Initial Dynamic Security Scan of the Hackazon Application

Hayden Eubanks

School of Business, Liberty University

CSIS 486-D01

Prof. Backherms

November 4, 2023

Initial Dynamic Security Scan of the Hackazon Application

Introduction:

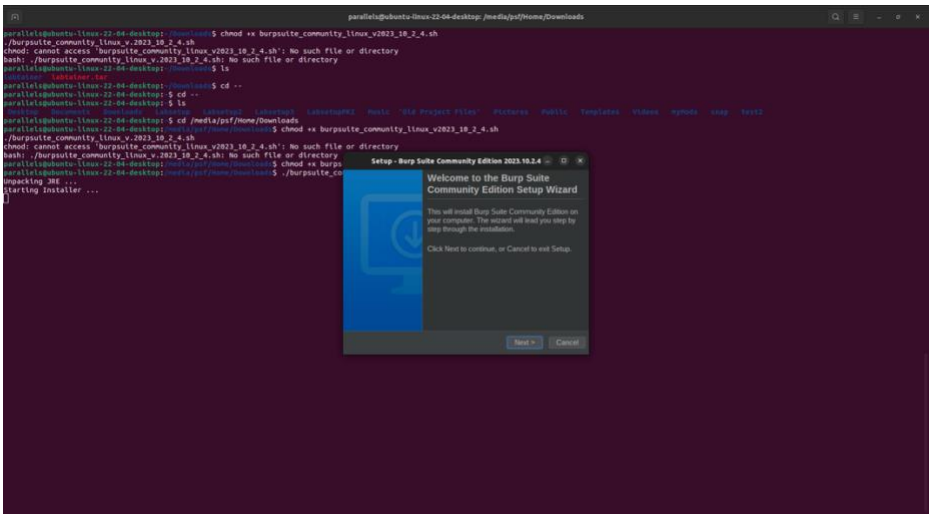
For a security professional to understand the risks facing a system they protect, they must be able to adopt the mindset of an attacker and view the system in a way that reveals what information is available to malicious actors (Simpson & Anthill, 2017). Understanding the ways that attackers may try to exploit a system can then reveal vulnerabilities that the system owners may otherwise have been blind to and allow for mitigation techniques to be applied before the vulnerabilities are exploited. This form of testing is often referred to as black-box testing as it reveals what vulnerabilities can be discovered when information regarding the internal infrastructure of the system is unknown replicating the perspective of an external malicious actor (OWASP, 2023). This process involves dynamically interacting with the components of a system and this interaction with a system in an attempt to discover vulnerabilities is a major activity of penetration testing (NCSC, 2017). Further, to increase effectiveness vulnerability scanning tools can be introduced into the penetration testing process which assists in effectively identifying aspects of a system that are prone to exploitation (Simpson & Anthill, 2017). These tools are often publicly available and as such are available to both security professionals and malicious actors alike highlighting the extreme importance for a security professional in understanding these tools as attackers may use them to profile a target system (Geeks for Geeks, 2022).

One of the most popular tools for dynamically scanning a system to locate vulnerabilities is known as the Burp Suite of tools (PortSwigger, 2023a) and this toolset allows for the easy automation of vulnerability scanning on a target system. The Burp Suite toolset greatly reduces the barrier of entry for dynamic vulnerability scanning and as such can easily be adopted by malicious actors to locate system vulnerabilities. This then further highlights the value of a

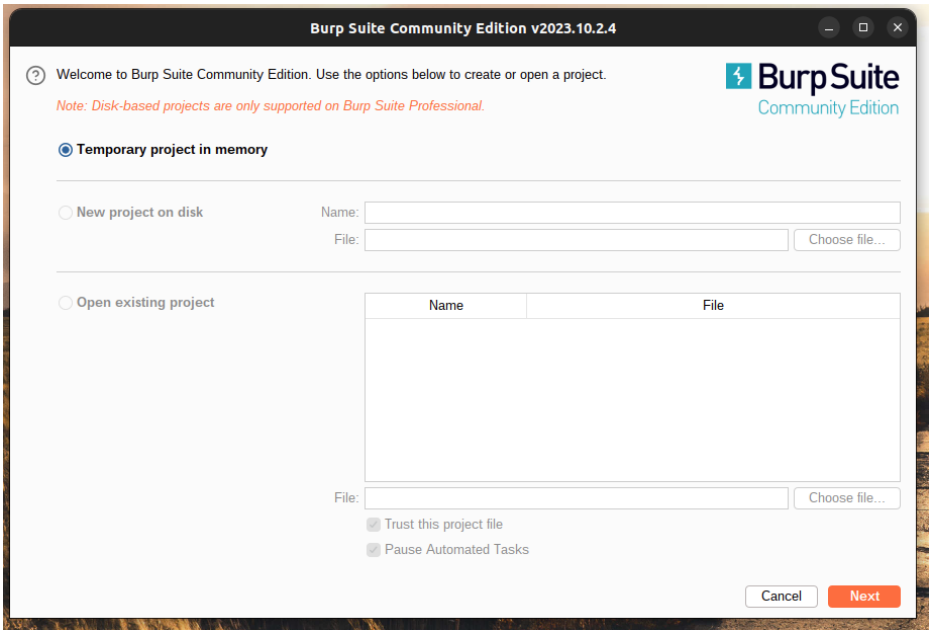
security professional understanding this tool so they can understand what vulnerabilities are advertised to malicious actors and allows for mitigation strategies to be effectively employed before exploits are performed. As such, Burp Suite will be utilized in this report to perform a dynamic security scan on the Hackazon application to discover vulnerabilities that may lie within. This information will then be used as the basis for determining the foundations of ethical reporting and exploring how this reporting can best be carried out given the sensitive nature of the exploits themselves. The dynamic scanning of a system for vulnerabilities is a powerful tool in the mitigation of risk (Geeks for Geeks, 2022), and as such it is essential that security professionals understand how tools such as Burp Suite can be used and applied to the field of ethical hacking.

Evidence of Burp Suite Configuration:

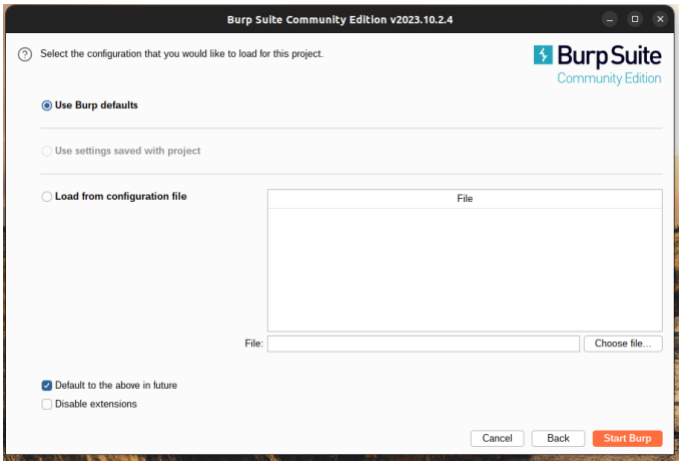
Screenshot 1: Burp Suite Community Installation



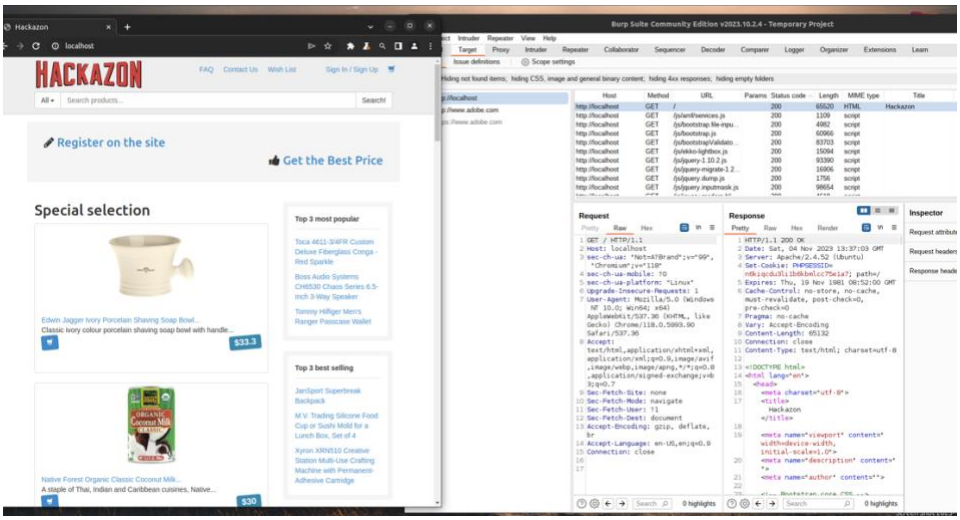
Screenshot 2: Burp Suite Configuration



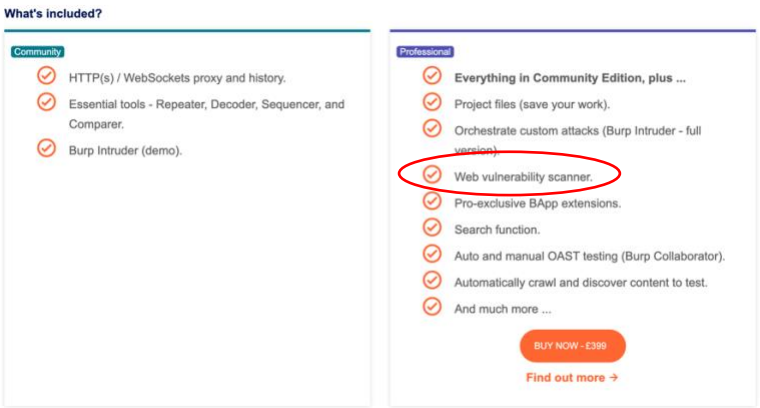
Screenshot 3: Burp Suite Configuration Continued



Screenshot 4: Burp Suite Hackazon Proxy Scan of HTTP Requests



Screenshot 5: Scanning only available in the Pro version



Vulnerability Report:

During my initialization of the Burp Suite toolset, I discovered that the automated vulnerability scanning portion of the application was unavailable in the free community version as evidenced in screenshot five above. This limitation therefore resulted in an inability to perform the vulnerability scan on the Hackazon application as detailed in the instructions. However, despite this limitation, research has been performed to investigate other applications of the Burp Suite vulnerability scanner and with this, a more generalized analysis of the vulnerability scanner will be detailed below with special emphasis being placed on the types of vulnerabilities the scanner is able to detect. Further, several vulnerabilities were discovered in the Hackazon application during the first phase of the project and an examination of Burp Suite's ability to detect these vulnerabilities will be performed to demonstrate the value of the tool within the context of the project environment.

Within the Burp Suite toolset exists a dynamic vulnerability scanner that is able to target an IP address and scan that address for known vulnerabilities (PortSwigger, 2023b). The Burp Suite scanner can detect well over a hundred vulnerability types that may be present on a system including vulnerability to SQL injection, file path traversal, cross-site scripting, web cache poisoning, cross-site request forgery, the cleartext submission of passwords, and cookie manipulation (PortSwigger, 2023b). These vulnerabilities are then classified by severity and the graphical interface of the application clearly denotes the severity of the vulnerability making it easy for a security professional to quickly identify the most pressing risks demonstrated by the system (PortSwigger, 2023b). Examining the list of vulnerabilities covered by the Burp Suite scanner then identifies that all of the most prominent vulnerabilities identified by OWASP's top ten list are discoverable through the use of the scanner (OWASP, 2021), and this view of the

vulnerabilities can allow a security professional to quickly identify the segments of the webpage that are vulnerable to attack.

Within the Hackazon webpage, several vulnerabilities exist that if exploited could cause severe damage to the application itself, the data of its users, and the reputation of the owning company. Some of the specific vulnerabilities discovered during the first phase of the project include vulnerability to SQL injection, the cleartext transfer of passwords, file tree manipulation to break access control, and session hijacking due to unencrypted session IDs. These vulnerabilities demonstrate exploits existent both in the front-end of the webpage and in the back-end of the server highlighting the potential dangers of these exploits being discovered. Fortunately, the Burp Suite scanner can detect all of these vulnerabilities and by applying the scanner to the Hackazon web application these vulnerabilities can be easily discovered and mitigation techniques prepared to strengthen system security. However, it is vital for a security professional to understand that these same tools are available to those with malicious intent and a malicious actor can just as easily identify these vulnerabilities if mitigation strategies are not put in place (Simpson & Anthill, 2017). Applying a dynamic security scanner such as Burp Suite then allows a security professional to adopt the view of a malicious actor and understand what vulnerabilities are freely discoverable within their system and then report those findings to the product owner for informed decision-making regarding mitigation techniques. Dynamic security scanners are powerful tools in footprinting a system and security professionals can adopt these tools to monitor system security and implement stronger security solutions.

Ethical Disclosure Plan:

The information provided from a dynamic security scan is information that is valuable to both security professionals and malicious actors alike and for this reason, great consideration must be placed on the format for ethically disclosing this information. For example, if a security professional discovered a severe vulnerability within a web application and then posted the information about the vulnerability publicly in the tech support forum for that application's site, a malicious actor may be able to discover the vulnerability and exploit it before mitigation strategies can be put in place. However, ethical reporting is not exclusive to the mode by which the information is reported, but also to the timeliness of the reporting (Moisset, 2023). If a vulnerability is discovered but not reported promptly, a malicious actor may have the time to discover the vulnerability and exploit it. Additionally, the information included in a report is essential for an organization to make decisions regarding mitigation strategies, and as such it is vital that the information included within a report is honest, accurate, and complete. Without an honest and complete evaluation of the vulnerabilities discovered, an organization may not fully comprehend the risks facing the system or may only partially cover the vulnerabilities resulting in the attack surface being larger than the stakeholders realize. These reporting principles are especially relevant when reporting is being performed by an external third party (Moisset, 2023), and in these circumstances, copies of the vulnerabilities discovered should be fully turned over to the owning organization.

With this in mind, it can be seen that timeliness, completeness, accuracy, honesty, and confidentiality are all essential aspects of ethically reporting vulnerabilities found within a system (Moisset, 2023). Understanding these principles then highlights that any information found during a vulnerability scan must be communicated to company stakeholders in a secure

manner such as through strongly encrypted channels and that enough information should be given for the stakeholders to accurately evaluate the risk and severity of the vulnerabilities discovered. Reporting is an essential aspect of system security as it is ultimately the product owners who assume the risk of system vulnerabilities and as such, great care should be taken in reporting these vulnerabilities to stakeholders.

References

Geeks for Geeks. (14 January, 2022). *Cyber security- Types of enumeration*. Geeks for Geeks. https://www.geeksforgeeks.org/cyber-security-types-of-enumeration/

Moisset, S. (2023). *Ethical hacking: reporting your findings*. Snyk. https://snyk.io/series/ethical-hacking/reporting-for-hackers/

NCSC. (August 8, 2017). *Penetration testing: How to get the most from penetration testing.* National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/penetration-testing

OWASP. (2023). *OWASP DevSecOps guideline – v-0.2: Dynamic application security testing (DAST)*. OWASP. https://owasp.org/www-project-devsecops-guideline/latest/02b-Dynamic-Application-Security-Testing

OWASP. (2021). *OWASP top ten: Top 10 web application security risks*. OWASP. https://owasp.org/www-project-top-ten/

PortSwigger. (2023a). *Cybersecurity solutions*. PortSwigger. https://portswigger.net/solutions

PortSwigger. (October, 2023b). *Vulnerabilities detected by Burp scanner*. PortSwigger. https://portswigger.net/burp/documentation/scanner/vulnerabilities-list

Simpson, M. T., Anthill, N. (2017). *Hands-on ethical hacking (3rd ed.)*. Cengage Learning. https://ng.cengage.com/static/nb/ui/evo/index.html?deploymentId=5681612456081340358553076923&eISBN=9781337271721&id=1937025370&snapshotId=3720027&