Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021

Unveiling the Ultimate Toolkit: Mastering Ethical Hacking & Bug Bounties with Top 5 Tools & Tricks 2021

Introduction:

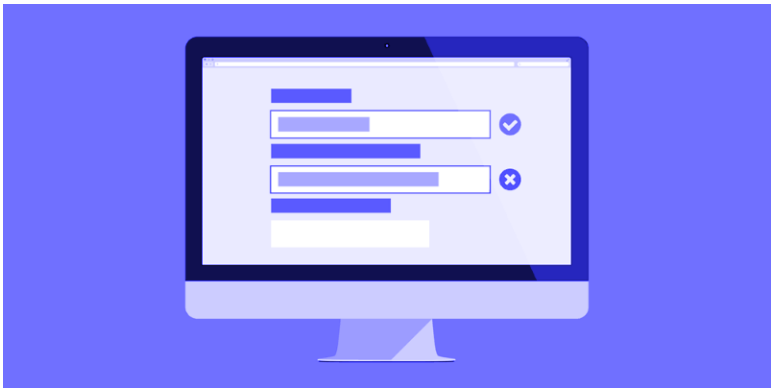
In the dynamic landscape of cybersecurity, staying one step ahead of potential threats is paramount. Ethical hackers, penetration testers, and bug bounty hunters are the guardians of this digital realm, armed with knowledge, skills, and cutting-edge tools. Welcome to the transformative Udemy course "Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021." In this article, we'll provide you with a glimpse into the exciting world of this course, which unveils the quintessential tools and techniques that can empower you to become a skilled cybersecurity professional.

10 best practices to prevent Open Redirect Vulnerabilities:

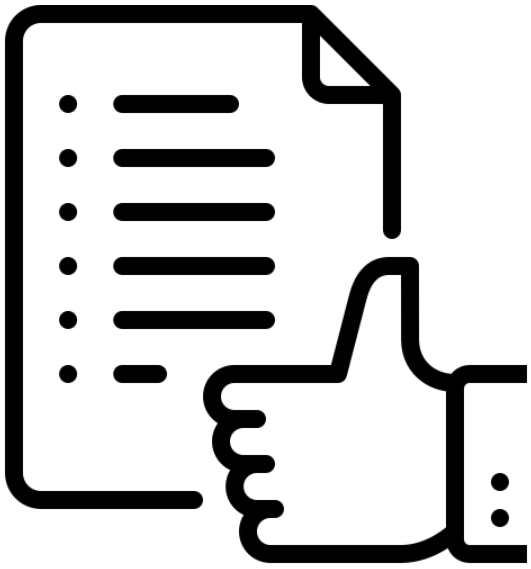
1. Avoid using forwards and redirects: Do not use them in your application to prevent open redirect vulnerabilities

2. Do not allow URLs as user input for a destination: If it's absolutely necessary to accept a URL from users, ask the users to provide a short name, token, or ID that is mapped server-side to the full target URL

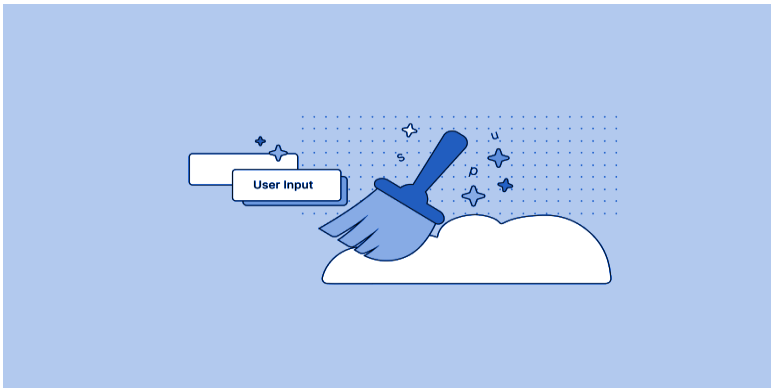
3. Validate input: Validate the input in the parameter so that only legitimate locations are allowed



4. Use whitelisting: Implement whitelisting and validate if the URL is relative or not while implementing redirects

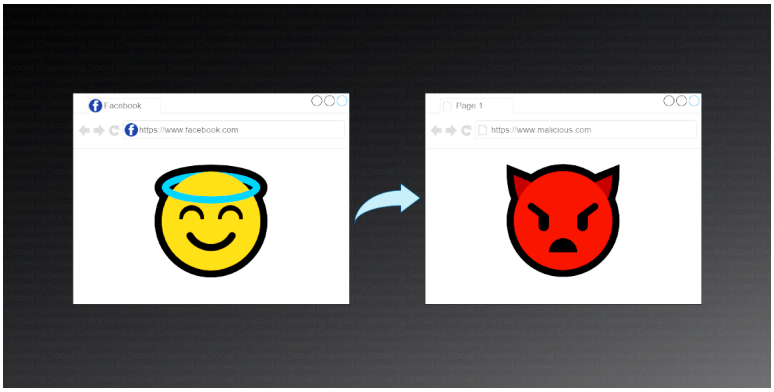


5. Sanitize input: Create a list of trusted URLs (lists of hosts or a regex) and sanitize the input based on an allow-list approach, rather than a block list

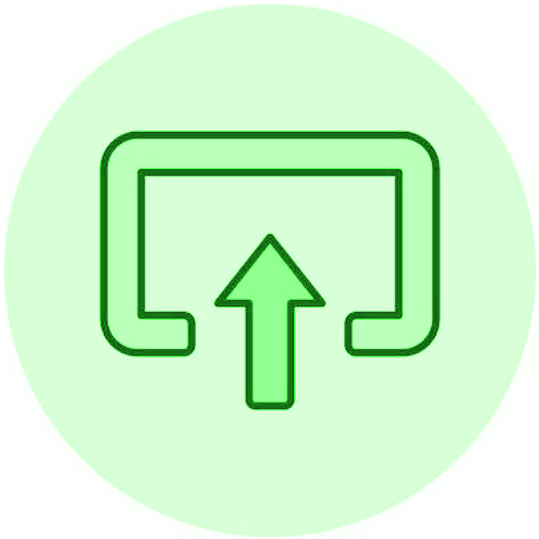


6. Force all redirects to first go through a page notifying users: This ensures that users are aware that they are being redirected and can confirm the destination

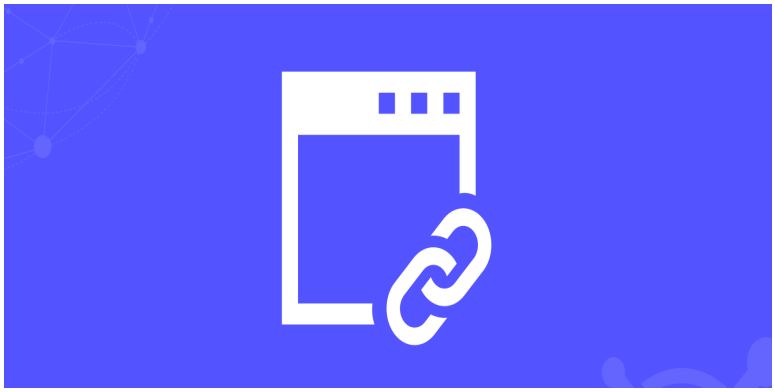
7. Safe use of redirects and forwards: If used, do not allow the URL as user input for the destination



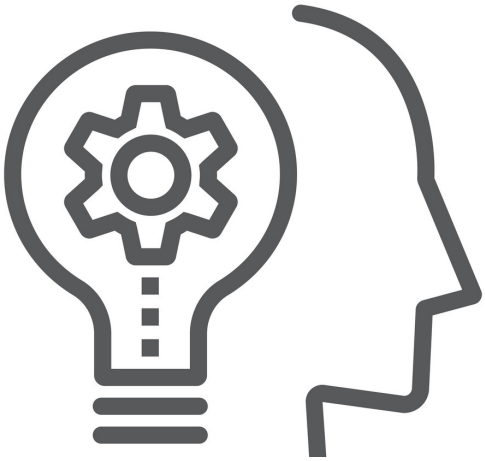
8. Ensure the supplied value is valid and appropriate for the application: If user input can't be avoided, ensure that the supplied value is valid, appropriate for the application, and is authorized for the user



9. Use relative URLs: Whenever possible, use relative URLs for redirects instead of absolute URLs



10. Educate developers: Educate developers about the risks associated with open redirect vulnerabilities and the best practices to prevent them



References:-

1. https://www.appknox.com/cyber-security-jargons/open-redirects
2. https://www.invicti.com/blog/web-security/open-redirect-vulnerabilities-invicti-pauls-security-weekly/
3. https://brightsec.com/blog/open-redirect-vulnerabilities/
4. https://learn.snyk.io/lesson/open-redirect/

5. https://www.linkedin.com/pulse/open-redirect-attacks-protecting-users-data-integrity-hacktifycs-kmjuf/