OWASP®

OWASP Phoenix Chapter - May 2024 Meetup

https://www.meetup.com/owasp-phoenix-chapter

https://owasp.org/www-chapter-phoenix

Thank You!

HeatSync Labs

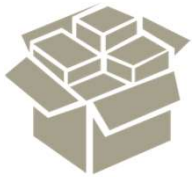
https://www.heatsynclabs.org

- A hackerspace where you can make things.
- A grassroots co-op of volunteers— No staff.
- Open for everyone during public hours and events.

- ✓ Please be courteous of project work.
- ✓ Bathrooms are in back.
- ✓ Snacks and drinks available along East wall. Donation requested (box on fridge).

Agenda

GitHub Supply Chain Attack

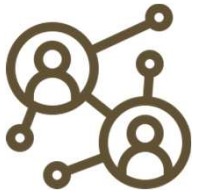


5 Minutes

OWASP Top 10 Web App Risks Quiz

15 – 20 Minutes

Open Discussion / Networking



Time Remainder

GitHub Supply Chain Attack

MARIA BROWN

maria.brown@owasp.org

GitHub Developers Hit in Complex Supply Chain Cyberattack

The attacker employed various techniques, including distributing malicious dependencies via a fake Python infrastructure linked to GitHub projects.

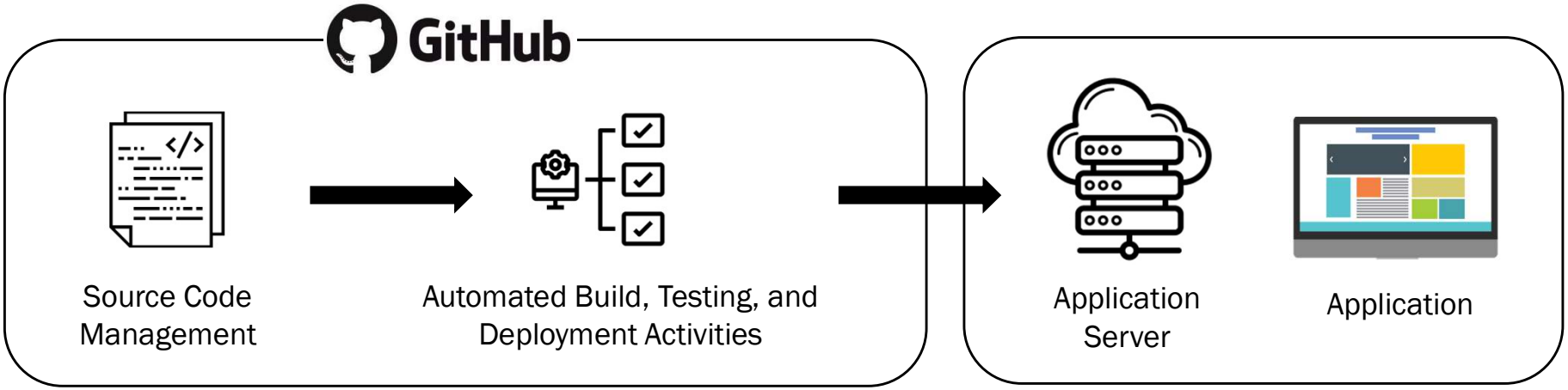
Nathan Eddy, Contributing Writer

March 25, 2024

DARKReading

3 Min Read

What is GitHub?

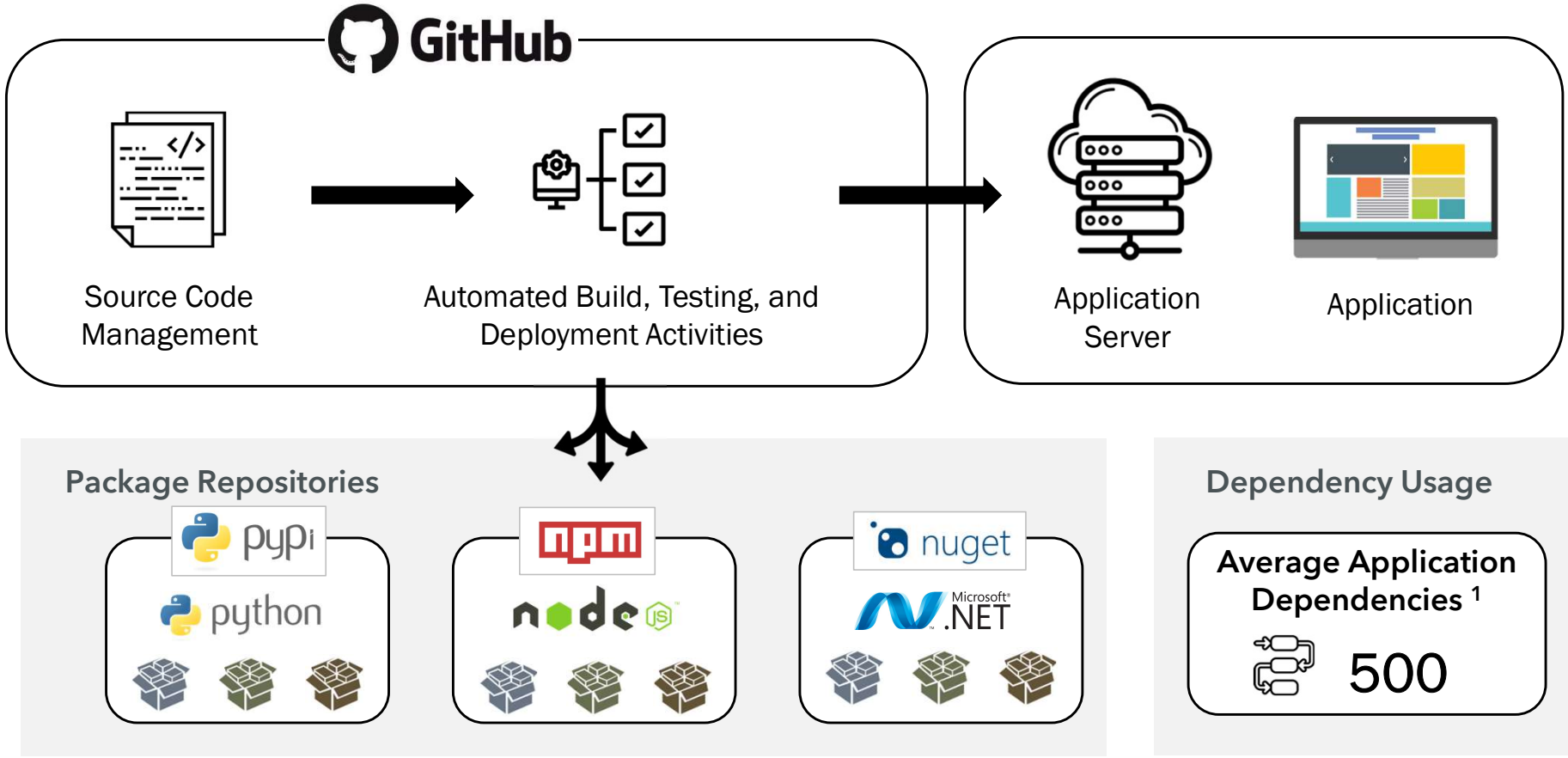


Key Points

Any development platform and any developer at risk of supply chain attack.

GitHub targeted due to size like **Outlook** targeted for email attacks.

Third Party Software Packages



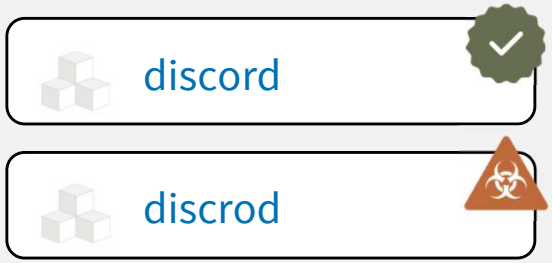
1- https://www.darkreading.com/application-security/dependency-problems-increase-for-open-source-components

Fake Dependency Mirroring and Typosquatting

Fake Dependency Mirror

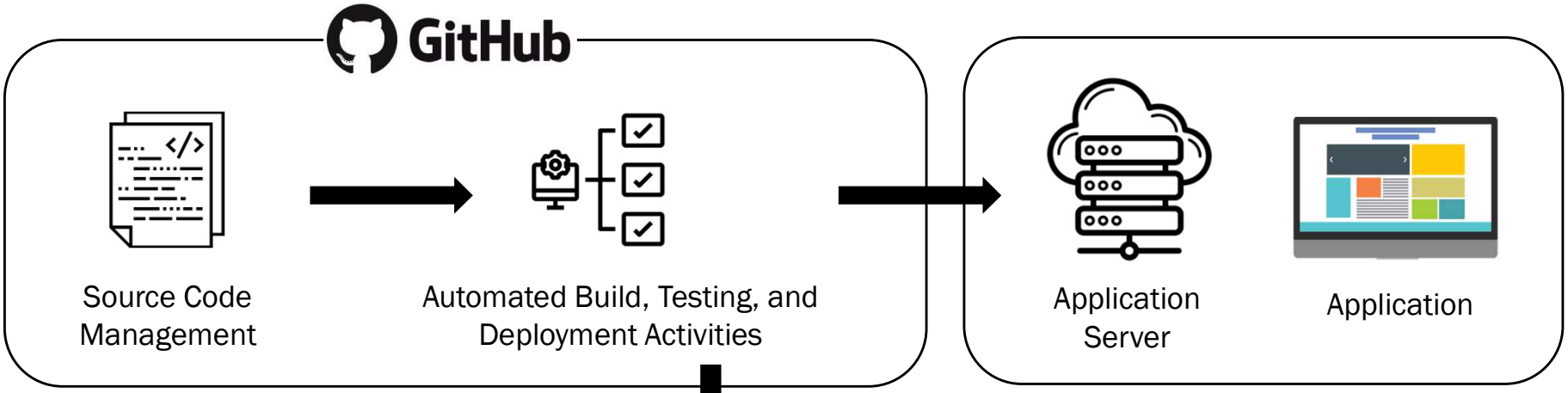
Fake Python Mirror - https://checkmarx.com/blog/over-170k-users-affected-by-attack-using-fake-python-infrastructure/

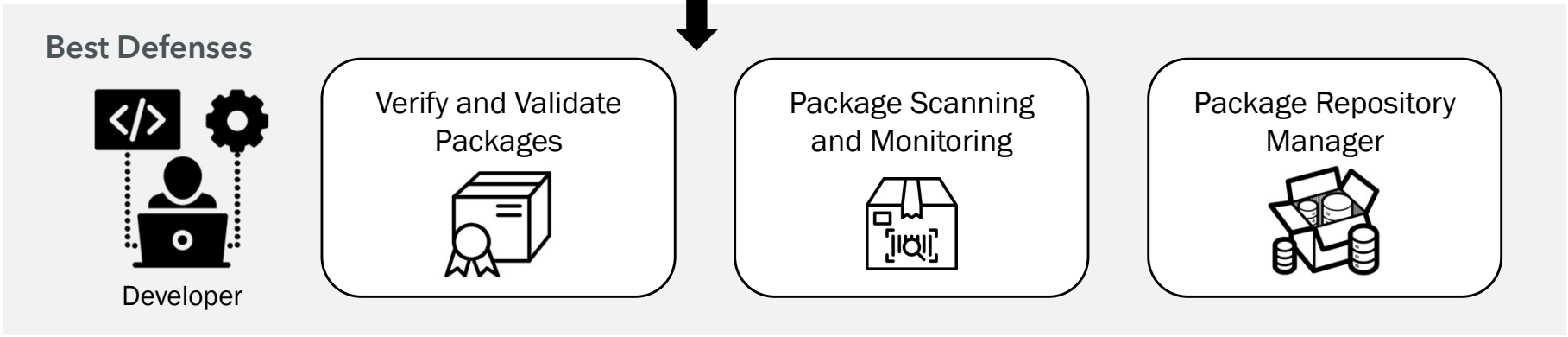
Typosquatting Packages



Discord vs Discrod - https://checkmarx.com/blog/recently-discovered-supply-chain-worm/

Supply Chain Attack Defenses





OWASP Top 10 Web Application Risks Quiz

MARIA BROWN

maria.brown@owasp.org

The OWASP Top 10 is a standard awareness document for developers and web application security.

It represents a broad consensus about the most critical security risks to web applications.

OWASP TOP 10

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

A10:2021-Server-Side Request Forgery

OWASP TOP 10

https://owasp.org/www-project-top-ten/

Question #1

What is the attack technique used to exploit websites by altering backend database queries through inputting manipulated queries?

A. LDAP Injection

B. XML Injection

C. SQL Injection

D. OS Commanding

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

C. SQL Injection

- SQL Injection is the correct answer because it is a technique used to exploit web sites by altering backend database queries through inputting manipulated queries.
- In SQL Injection, an attacker inserts malicious SQL code into input fields, which is then executed by the application's database.
- This allows the attacker to manipulate the database and potentially gain unauthorized access to sensitive information or perform unauthorized actions on the website.

Question #2

What happens when an application takes user-inputted data and sends it to a web browser without proper validation and escaping?

A. Security Misconfiguration

B. Cross Site Scripting

C. Insecure Direct Object Reference

D. Broken Authentication and Session Management

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

B. Cross Site Scripting

- When an application takes user-inputted data and sends it to a web browser without proper validation and escaping, it can lead to Cross Site Scripting (XSS) attacks.
- XSS occurs when an attacker injects malicious code into a website, which is then executed by the victim's browser.
- This can allow the attacker to steal sensitive information, manipulate website content, or perform other malicious actions.
- Proper validation and escaping of user-inputted data is essential to prevent XSS vulnerabilities and protect the application and its users.

Question #3

What flaw arises from session tokens having poor randomness across a range of values?

A. Insecure Direct Object References

B. Session Replay

C. Session Fixation

D. Session Hijacking

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

D. Session Hijacking

- The flaw that arises from session tokens having poor randomness across a range of values is Session Hijacking.
- Session hijacking occurs when an attacker intercepts and steals a user's session token, allowing them to impersonate the user and gain unauthorized access to their account or sensitive information.
- If session tokens have poor randomness, it becomes easier for attackers to guess or predict these tokens, increasing the likelihood of successful session hijacking attacks.

Question #4

An attack technique that forces a user's session credential or session ID to an explicit value.

A. Brute Force Attack

B. Session Hijacking

C. Session Fixation

D. Dictionary Attack

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

C. Session Fixation

- Session fixation is an attack technique where an attacker forces a user's session credential or session ID to an explicit value.
- This is typically done by tricking the user into using a predetermined session ID, which the attacker can then use to gain unauthorized access to the user's session.
- By fixing the session ID, the attacker can bypass authentication and gain control over the user's session, potentially leading to unauthorized actions or data theft.

Question #5

What threat arises from not flagging HTTP cookies with tokens as secure?

A. Session Hijacking

B. Insecure Cryptographic Storage

C. Access Control Violation

D. Session Replay

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

A. Session Hijacking

- Not flagging HTTP cookies with tokens as secure can lead to the threat of session hijacking.
- Session hijacking refers to an attacker gaining unauthorized access to a user's session by stealing or intercepting their session token.
- By not flagging cookies as secure, they can be transmitted over insecure channels, making them vulnerable to interception and misuse.
- This can allow an attacker to impersonate the user and perform actions on their behalf, compromising the security and integrity of the session.

Question #6

Which attack can execute scripts in the user's browser and is capable of hijacking user sessions, defacing websites, or redirecting the user to malicious sites?

A. SQL Injection

B. Cross Site Scripting

C. Malware Uploading

D. Man In The Middle

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

B. Cross Site Scripting

- Cross-site scripting (XSS) is an attack that allows an attacker to inject malicious scripts into web pages viewed by users.
- These scripts can then be executed in the user's browser, giving the attacker the ability to hijack user sessions, manipulate website content, or redirect users to malicious sites. XSS attacks are a significant threat to web applications and can lead to various security vulnerabilities if not properly mitigated.

Question #7

Which threat can be prevented by having unique usernames generated with a high degree of entropy?

A. Crypt-analysis of hash values

B. Spamming

C. Authorization Bypass

D. Authentication Bypass

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

D. Authentication Bypass

- Having unique usernames generated with a high degree of entropy can prevent authentication bypass.
- This is because using unique and complex usernames makes it difficult for attackers to guess or brute force their way into an account.
- By increasing the entropy, the likelihood of successfully bypassing the authentication system is significantly reduced, enhancing the overall security of the system.

Question #8

What threat are you vulnerable to if you do not validate the authorization of the user for direct references to restricted resources?

A. SQL Injection

B. Cross Site Scripting

C. Cross Site Request Forgery

D. Insecure Direct Object Reference

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

D. Insecure Direct Object Reference

- If you do not validate the authorization of the user for direct references to restricted resources, you are vulnerable to Insecure Direct Object References.
- This means that an attacker could bypass the intended restrictions and directly access sensitive information or perform unauthorized actions on restricted resources.

Question #9

For a connection that changes from HTTP to HTTPS, what flaw arises if you do not change the session identifier?

A. Session Replay

B. Cross Site Scripting

C. Cross Site Request Forgery

D. Session Hijacking

Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

A. Session Replay

- If a connection changes from HTTP to HTTPS without changing the session identifier, the flaw that arises is session replay.
- Session replay refers to the act of an attacker intercepting and replaying a session token or identifier to gain unauthorized access to a user's session.
- In this scenario, if the session identifier remains the same during the transition from HTTP to HTTPS, an attacker can capture the session identifier and use it to replay the session, effectively impersonating the user and gaining unauthorized access to their session.

Question #10

For every link or form which invokes state-changing functions with an unpredictable token for each user what attack can be prevented?

A. OS Commanding

B. Cross Site Scripting

C. Cross Site Request Forgery

D. Cross Site Tracing

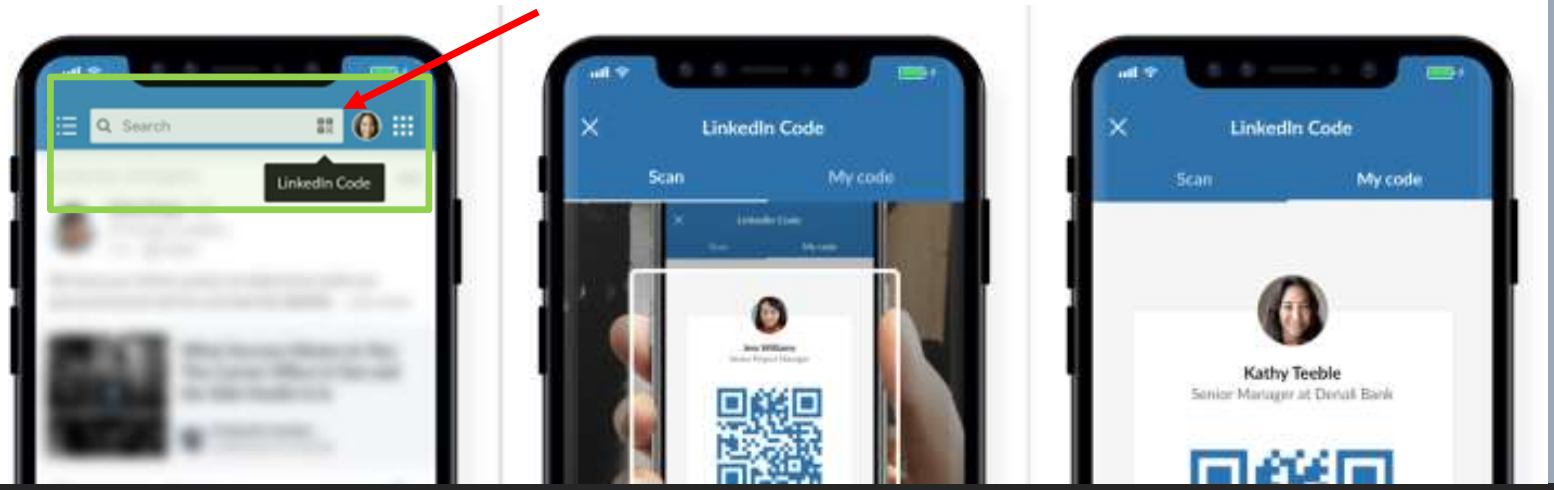
Credit: ProProfs Quizzes
https://www.proprofs.com/quiz-school/story.php?title=owasp-top-10

C. Cross Site Request Forgery

- Cross-Site Request Forgery (CSRF) attack can be prevented by using unpredictable tokens for each user when invoking state-changing functions through links or forms.
- CSRF attacks occur when an attacker tricks a user's browser into making a malicious request on behalf of the user, without their knowledge or consent.
- By using unpredictable tokens, it becomes difficult for attackers to forge valid requests as they would not be able to predict the token associated with a particular user session.
- This helps to prevent unauthorized actions and protect against CSRF attacks.

Open Discussion and Networking

LinkedIn Profile Sharing with Barcode



Noun Project Icons Credit