HAKIN9

CAL PROTECTION

IT SECURITY MAGAZINE

VOL.18, NO.03

BURPGPT

PENETRATION TESTING WITH BURPSUITE
ENHANCING WEB APPLICATION SECURITY

CYBER THREAT WITH CHATGPT

EXCLUSIVE INTERVIEW WITH ALEXANDRE TEYAR
THE CREATOR OF BURPGPT

AND MORE...

Team

Editor-in-chief:

Joanna Kretowicz
joanna.kretowicz@hakin9.org

Managing Editor:

Agata Staszelis
agata.staszelis@hakin9.org

Editors:

Bartek Adach
bartek.adach@pentestmag.com

Ewa Dudzic
ewa.dudzic@eforensicsmag.com

Jacek Stankiewicz
jacek.stankiewicz@hakin9.org

Proofreader:

Lee McKenzie

Senior Consultant/Publisher:

Paweł Marciniak

CEO:

Joanna Kretowicz
joanna.kretowicz@hakin9.org

Marketing Director

Joanna Kretowicz
joanna.kretowicz@hakin9.org

DTP:

Agata Staszelis
agata.staszelis@hakin9.org

Cover Deisgn:

Hiep Nguyen Duc
Joanna Kretowicz

Beta Testers & Proofreaders

Lee McKenzie

Gabriele Biondo

Bryan Hoffower

Michal Jachim

Michael Hammond

Allan Murray

Skwarek, Volker

Salman Aslam

Thomas Moosmüller

Amit Chugh

David Kosorok

Girshel C

Zaher el-Siddik

Alex Lucas

Jordan M. Bonagura

Hammad Arshed

Kevin Goosie

Publisher:

Hakin9 Media Sp. z o.o.
00-585 Warszawa
ul. Bagatela 10
1 917 338 3631
www.hakin9.org

TABLE OF CONTENTS

INTRODUCTION

Jacek Stankiewicz

Dear Readers,

AI is still an important and popular tool, therefore, we have decided to still talk about it, but also to mix it a bit with pentesting. Burp Suite is a pentesting tool used by many professionals and BurpGPT is an extension that allows it to use ChatGPT for pentesting. This is a great mixture of both Pentesting and ChatGPT. Thus, we decided to make that extension the main topic of the magazine. With that explained, we invite you to enjoy this edition's content!

At the beginning, we decided to talk about Burp Suite and its use in Pentesting. An article from a returning author explains how useful Burp Suite can be in pentesting and how to use it in your work. The next article dives into ChatGPT, especially the threat it can create by being exploited or misused.

We also provided you with an interview! Alexandre Teyar, the creator of BurpGPT agreed to talk with us about his tool, his future plans and the importance of AI in Cybersecurity. After that, you can delve into the world of APIs inside of IoT devices in this two-part article.
This edition is also a premier of Hakin9 Crime Corner, articles about the Dark Web, and the many threats within it. Our author, who is an experienced investigator, explained his work with real life examples!
One of a few articles we had to censor.
One of our authors will help you protect yourself from people like him, as he is a pentester who uses social engineering, OSINT and other tools to get information. We will also talk about REDOS, and Google's new TLDs and their impact on cybersecurity, especially of internet sites. In the last article, you'll read about Personal Network Security.

Without further ado, grab something cold to drink and enjoy this summer's edition of the Hakin9 Magazine!
Jacek Stankiewicz and the Hakin9 Editorial Team

Opinder Singh

Penetration Testing with Burp Suite: Enhancing Web Application Security

In today's interconnected world, web applications play a critical role in various aspects of our lives, ranging from online banking to e-commerce and social media. However, with the increasing complexity and sophistication of cyber threats, it has become more important than ever to ensure the security and integrity of these applications. This is where penetration testing, combined with powerful tools like Burp Suite, becomes crucial.

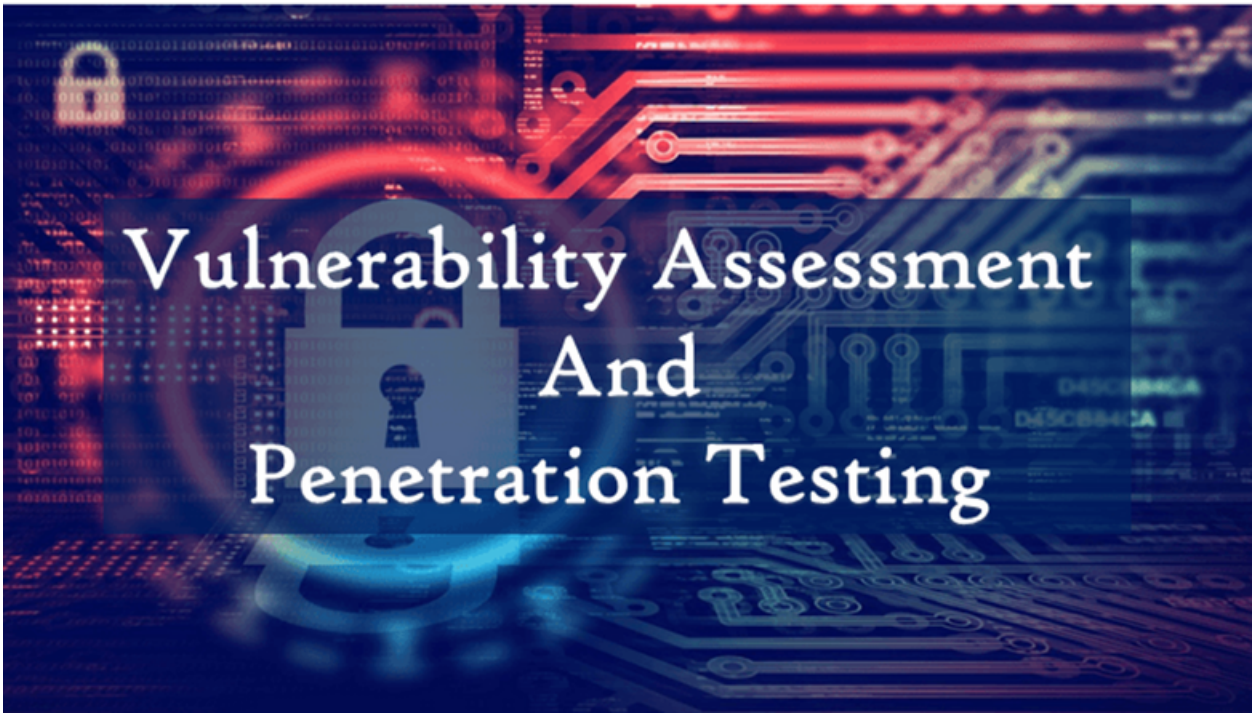
What is Penetration Testing?

Penetration testing, also known as ethical hacking or white-hat hacking, is a proactive approach to identifying vulnerabilities and weaknesses in a system or application. Penetration testing involves simulating real-world attacks on an organization's systems to identify vulnerabilities, weaknesses, and potential entry points that malicious attackers could exploit.

The primary objective of penetration testing is to uncover security vulnerabilities before they are discovered and exploited by actual attackers. By conducting controlled and authorized testing, organizations can proactively identify and address weaknesses in their security defenses, reducing the risk of unauthorized access, data breaches, and other security incidents.

Introduction to Burp Suite

Burp Suite is a powerful and widely used web application security testing tool designed to help security professionals identify vulnerabilities in web applications. It has become an essential tool in the arsenal of penetration testers and security researchers who are responsible for ensuring the security of web applications.



Developed by PortSwigger, Burp Suite provides a comprehensive set of features that enable users to thoroughly analyze the security posture of web applications. With its intuitive user interface and extensive functionality, Burp Suite allows users to perform a variety of security testing tasks, including scanning for common vulnerabilities, intercepting and modifying web traffic, and actively probing applications for weaknesses.

With the help of Burp Suite, pentesters can dive deep into the application's functionality and identify more complex vulnerabilities. Activities like fuzzing, brute-forcing, and parameter manipulation can be

performed to uncover hidden security flaws that automated scanners might miss.

Burp Suite consists of several key features that aid in various stages of the security testing process. Let's explore these features in detail:

1. Proxy: The Proxy module acts as an intermediary between the browser and the target application. It allows you to intercept and modify the HTTP and HTTPS traffic exchanged between the client and the server. This feature helps in analyzing and modifying requests and responses, enabling you to identify security flaws, such as injection attacks, cross-site scripting (XSS), and many more.

2. Spider: The Spider feature automates the process of crawling a website to identify its structure and discover hidden or unlinked content.
It maps out the application's functionalities and identifies additional endpoints and pages that might not be readily accessible. This feature is useful for comprehensive application mapping and identifying potential attack vectors.

3. Scanner: Burp Suite's Scanner module is designed to automatically identify security vulnerabilities in web applications. It performs a wide range of security tests, including SQL injection, cross-site scripting (XSS), directory traversal, and many other common web vulnerabilities. The Scanner module assists in automating the vulnerability identification process and provides detailed reports for analysis and remediation.

4. Intruder: The Intruder tool allows you to perform automated attacks on web applications, such as fuzzing and brute-forcing. It enables you to define payloads and attack parameters, such as injection points, to test the application's resilience against different attack vectors. This feature

is beneficial for identifying vulnerabilities related to user input handling and authentication mechanisms.

5. Repeater: The Repeater tool provides a simple and intuitive interface for manual request/response modification and replay. It allows you to modify specific aspects of an intercepted request and resend it to the server. This feature is helpful for manual testing, experimenting with different inputs, and analyzing the application's behavior to identify security weaknesses.

6. Sequencer: The Sequencer module analyzes the randomness and quality of session tokens or other values used for security-critical operations. It helps in identifying weaknesses in the generation or usage of random values, which can be exploited by attackers to predict or bypass security measures.

7. Decoder: The Decoder feature aids in encoding/decoding various data formats commonly used in web applications. It supports a wide range of encodings, including URL encoding, Base64 encoding, HTML encoding, and more. This feature is valuable for analyzing and manipulating data payloads, understanding how data is transformed, and identifying potential security issues arising from encoding or decoding operations.

8. Collaborator: Burp Suite's Collaborator functionality allows you to interact with external systems during testing to detect blind vulnerabilities. It provides a unique subdomain and various other interaction methods that can be used to determine if the application is making any unexpected requests or leaking sensitive information.

9. Extensibility: Burp Suite supports a powerful extension API that allows you to enhance its functionality through custom-built extensions. You can develop your own extensions or leverage the wide range of existing extensions developed by the Burp Suite community. This extensibility enables you to integrate Burp Suite into your existing security workflow, automate repetitive tasks, and customize the tool according to your specific needs.

Some popular Burp extensions that are widely used by security researchers and penetration testers include:

- **Authorize:** The “Authorize” extension is a plugin in Burp Suite that allows you to test the authorization and access controls of a web application. Authorize allows you to simulate different user roles and permissions to see how the web application behaves. For example, you can test whether a user with limited access can access or modify sensitive data, or whether a user can perform actions that they are not authorized to perform. By testing different user roles and permissions, you can identify potential vulnerabilities and take steps to address them before attackers can exploit them.
- **Param Miner:** This extension helps researchers identify hidden parameters in web applications. It can be used to identify parameters that are not visible in the user interface but can be manipulated by attackers to exploit vulnerabilities.
- **Upload Scanner:** File upload functionality is common in many web applications and allows users to upload files to the server. However, if this functionality is not properly secured, it can lead to security vulnerabilities, such as remote code execution or file disclosure. The “Upload Scanner” extension can help security professionals to identify such vulnerabilities by scanning the uploaded files for malicious content.
- **JWT Editor:** The JWT Editor extension allows you to decode and view the contents of the JWT, including the header, the payload, and the signature. You can also modify the contents of the JWT, such as changing the user ID or role, to test the behavior of the web application. Additionally, the JWT Editor extension can detect common vulnerabilities in the JWT implementation, such as weak algorithms or missing expiration times.
- **Reflected Parameters:** Reflected parameters are user-controlled values that are reflected in the response of a web application. Attackers can exploit these parameters to execute various attacks, such as cross-site scripting (XSS), by injecting

malicious code into the parameter value. The “Reflected Parameters” extension can help security professionals to identify such parameters and test for potential vulnerabilities.

- **js:** This extension can be used to scan JavaScript files and HTML pages for outdated libraries and known vulnerabilities. It supports scanning both static and dynamic JavaScript files, including those loaded through AJAX requests. The plugin integrates with Burp Suite’s scanner and can also be used in manual mode for more focused testing.

Steps to be followed to get started with Burp Suite:

1. Set up Burp Suite: Before testing vulnerabilities, you need to set up Burp Suite. First, install the tool on your system. Next, set up your proxy by going to the “Proxy” tab in Burp Suite and selecting the “Intercept is on” button. Finally, configure your browser to use the Burp Suite proxy by changing the proxy settings.

2. Identify the target: Identify the web application you want to test for vulnerabilities. To avoid capturing any unwanted traffic, add the target URL to Burp Suite’s scope by going to the “Target” tab and clicking on “Scope”. Then, click on “Add” and enter the target URL.

3. Reconnaissance: Conduct reconnaissance to gather information about the web application. Manually visit each and every functionality of the website with proxy ON or, additionally, use Burp Suite’s features like the Target Analyzer, Spider, and Sitemap generator to collect information about the application’s structure, functionality, and endpoints. The Target Analyzer automatically analyzes the target URL and identifies common web technologies and directories. The Spider tool crawls the target application to discover all available pages and functionality. The Sitemap generator creates a graphical representation of the application’s structure.

4. Vulnerability Scanning: Before manually looking for vulnerabilities, use Burp Suite's vulnerability scanner to scan for common web application vulnerabilities. Burp Suite's active scanner performs a series of tests to check for various types of vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), Remote File Inclusion (RFI), Local File Inclusion (LFI), and more. The active scanner sends crafted requests to the web application, analyzes the responses, and reports any potential vulnerabilities.
To scan for vulnerabilities, go to the "Scanner" tab and click on "New scan". Select the target scope and choose the scan configuration.
Note that active scanning generates more noise and false positives, so it is essential to carefully run such scans and manually investigate all the findings.

5. Manual Testing: Manual testing is an essential part of security testing as it can identify vulnerabilities that most of the automated scanners miss. Burp Suite helps a lot in identifying and exploiting the vulnerabilities. Its various modules and rich features like Proxy, Repeater, and Intruder can be utilized to simulate attacks on the application.
For example, use the Proxy tool to intercept and modify requests and responses. Use the Repeater tool to repeat and modify specific requests to test for vulnerabilities like SQL injection, CSRF, XSS, etc. Use the Intruder tool to automate the process of testing for vulnerabilities by brute-forcing parameters and payloads.

6. Reporting: After identification and exploitation you can document your findings. The report should include the vulnerabilities found, POC, the impact of each vulnerability, and recommendations for remediation.

To learn more and gain hands-on experience of Burp Suite and web application security, you can check out PortSwigger labs.

Conclusion

Web application security is of utmost importance in today's threat landscape, and penetration testing plays a vital role in identifying and mitigating potential vulnerabilities. Burp Suite, with its extensive set of features and flexibility, has emerged as a leading tool for performing effective web application security assessments. By leveraging its capabilities, security professionals can enhance the security posture of web applications, protect sensitive data, and stay one step ahead of potential attackers.

Jacek Stankiewicz

Exclusive Interview with Alexandre Teyar – the creator of BurpGPT

Dear Readers, Burp Suite and ChatGPT have been hot topics in the world of Cybersecurity. That is why we have decided to talk with the person who connected them both. The guest in this interview is Alexandre Teyar, the creator of BurpGPT, but it's best he introduces himself.

- **[Hakin9]** Could you tell us a little bit more about yourself? What got you into Cybersecurity

[Alexandre] My passion for cyber security and IT began during my teenage years when I started reverse engineering and cracking games. I went on to pursue a master's degree in Computer Science, Network, and Telecommunication Systems from a French engineering school, where I had the opportunity to study in Ireland and Sweden, adding an international perspective to my education. My first job was as a pentester for a vulnerability scanner vendor, where I gained a strong foundation in offensive security. Currently, I am the Managing Director at Aegis Cyber, a UK-based cyber boutique that provides high-quality security services. Over the past decade, I have worked with more than 100 clients from diverse industries, including defense, oil, fintech, and crypto, to secure their information systems. I have experience in securing mobile apps, cloud infrastructure, web apps, and IoT devices. As a researcher, I have published papers on various topics, including mobile banking application security. I have also developed cutting-edge hacking techniques such as smali malware injection and evil twin attacks. Additionally, I am a developer who has created multiple cybersecurity tools that have become industry standards. BurpGPT is one such example.

- **[Hakin9]** Do you see the impact of AI on cybersecurity even now and do you think it will start becoming more and more important?

[Alexandre] AI is undeniably transforming the landscape of cybersecurity. At present, the most significant impact can be observed on the defensive side, with the widespread adoption of AI-powered intrusion detection and prevention systems (IDS/IPS) and other cutting-edge technologies employed by blue teams. On the offensive side, red teams are only just beginning to harness the potential of AI for cyberattacks, which has sparked numerous ethical debates on professional platforms like LinkedIn. As AI continues to evolve, its role in cybersecurity will undoubtedly become increasingly vital, shaping both the strategies of cyber defenders and the tactics of attackers.

- **[Hakin9]** In your opinion, can ChatGPT be a useful tool for cybersecurity specialists?

[Alexandre] ChatGPT showcases the potential of AI, particularly large language models, in addressing intricate challenges that would typically necessitate expertise in specialized fields, such as advanced cryptography, as well as considerable time and resources. When properly implemented and utilized, ChatGPT can undoubtedly offer valuable insights and support in tackling a wide array of network traffic and cybersecurity issues. As the technology continues to develop, cybersecurity specialists can benefit greatly from incorporating AI-powered tools like ChatGPT into their arsenal.

- **[Hakin9]** Have you created any other Burp extensions? What got you interested in Burp?

[Alexandre] I have created numerous Burp extensions, with the most prominent ones being the OpenAI parser and BurpGPT. Both were developed to tackle issues that Burp Suite initially had no built-in

solutions for, and they rapidly gained recognition as industry standards. My interest in Burp Suite stemmed from my career as a penetration tester. Having been immersed in offensive cybersecurity for as long as I can remember, I have utilized essential tools in the red teamers' arsenal. Burp Suite has consistently been a top choice (alongside OWASP ZAP, and more recently, Nuclei and other modern frameworks) for web application testing. Consequently, I have devoted considerable time to mastering Burp Suite at its core, extending its innate capabilities to leverage its robust scanning engine for custom engagements tailored to my clients' needs.

- **[Hakin9]** Are there any more projects you're working on?

[Alexandre] Currently, I am working on a Pro edition of BurpGPT that is slated for release in the near future. This upgraded version is designed to address the feedback gathered from the expert community after BurpGPT's initial launch. Stay tuned for updates on this exciting development as I continue to refine and expand the capabilities of this AI-driven tool for cybersecurity professionals.

- **[Hakin9]** Can AI-solutions be key in securing private resources?

[Alexandre] AI solutions for cybersecurity can be a double-edged sword, resembling a cat-and-mouse game. As AI progresses, its power will be harnessed by both blue and red teamers, potentially neutralizing each other's advancements. Additionally, data privacy concerns arise due to the current model, which necessitates sending data to centralized servers for analysis before receiving a response. This issue can be somewhat alleviated by deploying enterprise on-premises servers, but doing so requires specialized knowledge, and not all users may prioritize addressing these data privacy concerns. Consequently, striking a balance between AI-driven security benefits and data privacy remains an ongoing challenge in the field of cybersecurity.

• **[Hakin9]** What else may be a game changer in cybersecurity in your opinion?

[Alexandre] In my view, AI represents the most significant technological leap of the century, if not the millennium, and we are just at the dawn of this new era. The only other contender in the realm of information technology would be quantum computing, which faces physical and technological constraints that place it second on my list.

• **[Hakin9]** What's the difference between your new project BurpGPT Pro and BurpGPT?

[Alexandre] BurpGPT Pro offers a wide range of features that have been highly requested by the community of specialists. One of the most notable features is the ability to run everything locally, ensuring that no data ever leaves the network when using local Large Language Models. This is particularly advantageous for security specialists who need to perform engagements for their clients without compromising any data privacy requirements. Additionally, users can now create and use custom-trained models, which means that companies and specialists alike can spend time training a model on a very specific type of traffic analysis and then utilize it with Burp through BurpGPT Pro. This opens up a world of practical applications. Along with these significant improvements, the UI/UX has been enhanced, and a prompt library has been added. For more information, please visit https://burpgpt.app.

• **[Hakin9]** With the implementation of AI, can cybersecurity specialists be afraid of their jobs?

[Alexandre] Artificial Intelligence (AI) is rapidly changing the cybersecurity landscape. With the increasing ability of models to understand the expected behavior of complex applications, they can detect logic bugs, which is something that non-AI vulnerability scanners

struggle with. This is one of the reasons why offensive security jobs still exist. However, this transition will take some time, and I believe that there will always be a need for highly skilled specialists to instruct and operate these models/AI co-pilots. This is also true for the blue team side of things, as we see blue team tooling gaining new “AI-features” every day. Once these technologies reach maturity, I believe there will be two possible outcomes. The first outcome is massive layoffs within the cybersecurity industry as staff gets replaced by AI-powered tools. The second outcome is huge productivity gains by assisting, training, and educating staff with these AI tools. The way companies choose to adopt AI tools will heavily depend on industry-specific factors and economic factors.