Các tấn công vào cơ sở dữ liệu (Database Attacks)

Giảng viên: Trần Thị Lượng

- Thực tế cho thấy, sự cố về an ninh xảy ra với CSDL có thể ảnh hưởng nghiêm trọng đến danh tiếng của công ty và quan hệ với khách hàng.

Hãng bảo mật SecureWorks cho biết đã phát hiện tới 8.000 vụ tấn công lên các cơ sở dữ liệu mỗi ngày

Tổn thất tài chính rất lớn

Một trong những vụ tấn công nổi tiếng nhất chính là vụ tấn công vào CardSystems Solutions - một hãng chuyên lưu trữ có sở dữ liệu thanh toán thẻ tín dụng.
Tin tặc đã sử dụng giải pháp tấn công SQL Injection để chiếm quyền điều khiển hệ thống cơ sở dữ liệu của CardSystems và chuyển toàn bộ cơ sở dữ liệu ra ngoài. Đã có khoảng 40 triệu thẻ tín dụng của khách hàng (bao gồm Master Card và Visa Card) rơi vào tay chúng gây ra thiệt hại hàng triệu USD

Theo SecureWorks 7/2007

Hacker tấn công vào website Microsoft-UK

Làm mất thể diện và danh tiếng

6 – 8/2005

Hacker tấn công cơ sở dữ liệu không quân Mỹ

đánh cắp thông tin cá nhân của gần 33.000 quân nhân đang phục vụ cho không quân Mỹ. Số liệu bị đánh cắp bao gồm cả ngày tháng năm sinh và số thẻ an ninh (Social Security).

Làm lộ thông tin bí mật quốc gia và giảm thế mạnh quân sự

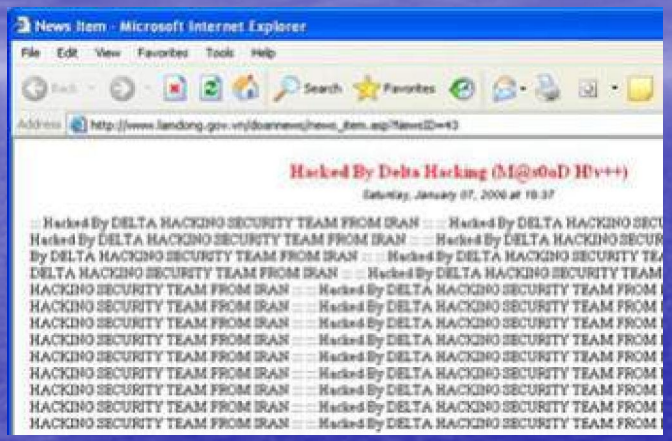
12/2007

Hacker TQ tấn công phòng thí nghiệm hạt nhân Oak Ridge của Mỹ

nhằm đánh cắp dữ liệu từ dự án tuyệt mật của phòng thí nghiệm.

Theo Quantrimang.com

6/2/2006
Website của tỉnh Lâm Đồng (lamdong.gov.vn) bị hacker nước ngoài tấn công, và thay đổi hoàn toàn nội dung một trang tin tức.



10/5/2005
60% website .gov.vn đã bị tấn công và nắm quyền kiểm soát

- Các website vẫn hoạt động như bình thường, và không hề hay biết mọi cơ sở dữ liệu quan trọng, thậm chí ở cấp quốc gia, đều đã bị sao chép, ăn cắp.
- Các đầu mối thông tin chính trên các website đã bị kiểm soát có thể được sửa đổi với mục đích xấu, khiến người truy cập web hiểu sai thông tin, dẫn tới nhiều hậu quả nguy hiểm.

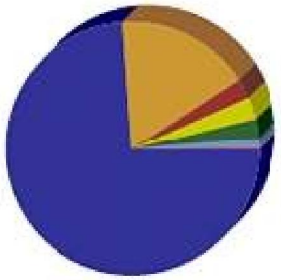
Theo Vietnamnet.vn

APPLICATION SECURITY, INC.

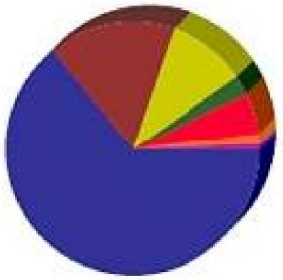
Username: audit1 [Logout] (Admin User)

Home | Alerts | Dashboard | Reports | Policies | Filters | Sensors | System Settings | Help

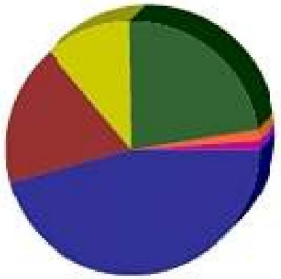
Vulnerability Assessment



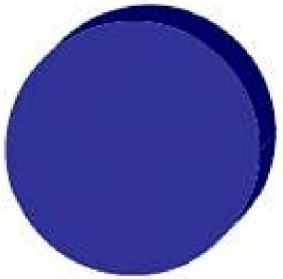
High



Low



Medium



Informational

Check Category Description

- Access Control
- User-Defined
- Application Integrity
- Vulnerabilities
- Icentification/Password Control
- Password Attacks
- Denial of Services
- OS Integrity
- Misconfigurations

APPLICATION SECURITY, INC.

Top 10 database attacks

- 1. Excessive privileges
- 2. Privilege abuse
- 3. Unauthorized privilege elevation
- 4. Platform vulnerabilities
- 5. SQL injection
- 6. Weak audit
- 7. Denial of service
- 8. Database protocol vulnerabilities
- 9. Weak authentication
- 10. Exposure of backup data

Lỗ hổng hệ quản trị CSDL

- Ngày 22/12/2008, Microsoft đã cảnh báo một lỗ hổng trong hệ quản trị Cơ sở dữ liệu (CSDL) Microsoft SQL Server. Đây là lỗ hổng tràn bộ đệm cho phép Hacker tấn công và chiếm quyền kiểm soát máy tính từ xa. Lỗ hổng này do hãng an ninh SEC Consult công bố cùng với mã khai thác.
  sp_replwritetovarbin

(Theo Trung tâm an ninh mạng Bkis)

Ngày công bố	Phần mềm có lỗi	Mức độ nguy hiểm
22-12-2008	Microsoft SQL 2000 Microsoft SQL 2005 Windows Internal Database	Cao

Microsoft tiếp tục vá 4 lỗ hổng bảo mật

- Ngày 5.2, Microsoft thông báo sẽ phát hành các bản vá lỗi để bịt kín lỗ hổng bảo mật, trong đó có 2 lỗ hổng được xếp vào mức độ nghiêm trọng.
- 4 lỗ hổng này đều cho phép hacker thực thi các đoạn mã độc từ xa, tồn tại trong 4 ứng dụng phổ biến là Internet Explorer, SQL Server, Exchange Server và Visio. Trong số này, lỗ hổng của IE và Exchange được Microsoft xếp vào mức độ “nghiêm trọng” (critical),2 lỗ hổng còn lại được xếp vào mức "quan trọng” (important).

SQL Injection vẫn là món khoái khẩu của tin tặc

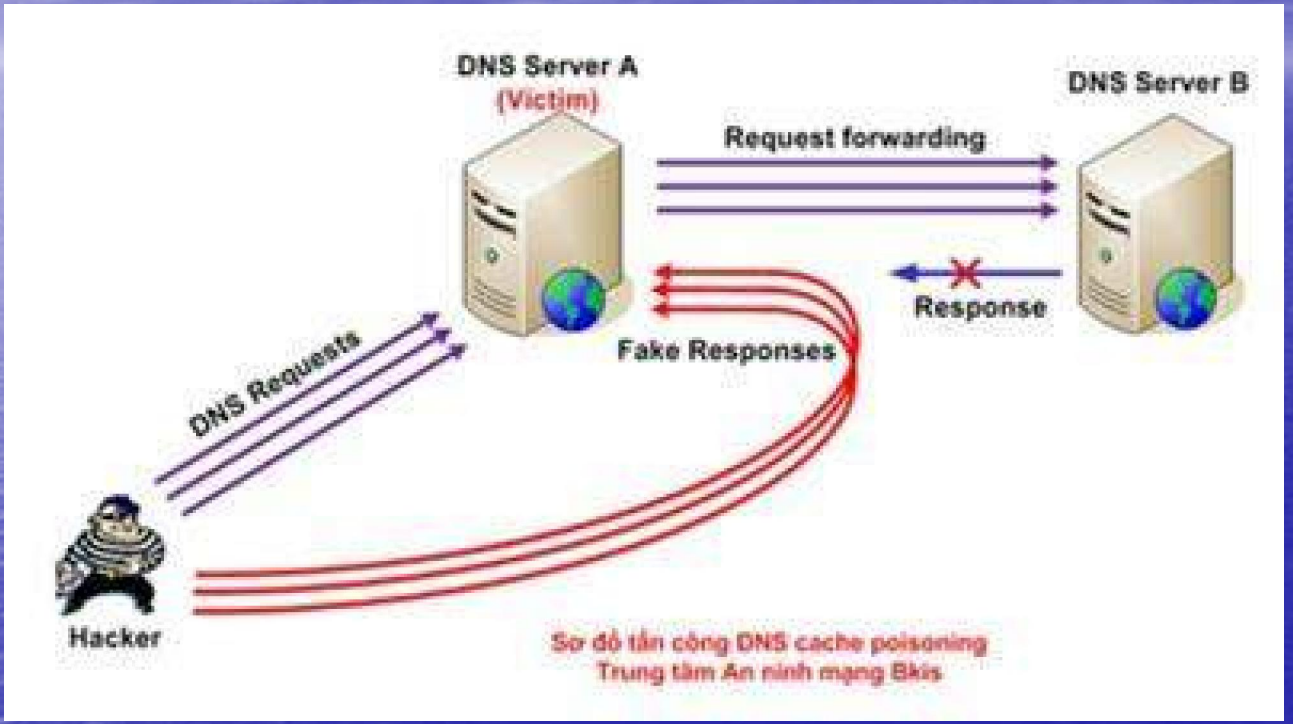
- SQL Injection là một cách thức tấn công khai tác lỗi trong việc kiểm tra dữ liệu đầu vào của các ứng dụng, để từ đó chạy các câu lệnh truy vấn (*query*) dữ liệu SQL có lợi cho kẻ tấn công. SQL Injection xảy ra ở tất cả các phần mềm có sử dụng ngôn ngữ truy vấn dữ liệu SQL, và thường gặp nhất là ở các web-application.
- Cho đến nay, SQL Injection vẫn là phương thức thông dụng nhất của tin tặc khi tấn công một website vì cơ sở dữ liệu được xem là trái tim của website. Số lượng website bị tin tặc "nắm giữ" lên đến vài trăm ngàn và thường được dùng để phát tán mã độc, malware hay lừa đảo trực tuyến (*phishing*) khi khách truy cập truy xuất vào website.
- Những vụ "SQL Injection" đình đám trong năm 2008 phải kể đến như việc mất 10.597 sổ an sinh xã hội và hồ sơ pháp lý của các công dân thuộc Oklahoma khi website này bị tin tặc tấn công qua phương thức SQL Injection hoặc đợt tấn công trên quy mô lớn đã gây tổn thất cho hơn nửa triệu website...
- Việc chống trả từ những webmaster xem ra còn khá yếu ớt vì đại đa số vẫn sử dụng những hệ thống máy chủ cơ sở dữ liệu dùng chung hoặc không được bảo vệ kỹ, cách thức lập trình website còn sơ hở. Cả Microsoft và HP cùng tham gia hỗ trợ cho khách hàng của mình qua các công cụ miễn phí nhằm kiểm tra mức độ ngăn chặn các đợt tấn công SQL Injection.

(Theo Tuoi tre online)

Yếu điểm trong hệ thống DNS

- Tháng 7-2008, chuyên gia nghiên cứu bảo mật Dan Kaminsky đã làm chấn động làng CNTT qua phát hiện về yếu điểm trong hệ thống DNS (*Domain Name System*) toàn cầu. Yếu điểm này cho phép tin tặc dễ dàng tấn công vào các DNS server có chức năng hỏi hộ (*recursive*) và lưu giữ kết quả (*caching*) có điểm yếu: chấp nhận xử lý đồng thời nhiều yêu cầu truy vấn... với mục đích làm thay đổi ánh xạ tên miền và hướng người dùng đến một địa chỉ IP bất hợp lệ tùy ý.
- Đây là lỗi nghiêm trọng có thể giúp hacker lợi dụng tấn công các hệ thống DNS, chuyển những tên miền mà người truy cập muốn vào đến những website độc hại.

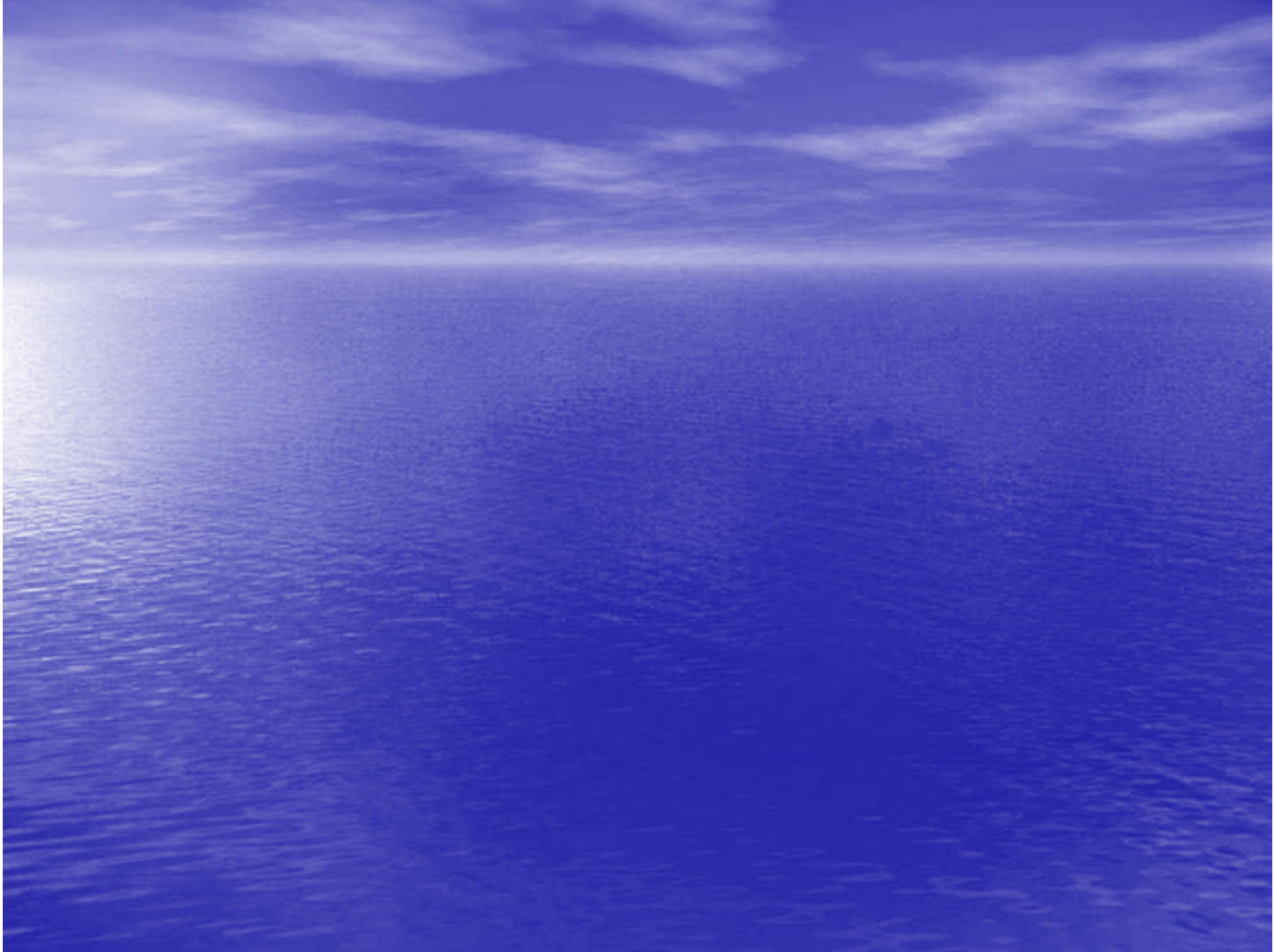
Sơ đồ tấn công DNS

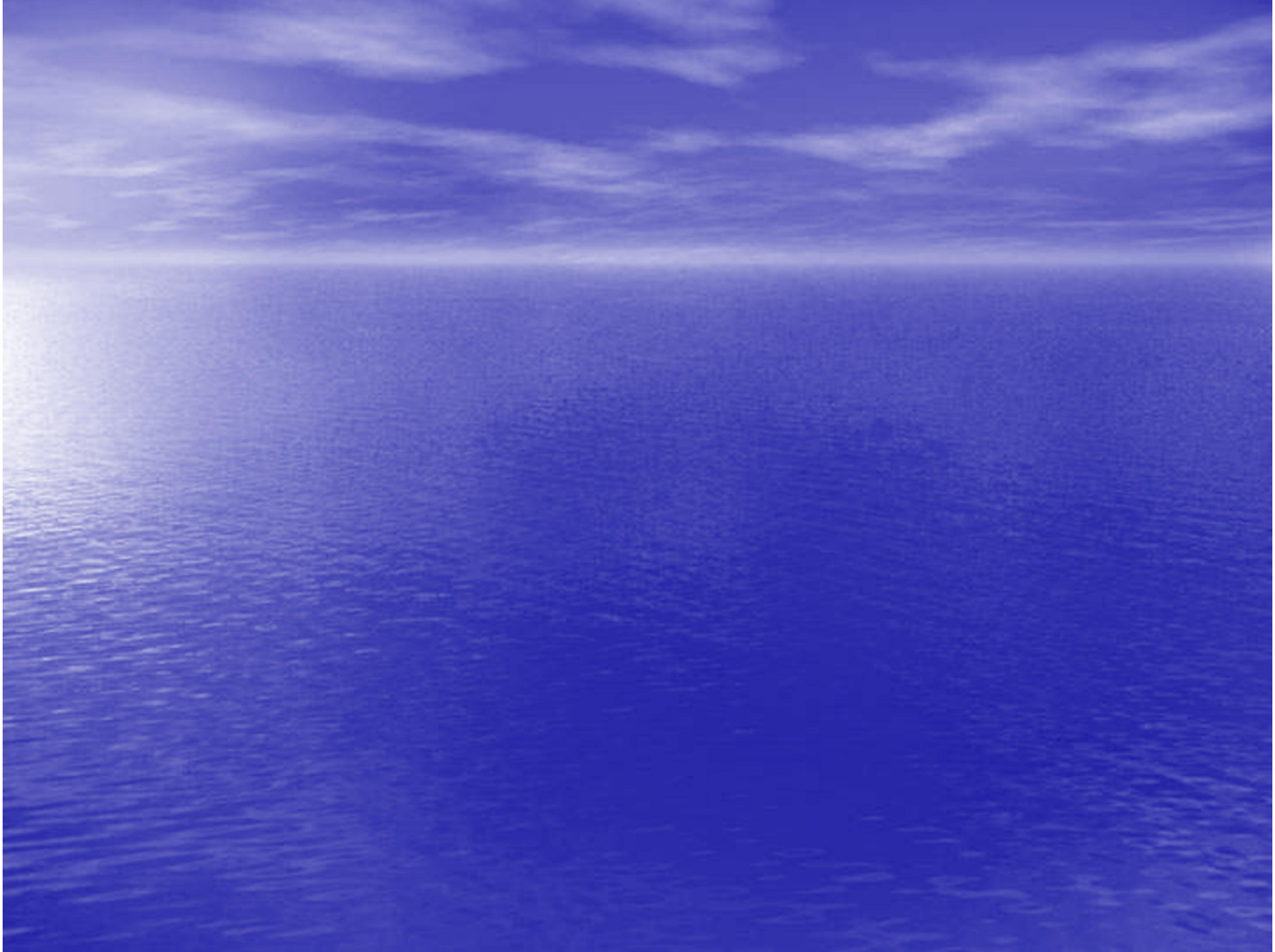


- Điều kiện thuận lợi cho tin tặc phát động những cuộc tấn công ồ ạt vào các hệ thống DNS trên thế giới, chuyển hướng người dùng đến những website giả mạo nhằm lừa họ cung cấp thông tin cá nhân, tài khoản ngân hàng trực tuyến, số thẻ tín dụng...

- Người làm tốt công tác bảo mật bao giờ cũng là người tuân thủ theo luật KISS!

  KISS = Keep It Simple, Stupid!





Những lỗ hổng trong website doanh nghiệp

- **Dữ liệu đầu vào không được kiểm tra tính hợp lệ**
  Trước tiên, hacker sẽ thiết lập một proxy đứng giữa trình duyệt và máy chủ ứng dụng web. Proxy này có khả năng chặn các gói dữ liệu trước khi chuyển đến máy chủ, do đó cho phép hacker sửa đổi dữ liệu truy cập và chèn các mã tấn công trước khi gửi đến ứng dụng web. Những cuộc tấn công dạng này đang có xu hướng ngày càng phổ biến hơn do số lượng các công cụ hỗ trợ các chức năng tạo tham số bất kỳ, tạo mã tấn công, tấn công lập trình máy (brute force) đang ngày càng tăng. Hậu quả của việc sử dụng các tham số không được kiểm tra sẽ gây khó khăn cho nhà lập trình web nếu họ không có một hệ thống tập trung kiểm tra tính hợp lệ của tất cả các truy xuất HTTP.
- **Lỗi kiểm soát truy cập nguồn tài nguyên**
  Những lập trình viên thường không đánh giá được mức độ khó khăn trong việc xây dựng một cơ chế quản lý kiểm soát truy cập dữ liệu. Đa số những chức năng này không được thiết kế từ lúc đầu mà được xây dựng kèm theo tùy tính năng của ứng dụng. Vì vậy, các chức năng kiểm soát được xây dựng ở khắp các module khác nhau trong mã nguồn. Khi ứng dụng được phát triển xong và đưa vào triển khai, các mã kiểm soát này trở nên không thống nhất và gây ra nhiều lỗ hổng nghiêm trọng khó phát hiện được.
- **Lỗi liên quan đến quá trình quản lý xác thực và phiên truy cập**

- Một số lượng lớn lỗi ứng dụng trong các hàm quản lý tài khoản và phiên truy cập có thể dẫn đến mối nguy cơ lộ tài khoản người sử dụng và thậm chí tài khoản của người quản trị. Ứng dụng web thường phải theo dõi và duy trì phiên truy cập của người dùng nhằm phân biệt các truy cập từ người dùng khác nhau. Giao thức HTTP không cung cấp khả năng trên do đó ứng dụng web phải tự tạo cơ chế này. Thông thường, môi trường phát triển ứng dụng cung cấp cơ chế quản lý phiên truy cập (thường là dưới hình thức mã hóa bằng những đoạn video hấp dẫn). Tuy nhiên, đa số các nhà lập trình nghiêng về phát triển cơ chế riêng của họ. Trong cả hai trường hợp, nếu token quản lý phiên truy cập không được bảo vệ, tin tặc có thể ăn cắp token truy cập tài khoản của người khác.
- **Lỗi tràn bộ đệm**
  Tin tặc sử dụng lỗi tràn bộ đệm nhằm ảnh hưởng đến dòng lệnh thực thi của ứng dụng web. Bằng cách gửi một đoạn mã được thiết kế đặc biệt đến ứng dụng, tin tặc có thể làm cho ứng dụng web thi hành bất kỳ đoạn mã nào, điều này tương đương với việc chiếm quyền làm chủ máy server. Mặc dù là một lỗi phổ biến, lỗi tràn bộ đệm là loại lỗi rất khó phát hiện và ngay cả khi đã được phát hiện, lỗi này rất khó bị lợi dụng do tin tặc cần một trình độ rất cao để có thể viết đoạn mã khai thác.
- **Lưu trữ thiếu an toàn**
  Đa số các ứng dụng web cần lưu trữ dữ liệu nhạy cảm, trong cơ sở dữ liệu hoặc trong một tập tin nào đó trong hệ thống. Thông tin nhạy cảm bao gồm: mật khẩu, số thẻ tín dụng, thông tin tài khoản, hoặc các thông tin cần bảo vệ khác. Các cơ chế mã hóa thường được sử dụng để bảo vệ những thông tin này. Mặc dù, sử dụng các hàm mã hóa không khó cho các lập trình viên. Tuy nhiên, lập trình viên vẫn thường mắc những lỗi cơ bản khi áp dụng vào ứng dụng web do không hiểu rõ hết các đặc điểm mã hóa. Những lỗi thông thường bao gồm: không mã hóa dữ liệu quan trọng như khóa, certificates và mật khẩu, lưu trữ các khóa bảo mật trong bộ nhớ bằng các cơ chế không an toàn, cơ chế tạo số ngẫu nhiên không đảm bảo, sử dụng sai thuật toán...

- **Từ chối dịch vụ**
  Một dạng tấn công DoS đó là, ứng dụng web dựa trên các lỗi trong chức năng của ứng dụng. Ví dụ một ứng dụng sử dụng cơ chế khóa tài khoản trong một tiếng hoặc hơn nếu nhận được quá 3 lần mật khẩu sai. Hacker có thể lợi dụng điểm yếu này, gửi đến quá 3 lần sai mật khẩu của một tài khoản hợp lệ, hậu quả là người dùng của tài khoản này không thể truy cập được trong một tiếng hoặc hơn. Trong một cuộc tấn công từ chối dịch vụ điển hình vào ứng dụng web, hackers sẽ tìm cách chiếm gần hết nguồn tài nguyên hệ thống trên máy chủ hoặc ứng dụng khiến người sử dụng hợp lệ không thể truy cập vào ứng dụng.
- **Quản lý cấu hình thiếu an toàn**
  Theo các thống kê hiện nay, thông thường các phần mềm và hệ điều hành trên máy chủ không được cập nhật kịp thời với bản vá lỗi bảo mật mới nhất. Lỗi trên phần mềm web hosting máy chủ cho phép liệt kê bất kỳ thư mục (hoặc tập tin) nào trong hệ thống như những tập tin mặc định, tập tin tạo ra để test như script, tập tin cấu hình không được xóa đi trong thư mục của trang web... Những tập tin này, thường có độ bảo mật yếu và có thể chứa những thông tin quan trọng.

Quy trình xử lý báo lỗi
Quy trình xử lý báo lỗi có thể gây ra nhiều vấn đề bảo mật cho một trang web. Vấn đề thông thường nhất là khi các thông báo lỗi có chứa các thông tin nhạy cảm như stack traces, thông tin cơ sở dữ liệu và các mã lỗi được thông báo cho người dùng. Những lỗi này cung cấp các thông tin về hệ thống, ứng dụng ở mức độ thấp và thông tin này phải được bảo mật. Sử dụng những thông tin này, hacker có thể dò tìm ra những lỗi khác của ứng dụng.

- *Với việc tìm ra hàng chục lỗi bảo mật trên các website DN, dự án bảo mật ứng dụng web đưa ra giải pháp nào để phòng chống, thưa ông ?*

-
- Vấn đề bảo mật ứng dụng web không phải là câu chuyện mới. Thực tế là phần lớn các vấn đề trên đã được hiểu rõ trong nhiều thập kỷ qua. Tuy nhiên, đến nay vẫn có khá nhiều dự án phát triển phần mềm còn mắc phải những lỗ hổng này và đe dọa không chỉ đến an toàn cho hệ thống của khách hàng mà còn ảnh hưởng chung đến an toàn của hệ thống Internet. Do tính chất phức tạp của ứng dụng, hiện nay chưa có một giải pháp tuyệt đối cho vấn đề này. Tuy nhiên các giải pháp sau được đề nghị để giảm thiểu các rủi ro liên quan đến bảo mật của ứng dụng web: Các tiêu chí về bảo mật phải được đặt ra ngay từ lúc thiết kế ứng dụng nhằm phát triển các module bảo vệ ngay từ giai đoạn đầu, ban hành một chuẩn tối thiểu về bảo mật cho toàn ứng dụng; thường xuyên cập nhật kiến thức bảo mật cho lập trình viên; sử dụng dịch vụ đánh giá bảo mật của một công ty ngoài để kiểm tra tính bảo mật của ứng dụng; sử dụng các công cụ dò và phát hiện lỗi của ứng dụng; cập nhật các phần mềm máy chủ web với các phiên bản vá lỗi bảo mật mới nhất; sử dụng các thiết bị tường lửa ứng dụng web để bảo vệ ứng dụng ở mức ngoại vi...