APPLICATION SECURITY TESTING AT MOVEINSYNC

Priyanka Mehta
E18CSE134
Team Head at Moveinsync: Vatsalya Singh

INTRODUCTION

- As an Application Security Intern at MoveInSync, I worked for three months. Throughout my time at work, I gained experience in a variety of areas, including API testing, web application testing, and mobile application testing.
- I also gained knowledge with professional tools such as Burp Suite Pro, Postman, GenY Motion, and Android Emulator, among many others. Because the company's security team was new, I was mostly in charge of the job, and as a result, I learned how to multitask, manage time, accept responsibility, and so on in the workplace.

ABOUT MY WORK

- Vulnerability Assessment and (Grey Box) Penetration Testing of Web Applications, APIs and Mobile Applications (Android) were my responsibilities at MoveInSync.
- I used a step-by-step approach to testing, first walking through the application to understand the flow, and then checking for all of the security concerns specified in the OWASP Top 10 criteria.

METHODOLOGY

1. Walkthrough of the application.
2. Understanding the application flow
3. Check for the issues listed in OWASP top 10 (in order)

- Injection
- Broken authentication
- Sensitive data exposure
- XML external entities (XXE)
- Broken access control
- Security misconfigurations
- Cross site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

LEARNINGS

- WEB APPLICATION SECURITY TESTING
- MOBILE APPLICATION SECURITY TESTING
- API SECURITY TESTING
- VARIOUS TOOLS AND BROSWER EXTENSIONS

METHODOLOGY

1. Install XAMPP
2. Download the phpList folder from github
3. Copt the lists folder present in phpList to the htdocs folder inside the xampp folder.
4. Start the apache and mysql service through xampp.
5. Create a local mysql database.
6. Change the config_extended file to config and config file to config_old.
7. Open the config.php file and make sure all the details regarding the databse are correct, if not make the changes and save.
8. Go through the file and look for the place where smtp configurations are being done and modify the configuration file in order to configure the email settings of phpList.
9. Access the file through localhost and go th the admin directory and initialize the database.
10. Read to go!

LEARNINGS

- CREATION OF WEB SHELLS: HOW TO CREATE WEB SHELL THAT HAVE A WIDE VARIETY OF CAPABILITIES AND IS ALSO UNDETECTABLE.
- HOW TO MAKE A WEB SHELL UNDETECTABLE: CODE OBFUSCATION, USE OF SHELLSHOCK, ENCRYPTION,
- HOW TO INCORPORATE FILE MANAGER INTO A WEB SHELL.
- HOW TO CREATE BULK MAILER USING PHP.
- PHPLIST: PHPLIST IS AN OPEN-SOURCE MAILING LIST MANAGEMENT PROGRAM. IT IS INTENDED FOR THE DISTRIBUTION OF INFORMATION TO A GROUP OF RECIPIENTS, SUCH AS NEWSLETTERS, NEWS, AND ADVERTISEMENTS. IT'S WRITTEN IN PHP, AND THE DATA IS STORED IN A MYSQL DATABASE.
- HOW TO AVOID THE EMAILS FROM LANDING INTO SPAM.

BENNETT UNIVERSITY
THE TIMES GROUP

INTRODUCTION

- It has been 2 weeks since the starting of my internship at DRDO.
- In these two weeks I was a part of one project which was related to Bulk Mailing. I have learnt about various things like phpList, local hosting, web development using php.
- I also got to learn to create web shells that includes all possible capabilities and stealth techniques.

ABOUT MY WORK

- At DRDO there are various projects one can choose to be a part of. I chose to be a part of the web shell development project and bulk mailing project.
- In the web shell project, we developed various web shells as per recent security standards.
- For the bulk mailing project, we used the phpList and made modifications according to requirements.

APPLICATION SECURITY TESTING AT DRDO

Priyanka Mehta
E18CSE134
Department Head at DRDO: Mr. Kaustubh