

20215118

phuc.dth215118@sis.hust.edu.vn

1	2	3	4	5
6	7	8	9	10
11	12	13	14	

### Câu hỏi


Câu hỏi #84e0dc

1 điểm (không tích lũy, không hiển thị kết quả)

Origin có thể đóng vai trò gì trong việc quyết định chia sẻ tài nguyên giữa các trang web?

- ☐ Nó không ảnh hưởng đến việc chia sẻ tài nguyên.
- ☒ Nó có thể đảm bảo rằng tài nguyên chỉ được chia sẻ giữa các trang web cùng một Origin.
- ☐ Nó xác định số lượng tài nguyên trang web có thể chia sẻ.
- ☐ Nó có thể quyết định cho phép chia sẻ tài nguyên khi trang web yêu cầu.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #b01859

1 điểm (không tích lũy, không hiển thị kết quả)

SQL injection có thể xảy ra trong phạm vi của ứng dụng nào?

- ☐ Chỉ trong ứng dụng web
- ☐ Chỉ trong ứng dụng di động
- ☒ Có thể xảy ra trong cả ứng dụng web, di động, desktop
- ☐ Chỉ trong ứng dụng desktop

Gửi

 Câu trả lời đã được gửi.

Câu hỏi #10e059

1 điểm (không tích lũy, không hiển thị kết quả)

Trong HTTPS, "SSL/TLS Certificates" được phát hành bởi ai và có thể chứa thông tin gì?

- ☐ Phát hành bởi người quản trị hệ thống, chứa thông tin về địa chỉ IP.
- ☒ Phát hành bởi tổ chức chứng nhận (CA), chứa thông tin về danh tính của chủ sở hữu và khóa công khai của họ.
- ☐ Phát hành bởi máy chủ web, chứa mã nguồn của trang web.
- ☐ Phát hành bởi trình duyệt web, chứa tên người sử dụng và mật khẩu.

Gửi

 Câu trả lời đã được gửi.

Câu hỏi #2d5b9f

1 điểm (không tích lũy, không hiển thị kết quả)

Tại sao việc xác định Origin quan trọng trong bảo mật?

- ☐ Để kiểm soát việc tải trang web.
- ☒ Để ngăn chặn các tấn công chéo trang web (Cross-Site) và đảm bảo rằng dữ liệu chỉ được chia sẻ giữa các trang web cùng một Origin.
- ☐ Để xác định loại nội dung trên trang web.
- ☐ Chỉ để quản lý cấp độ quyền truy cập của người dùng.

Gửi

 Câu trả lời đã được gửi.

Câu hỏi #bff277

1 điểm (không tích lũy, không hiển thị kết quả)

Content-Security-Policy (CSP) cung cấp giải pháp bảo mật như thế nào?

- ☐ Content-Security-Policy (CSP) là một trường (field) trong header của HTTP. CSP không liên quan đến bảo mật và chỉ đơn giản là một tiêu chuẩn định dạng dữ liệu.
- ☒ CSP cung cấp khả năng cho phép thực thi script theo Origin hoặc một domain, do vậy có thể giảm thiểu hoặc ngăn chặn tấn công Cross-Site Scripting (XSS).
- ☒ CSP cung cấp thiết lập frame-ancestors, kiểm soát nguồn nào được phép nhúng với iframe, vì vậy có thể ngăn chặn cuộc tấn công Clickjacking.
- ☐ CSP áp dụng cho việc tải API và không ảnh hưởng đáng kể đối với việc ngăn chặn Clickjacking

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #5576de

1 điểm (không tích lũy, không hiển thị kết quả)

Đâu là các thành phần chính của giao thức HTTPS?

- ☒ SSL/TLS để mã hóa dữ liệu.
- ☒ Chứng chỉ SSL/TLS để xác thực máy chủ.
- ☐ Cookie với trường `Secure` để mã hóa
- ☐ Chứng chỉ DNSSEC để xác thực DNS.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #42d58d

1 điểm (không tích lũy, không hiển thị kết quả)

Tại sao việc triển khai giao thức HTTPS là quan trọng trong môi trường truyền thông trực tuyến?

- ☐ Để tối ưu hóa hiệu suất trang web.
- ☒ Để bảo vệ dữ liệu truyền tải giữa máy khách và máy chủ khỏi tấn công và nguy cơ đánh cắp thông tin.
- ☐ Để kiểm soát quyền truy cập vào nội dung trang web
- ☐ Để xác minh danh tính của người truy cập trang web.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #3cd6d7

1 điểm (không tích lũy, không hiển thị kết quả)

Clickjacking là gì và làm thế nào nó thực hiện một cuộc tấn công trong môi trường web?

- ☐ Clickjacking là một kỹ thuật tấn công vào cơ sở dữ liệu
- ☒ Clickjacking tạo ra khả năng khiến người dùng nhấp chuột vào nút hoặc liên kết mà họ không biết.
- ☒ Clickjacking là một cuộc tấn công thực hiện bằng cách ẩn các phần tử trang web dưới các phần tử khác.
- ☐ Clickjacking liên quan đến việc dấu các phần tử ẩn của trang web bằng cookie.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #d359e5

1 điểm (không tích lũy, không hiển thị kết quả)

Cuộc tấn công Man-in-the-Middle (MitM) có tính chất nào?

- ☐ Social Engineering Attack.
- ☒ Cả hai Active và Passive Attack.
- ☐ Active Attack.
- ☐ Passive Attack.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #bf3e10

1 điểm (không tích lũy, không hiển thị kết quả)

Trong HTTPS, tại sao chúng ta cần sử dụng chứng chỉ SSL/TLS (SSL/TLS certificates)?

- ☒ Để máy khách có thể xác minh danh tính của máy chủ.
- ☐ Để kiểm tra tính toàn vẹn của dữ liệu.
- ☐ Để mã hóa mật khẩu truyền trên mạng.
- ☐ Để tạo chữ ký số cho dữ liệu truyền.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #801898

1 điểm (không tích lũy, không hiển thị kết quả)

Đâu là lợi ích của việc sử dụng HTTPS?

- ☒ Ngăn chặn tấn công Man-in-the-Middle (MITM).
- ☒ Đảm bảo tính toàn vẹn của dữ liệu.
- ☐ Ngăn chặn tất cả các tấn công XSS
- ☐ Giảm độ trễ và tăng tốc độ tải trang.

Gửi

 Câu trả lời đã được gửi.


Câu hỏi #7f86e6

1 điểm (không tích lũy, không hiển thị kết quả)

Trong SSL Handshake, loại khóa bảo mật nào được sử dụng để thực hiện quá trình thỏa thuận thông số bảo mật giữa máy khách và máy chủ?

- ☐ Khóa mã PIN.
- ☒ Khóa công khai và khóa bí mật.
- ☐ Khóa đối xứng.
- ☐ Khóa cảm biến vân tay.

Gửi

 Câu trả lời đã được gửi.

Câu hỏi #708c41

1 điểm (không tích lũy, không hiển thị kết quả)

Chọn các phát biểu đúng về DOM-based XSS Attacks

- ☐ DOM-based XSS Attacks không phải là một loại tấn công XSS và chỉ là một thuật ngữ không liên quan.
- ☐ DOM-based XSS Attacks chỉ áp dụng cho các ứng dụng di động và không ảnh hưởng đến trình duyệt trên máy tính.
- ☒ DOM-based XSS Attacks không làm thay đổi bản thân trang web gốc

- ☒ DOM-based XSS Attacks làm sửa đổi môi trường DOM của nạn nhân
- ☐ DOM-based XSS Attacks chỉ xảy ra khi người dùng chia sẻ cookie với trang web khác Origin và không ảnh hưởng đến trang web người dùng.

Gửi

 Câu trả lời đã được gửi.

Câu hỏi #ae51b1

1 điểm (không tích lũy, không hiển thị kết quả)

Cookie được tạo ra (tại server) và lưu trữ (tại browser) bằng kiểu dữ liệu clear-text. Vậy nó có thể được đảm bảo an toàn, chống bị đánh cắp hay nghe trộm hay không?

- ☒ Cookie là clear-text, bản thân không có cơ chế mã hóa chống nghe trộm.
- ☒ Sử dụng cookie với HTTP có thể dẫn đến các tấn công man-in-the-middle.
- ☐ Thuộc tính `Secure` có thể được thiết lập cho cookie để mã hóa cookie, chống nghe trộm
- ☐ Browser và Server có thể thiết lập cơ chế mã hóa cookie với hệ thống khóa công khai. Khi đó cookie được lưu trữ (ở browser) và tạo ra (ở server) đều được mã hóa.

Gửi