn:
 - Xác định các trường biểu mẫu ẩn trong trang web và thao tác với các thẻ và trường để khai thác trang web trước khi truyền dữ liệu đến máy chủ.
 - Tấn công các tiện ích mở rộng của trình duyệt:
 - Cố gắng chặn lưu lượng truy cập từ các tiện ích mở rộng của trình duyệt hoặc dịch ngược các tiện ích mở rộng của trình duyệt để thu thập dữ liệu người dùng.
 - Thực hiện rà soát mã nguồn:
 - Thực hiện rà soát mã nguồn để xác định các lỗ hổng trong mã mà các công cụ quét lỗ hổng truyền thống không thể xác định được.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công cơ chế chứng thực
 - Trong quá trình phân tích ứng dụng web, những kẻ tấn công cố gắng tìm ra các lỗ hổng chứng thực chẳng hạn như mật khẩu yếu (ví dụ: ngắn hoặc trống, các từ hoặc tên từ điển phổ biến, tên người dùng, mặc định).
 - Những kẻ tấn công khai thác các lỗ hổng này để giành quyền truy cập vào ứng dụng web bằng cách nghe trộm mạng, tấn công vét cạn, tấn công từ điển, tấn công phát lại cookie, đánh cắp thông tin xác thực, v.v.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công cơ chế xác thực
 - Ứng dụng web chứa cơ chế xác thực (ủy quyền) hạn chế quyền truy cập vào tài nguyên cụ thể hoặc chức năng (ví dụ: trang Quản trị) từ những người dùng đã chứng thực.
 - Ứng dụng web luôn thực hiện ủy quyền người dùng sau khi chứng thực.
 - Kẻ tấn công thực hiện cơ chế ủy quyền thiếu sót trong ứng dụng web và lợi dụng cơ chế đó để truy cập các trang bị hạn chế bằng cách nâng cao đặc quyền. Kẻ tấn công cố gắng truy cập thông tin mà không có thông tin xác thực thích hợp



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công cơ chế quản lý phiên
 - Quản lý phiên ứng dụng web liên quan đến việc trao đổi thông tin nhạy cảm giữa máy chủ và máy khách của nó ở bất kỳ nơi nào được yêu cầu.
 - Nếu việc quản lý phiên như vậy không an toàn, kẻ tấn công có thể lợi dụng việc quản lý phiên còn thiếu sót để tấn công ứng dụng web thông qua cơ chế quản lý phiên, đây là thành phần bảo mật quan trọng trong hầu hết các ứng dụng web.
 - Ngày nay, hầu hết những kẻ tấn công nhắm mục tiêu vào quản lý phiên ứng dụng để khởi động các cuộc tấn công độc hại chống lại các ứng dụng web, cho phép chúng dễ dàng vượt qua các kiểm soát xác thực và giả dạng như những người dùng khác mà không cần biết thông tin đăng nhập của họ (tên người dùng, mật khẩu).
 - Những kẻ tấn công thậm chí có thể chiếm quyền kiểm soát toàn bộ ứng dụng bằng cách xâm nhập tài khoản của quản trị viên hệ thống.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công Injection

- Các cuộc tấn công tiêm (Injection) rất phổ biến trong các ứng dụng web.
- Chúng khai thác cơ chế xác thực đầu vào dễ bị tổn thương do ứng dụng web thực hiện.
- Có nhiều loại tấn công tiêm nhiễm, chẳng hạn như đưa vào tập lệnh web, tiêm lệnh hệ điều hành, tiêm SMTP, tiêm LDAP và tiêm XPath.
- Một cuộc tấn công thường xuyên xảy ra khác là một cuộc tấn công SQL injection.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công Injection

- **Chèn mã web** (Web Scripts Injection):

- Nếu đầu vào của người dùng được sử dụng thành mã được thực thi động, hãy nhập đầu vào được tạo thủ công phá vỡ ngữ cảnh dữ liệu dự kiến và thực hiện các lệnh trên máy chủ.

- **Chèn lệnh hệ điều hành** (OS Commands Injection):

- Khai thác hệ điều hành bằng cách nhập mã độc hại vào các trường đầu vào nếu ứng dụng sử dụng đầu vào của người dùng trong lệnh cấp hệ thống.

- **SMTP Injection:**

- Đưa các lệnh SMTP tùy ý vào cuộc hội thoại của ứng dụng và máy chủ SMTP để tạo ra một lượng lớn email spam.

- **SQL Injection:**

- Nhập một loạt các truy vấn SQL độc hại vào các trường đầu vào để thao tác trực tiếp cơ sở dữ liệu.

- **LDAP Injection:**

- Tận dụng các lỗ hổng đầu vào của ứng dụng web chưa được xác thực để vượt qua các bộ lọc LDAP để có được quyền truy cập trực tiếp vào cơ sở dữ liệu.

- **XPath Injection:**

- Nhập các chuỗi độc hại vào các trường đầu vào để thao tác XPath truy vấn để nó can thiệp vào logic của ứng dụng.

- **Tràn bộ đệm:**

- Chèn một lượng lớn dữ liệu không có thật vượt quá khả năng của trường đầu vào.

- **Canonicalization:**

- Thao tác với các biến tham chiếu đến các tệp bằng “dấu chấm-chấm-gạch chéo (../)” để truy cập các thư mục bị hạn chế trong ứng dụng.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công lỗ hổng logic của ứng dụng web
 - Trong các ứng dụng web, vô số logic được áp dụng ở mọi cấp độ.
 - Việc triển khai một số logic có thể dễ bị tấn công bởi nhiều cuộc tấn công khác nhau và sẽ không đáng chú ý.
 - Hầu hết những kẻ tấn công chủ yếu tập trung vào các cuộc tấn công cấp cao như SQL Injection, XSS scripting,... vì chúng có các dấu hiệu dễ nhận biết.
 - Ngược lại, các lỗi logic ứng dụng không liên kết với bất kỳ dấu hiệu chung nào làm cho các lỗi logic ứng dụng khó xác định hơn.
 - Việc kiểm tra thủ công hoặc máy quét lỗ hổng không thể xác định loại lỗ hổng này và điều này dẫn dụ những kẻ tấn công khai thác các lỗ hổng logic của ứng dụng để gây ra thiệt hại nghiêm trọng cho các ứng dụng web.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công ứng dụng web phía máy khách

- **Cross-Site Scripting:**

- Kẻ tấn công bỏ qua cơ chế bảo mật của mã khách hàng và có được các đặc quyền truy cập, sau đó đưa các tập lệnh độc hại vào các trang của một trang web. Những đoạn mã độc hại này thậm chí có thể viết lại nội dung HTML của trang web.

- **Tấn công chuyển hướng:**

- Những kẻ tấn công phát triển mã và liên kết giống với một trang web hợp pháp mà người dùng muốn truy cập; tuy nhiên, khi làm như vậy, URL sẽ chuyển hướng người dùng đến một trang web độc hại mà trên đó những kẻ tấn công có thể lấy được thông tin đăng nhập và thông tin nhạy cảm khác của người dùng.

- **HTTP Header Injection:**

- Những kẻ tấn công chia một phản hồi HTTP thành nhiều phản hồi bằng cách đưa một phản hồi độc hại vào tiêu đề HTTP. Bằng cách đó, những kẻ tấn công có thể phá hoại trang web, làm nhiễu loạn bộ nhớ cache và kích hoạt tập lệnh lặp, lặp lại.

- **Frame Injection:**

- Khi các tập lệnh không xác thực đầu vào của chúng, những kẻ tấn công sẽ chèn mã qua các khung. Điều này ảnh hưởng đến tất cả các trình duyệt và tập lệnh, không xác thực đầu vào không đáng tin cậy. Các lỗ hổng này xảy ra trong các trang HTML có khung. Một lý do khác cho lỗ hổng này là trình duyệt web hỗ trợ chỉnh sửa khung.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công ứng dụng web phía máy khách

- **Yêu cầu tấn công giả mạo:**

- Trong một cuộc tấn công giả mạo yêu cầu, những kẻ tấn công khai thác sự tin cậy của một trang web hoặc ứng dụng web trên trình duyệt của người dùng. Cuộc tấn công hoạt động bằng cách bao gồm một liên kết trên một trang, đưa người dùng đến một trang web đã được xác thực.

- **Cố định phiên:**

- Cố định phiên giúp những kẻ tấn công chiếm đoạt các phiên người dùng hợp lệ. Họ tự xác thực bằng cách sử dụng mã phiên đã biết và sau đó sử dụng mã phiên đã biết để chiếm đoạt phiên do người dùng xác thực. Do đó, những kẻ tấn công lừa người dùng truy cập vào một máy chủ web chính hãng bằng cách sử dụng giá trị mã phiên hiện có.

- **Các cuộc tấn công về quyền riêng tư:**

- Một cuộc tấn công về quyền riêng tư đang theo dõi được thực hiện với sự trợ giúp của một trang web từ xa bằng cách sử dụng trạng thái trình duyệt liên tục bị rò rỉ.

- **Tấn công ActiveX:**

- Những kẻ tấn công dụ nạn nhân qua email hoặc thông qua một liên kết mà kẻ tấn công đã xây dựng theo cách có thể truy cập được các kẽ hở của mã thực thi từ xa, cho phép kẻ tấn công có được đặc quyền truy cập ngang bằng với người dùng được ủy quyền.



Vượt qua cơ chế đảm bảo an toàn thông tin bằng tấn công dịch vụ web

WWW.UIT.EDU.VN



- Tấn công dịch vụ web phía máy chủ
 - Các ứng dụng web sử dụng các dịch vụ web để triển khai các chức năng cụ thể.
 - Nếu các dịch vụ web này có lỗi hổng thì chúng có thể ảnh hưởng đến các ứng dụng web dùng nó.
 - Chính vì vậy, bất kỳ cuộc tấn công nào vào dịch vụ web sẽ ngay lập tức làm lộ ra các lỗ hổng kinh doanh và logic của ứng dụng web.
 - Những kẻ tấn công có thể nhắm mục tiêu các dịch vụ web bằng nhiều kỹ thuật khác nhau, vì các ứng dụng web cung cấp các dịch vụ này cho người dùng thông qua nhiều cơ chế khác nhau.
 - Do đó, khả năng xảy ra các lỗi hổng sẽ tăng lên.
 - Những kẻ tấn công khai thác các lỗ hổng này để xâm nhập các dịch vụ web. Do đó, chúng ta không những đảm bảo các ứng dụng web an toàn, mà còn đảm bảo dịch vụ web và các thành phần liên quan được an toàn



Kiểm thử an toàn ứng dụng web



- Bước 1: Xác định mục tiêu
- Bước 2: Thu thập thông tin
- Bước 3: Kiểm tra quản lý cấu hình
- Bước 4: Kiểm tra xác thực
- Bước 5: Kiểm tra quản lý phiên
- Bước 6: Kiểm tra từ chối dịch vụ
- Bước 7: Kiểm tra xác thực dữ liệu
- Bước 8: Kiểm tra logic nghiệp vụ
- Bước 9: Kiểm tra ủy quyền
- Bước 10: Kiểm tra dịch vụ web
- Bước 11: Ghi lại tất cả các phát hiện



Câu hỏi ôn tập



Câu hỏi ôn tập



- **Câu 1:** Trình bày lỗi SQL Injection, cho ví dụ minh họa.
- **Câu 2:** Trình bày lỗi xác thực, đề xuất các giải pháp để giảm thiểu rủi ro của lỗi xác thực.
- **Câu 3:** Trình bày lỗi XSS, đề xuất các giải pháp để giảm thiểu rủi ro của lỗi XSS.
- **Câu 4:** Trình bày lỗi thiếu nhật ký và giám sát, đề xuất giải pháp để giảm thiểu rủi ro của lỗi thiếu nhật ký và giám sát.
- **Câu 5:** Trình bày các bước chính trong việc phân tích ứng dụng web.
- **Câu 6:** Trình bày các tác vụ chính của quá trình do thám thông tin dịch vụ web.
- **Câu 7:** Trình bày quá trình tấn công cơ chế chứng thực.



Câu hỏi trắc nghiệm

- Câu 6.1:
- Phát biểu nào sau đây đúng:
- Phát biểu A: SQL Injection là lỗi của ứng dụng Web.
- Phát biểu B: SQL Injection là lỗi của hệ quản trị cơ sở dữ liệu.
 - A. Phát biểu A đúng, Phát biểu B sai
 - B. Phát biểu A sai, Phát biểu B đúng
 - C. Phát biểu A và B đúng
 - D. Phát biểu A và B sai



Câu hỏi trắc nghiệm



- Câu 6.2:
- Loại tấn công nào khai thác các lỗ hổng trong các trang web được tạo động, cho phép những kẻ tấn công đưa tập lệnh độc hại phía máy khách vào các trang web được người dùng khác xem.
 - A. Lỗi kiểm soát truy cập
 - B. LDAP Injection
 - C. Cross-Site Scripting
 - D. SQL Injection



Câu hỏi trắc nghiệm

- Câu 6.3:
- Công cụ nào sau đây được dùng để xác định công nghệ được sử dụng phía máy chủ.
 - A. httpprint (<http://www.net-square.com>)
 - B. Burp Suite (<https://portswigger.net>)
 - C. WebScarab (<https://www.owasp.org>)
 - D. Teleport Pro (<http://www.tenmax.com>)



Câu hỏi trắc nghiệm

- Câu 6.4:
- Phát biểu nào sau đây đúng:
- Phát biểu A: Đánh cắp phiên là cách những kẻ tấn công đánh cắp mã phiên của người dùng từ một trang web đáng tin cậy để thực hiện các hoạt động độc hại.
- Phát biểu B: Phát lại phiên là cách những kẻ tấn công có được mã phiên của người dùng và sau đó sử dụng lại nó để có quyền truy cập vào tài khoản người dùng.
 - A. Phát biểu A đúng, Phát biểu B sai
 - B. Phát biểu A sai, Phát biểu B đúng
 - C. Phát biểu A và B đúng
 - D. Phát biểu A và B sai



Câu hỏi trắc nghiệm



- Câu 6.5:
- Bước đầu tiên của kiểm tra thâm nhập ứng dụng web là gì:
 - A. Xác định mục tiêu
 - B. Thu thập thông tin
 - C. Kiểm tra xác thực
 - D. Kiểm tra ủy quyền



Cảm ơn!