MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI

GOVERNMENT POLYTECHNIC DHARASHIV CERTIFICATE

"Reverse Shell Access Using PHP SHELL KB"

Submitted by Mr.: Shingare Om Prashant Roll no: - 49 in sixth semester of diploma in computer engineering has completed micro projects satisfactorily in the course **PHP (22518) academic** year 2023-2024 as prescribed in the curriculum.

Place: Dharashiv. Enrolment No- 2101180366

Date: / /2023 Exam Seat No-

Subject Teacher Head of the Department principal

Seal of Institution

GOVERNMENT POLYTECHNIC DHARASHIV

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI

Micro project title: - “Reverse Shell Access Using PHP SHELL KB”

Submitted by: -

Roll No	Name of student	Enrollment no.	Seat no.
49	Shingare Om Prashant	2101180366	

Under The Guidance Of
B.S. Mali Mam

ACKNOWLADGEMENT

I am grateful to Almighty God for giving me the strength, knowledge and understanding to complete this project. His love has been more than sufficient to keep and sustain me.

My profound gratitude goes to my wonderful supervisor B. S. Mali mam for her invaluable support, patience, time and guidance in seeing me to the completion of this micro project.

I extend gratitude and appreciation to our HOD sir Mr. Gaikwad sir in department who have taught me at one point or the other. May God continue to bless, protect and guide you all.

I also wish to acknowledge the great support of my parents, siblings who have been a source of inspiration towards my academic pursuit. God bless you all.

Om Shingare,
Computer eng.

INDEX

RATIONALE

The purpose of this project is to raise awareness about the security threats posed by PHP shells on a server. PHP shells are commonly used by both attackers and security researchers to gain unauthorized access to web applications and servers. Understanding the security threats associated with PHP shells is crucial for web developers, system administrators, and security professionals to ensure the security and integrity of their web applications and servers.

COURSES OUTCOMES

The theory, practical experiences and relevant soft skills associated with this course are to be taught and implemented, so that the student demonstrates the following industry-oriented COs associated with the above-mentioned competency:

1. Develop program using control statement.
2. Perform operations based on arrays and graphics.
3. Develop programs by applying various object-oriented concepts.
4. Use form controls with validation to collect user's input.
5. Perform database operations in PHP.

AIM

The primary aim of this project is to demonstrate the various security threats associated with PHP shells on a server. By doing so, the project aims to raise awareness about the potential risks and vulnerabilities that can arise from the use of PHP shells. Through this project, you will:

1. Identify and explain the different types of security threats that can be exploited through PHP shells, such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload.
2. Provide detailed examples of how these security threats can be exploited through PHP shells, thus helping web developers, system administrators, and security professionals to better understand the potential risks and vulnerabilities associated with these tools.
3. Discuss various mitigation strategies that can be implemented to secure PHP shells and protect web applications and servers from potential attacks.

PROJECT OUTCOMES

Here are the project outcomes:

1. A comprehensive understanding of PHP shells, their functionalities, and the potential security threats associated with them.
2. The ability to identify and exploit various security threats associated with PHP shells, such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload.
3. A thorough knowledge of various mitigation strategies that can be implemented to secure PHP shells and protect web applications and servers from potential attacks.
4. The development of essential skills in web security, which will be valuable in your future career as a web developer, system administrator, or security professional.
5. A contribution to the overall security of the web by sharing your knowledge and findings with the community, thus helping to reduce the number of vulnerable web applications and servers. By achieving these outcomes, you will be better equipped to identify, exploit, and mitigate security threats associated with PHP shells. This will enable you to contribute to a more secure web environment in your future career as a web developer, system administrator, or security professional.

REVIEW OF LITERATURE

project aims to demonstrate the various security threats associated with PHP shells on a server, with the ultimate goal of raising awareness about the potential risks and vulnerabilities that can arise from the use of these tools. By identifying and exploiting security threats such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload, and discussing various mitigation strategies to secure PHP shells and protect web applications and servers from potential attacks, you will gain a comprehensive understanding of PHP shells and their potential security threats. This project will equip you with the necessary knowledge and skills to identify, exploit, and mitigate security threats associated with PHP shells, ultimately contributing to a more secure web environment in your future career as a web developer, system administrator, or security professional.

INTRODUCTION

project focuses on demonstrating the security threat for the PHP shell on a server, with the ultimate goal of raising awareness about the potential risks and vulnerabilities that can arise from the use of these tools. The project aims to provide a comprehensive understanding of PHP shells, their functionalities, and the potential security threats associated with them.

Through this project, you will identify and exploit various security threats associated with PHP shells, such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload. By doing so, you will gain a thorough knowledge of the various types of PHP shells, their functionalities, and the potential security threats associated with them.

Furthermore, you will discuss various mitigation strategies that can be implemented to secure PHP shells and protect web applications and servers from potential attacks. This will enable you to develop essential skills in web security, which will be valuable in your future career as a web developer, system administrator, or security professional.

By completing this project, you will be better equipped to identify, exploit, and mitigate security threats associated with PHP shells. This will enable you to contribute to a more secure web environment in your future career as a web developer, system administrator, or security professional.

In summary, your project aims to provide a comprehensive understanding of PHP shells and their potential security threats, while also equipping you with the necessary knowledge and skills to identify, exploit, and mitigate these security threats. This project will ultimately contribute to a more secure web environment in your future career as a web developer, system administrator, or security professional.

PHP SHELL

PHP shells are web-based tools that allow users to execute system commands and interact with the underlying operating system. These tools are commonly used by both attackers and security researchers to gain unauthorized access to web applications and servers. PHP shells can be embedded within a web application's code or uploaded to a web server.

PHP shells come in various forms and functionalities. Some common functionalities of PHP shells include the ability to execute system commands, browse and manipulate files on the server, and interact with databases.

Your project focuses on demonstrating the security threat for the PHP shell on a server. The primary aim of this project is to raise awareness about the potential risks and vulnerabilities that can arise from the use of PHP shells.

By identifying and exploiting various security threats associated with PHP shells, such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload, and discussing various mitigation strategies to secure PHP shells and protect web applications and servers from potential attacks, you will gain a comprehensive understanding of PHP shells and their potential security threats.

This project will equip you with the necessary knowledge and skills to identify, exploit, and mitigate security threats associated with PHP shells, ultimately contributing to a more secure web environment in your future career as a web developer, system administrator, or security professional.

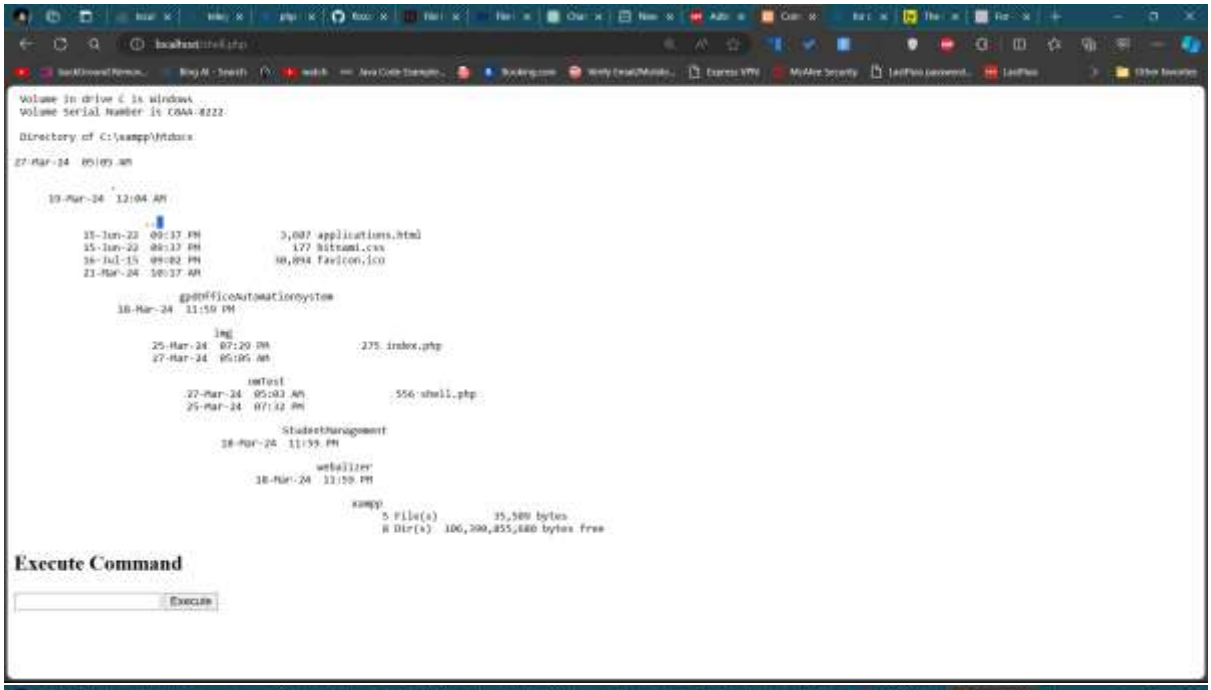
CODE

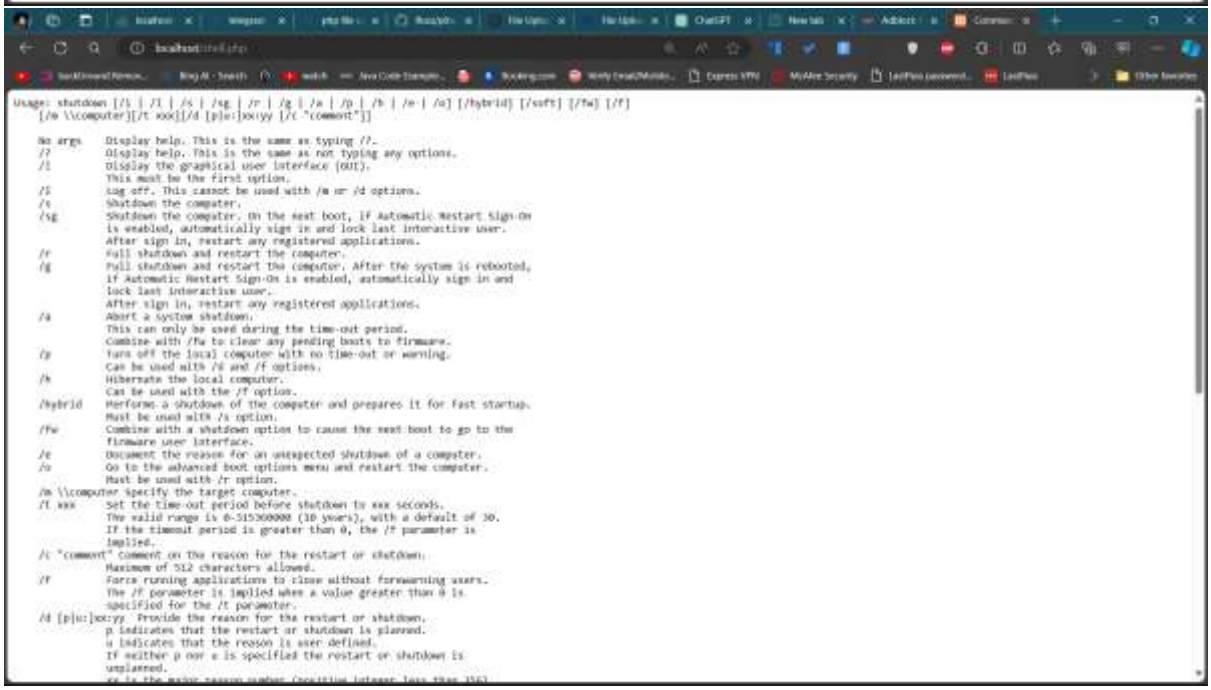
```php
<?php
// Check if the form has been submitted
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    // Extract the command from POST data
    $command = $_POST['command'];

    // Execute the command
    $output = shell_exec($command);

    echo "<pre>$output</pre>";
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>Command Execution</title>
</head>
<body>
    <h2>Execute Command</h2>
    <form method="post">
        <input type="text" name="command" required>
        <input type="submit" value="Execute">
    </form>
</body>
</html>
```

RESOURCES USED

Sr No.	Resources	Specs	Qty	Remarks
1.	Computer system	Ram: 8 GB, Rom: 512 SSD, OS: Windows	1	
2.	Software	Visual Studio, Maven Compilers.	1	
3.	Any other resources used	Maven Lib.	1	

OUTPUT IMAGES





aDEDICATION

Hello, I'm Om Shingare. Actually, I'm deeply passionate about creating projects that serve a purpose and have a meaningful impact on my college and the broader community. My dedication lies in the belief that technology should be a force for good, addressing real-world challenges and enhancing educational experiences.

In my journey as a developer, I have consistently focused on projects that are not just about code, but about their practical applications and the value they bring to others. I have a profound aversion to investing my time and skills in projects that do not contribute positively to society. Instead, my commitment is to craft innovative solutions that are helpful, accessible, and transformative for both my peers and educators.

My dedication stems from the conviction that every project I undertake should have a purpose beyond technical proficiency. It is not merely about coding; it is about creating solutions that matter. I am motivated by the prospect of making a difference, whether it is in the classroom, the learning experiences of my fellow students, or the educational landscape of my institution.

I strongly believe in the power of education and technology to drive positive change. By dedicating my efforts to projects that are genuinely helpful for my college and others, I aim to create an impact that resonates far beyond the confines of a computer screen. Each project I undertake is a testament to my commitment to meaningful innovation, and my dedication serves as a guiding principle in my journey as a developer and a lifelong learner.

Portfolio

REFERENCES

1. "Web Application Security: Exploiting and Securing Modern Applications" by Andrew Hoffman, John Viega, and John W. Viega.
2. "The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski.

Websites:

1. "PHP Security Consortium" - https://phpsec.org/
2. "Open Web Application Security Project (OWASP)" - https://owasp.org/
3. "PHP: The Right Way" - https://phptherightway.com/
4. "PHP: The Good Parts" - https://eev.ee/blog/2003/php-the-right-way/

Blogs:

1. "PHP Adventures" - https://stitch.com/series/php-adventures
2. "Secjuice" - https://secjuice.com/
3. "Websec" - https://websec.io/
4. "PHP Security" - https://phpsecurity.readthedocs.org/

APPLICATIONS

.

1. Web Application Security Testing: Your project can be used to identify and exploit vulnerabilities in web applications that use PHP shells. This can help security professionals and developers to improve the security of their web applications and protect them from potential attacks.
2. Bug Bounty Hunting: Your project can be used to identify and report vulnerabilities in web applications that use PHP shells. This can help companies to identify and fix security vulnerabilities in their web applications, while also providing you with an opportunity to earn money through bug bounty programs.
3. Penetration Testing: Your project can be used to simulate real-world attacks on web applications that use PHP shells. This can help companies to identify and fix security vulnerabilities in their web applications before they are exploited by attackers.
4. Security Awareness Training: Your project can be used to raise awareness about the potential risks and vulnerabilities associated with PHP shells. This can help companies to educate their employees about web security best practices and reduce the risk of security breaches.
5. Security Research: Your project can be used to contribute to the field of web security research. By identifying and exploiting vulnerabilities in PHP shells, you can help to advance the state of the art in web security and contribute to the development of new security tools and techniques.

CONCLUSION

In conclusion, project on demonstrating the security threat for the PHP shell on a server has provided you with a comprehensive understanding of PHP shells and their potential security threats. By identifying and exploiting various security threats associated with PHP shells, such as command injection, Remote Code Execution (RCE), Cross-Site Scripting (XSS), Information Disclosure, and File Inclusion/Upload, and discussing various mitigation strategies to secure PHP shells and protect web applications and servers from potential attacks, you have gained valuable knowledge and skills in web security.

The potential applications of your project are numerous, including web application security testing, bug bounty hunting, penetration testing, security awareness training, and security research. By using the knowledge and skills gained from your project, you can help to improve the security of web applications and protect them from potential attacks.

Overall, your project has been a valuable learning experience that has equipped you with the necessary knowledge and skills to identify, exploit, and mitigate security threats associated with PHP shells. This will enable you to contribute to a more secure web environment in your future career as a web developer, system administrator, or security professional.