Investigation of WordPress Security

By Maximum Effort, Maximum Efficiency:
Daniel Harper, Jack Gates and Matthew Stirling

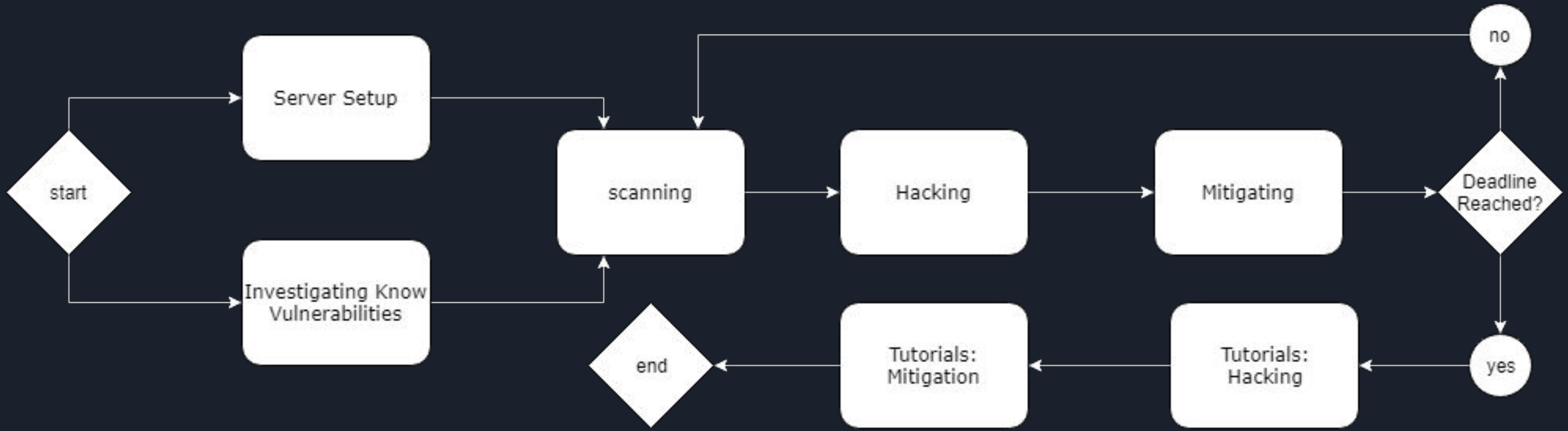
Project Background

- WordPress is the #1 CMS and is responsible for 28.9% of sites on the internet
- Such widespread use means its a likely target for malicious users
- The aim of this project is to identify weaknesses within the WordPress system and its plugins as well as to mitigate them appropriately, where possible
- Aim was to target popular, yet vulnerable plugins that typical users may use.

The Investigation

- The aim of this project was to launch an investigation into vulnerabilities surrounding the CMS - WordPress
- These vulnerabilities would then be analysed further, in terms of how they work and how they can be mitigated.
- Three documents will be created to present the results: a tutorial on how to perform attacks against these vulnerabilities; a tutorial on how to prevent these vulnerabilities and a whitepaper to bring it all together.
- Last semester a plan was originally created for the team to follow

Methodology



Mentally, this can be split up into three stages; the setup stage, the testing stage, and the documentation stage.

Methodology: Setup Stage

Server setup

- To set up the working environment that the client would be familiar with, the team had to:
    1. Set up a Web server that would host the CMS
    2. Create a MySQL Database
    3. Set up PHP 7.0
    4. Install WordPress, specifically 4.9.0
    5. Install of the plugins being tested
- After the environment was set up, the website was branched into two sections: an Ecommerce site, and a Blog site.
- This was done as it aided in splitting the workload as well as being able to isolate tutorials to satisfy client needs

Investigating known vulnerabilities

- The research for vulnerabilities was done online
- Much of the research aided in the decision on what vulnerabilities to test for
- Wordpress Vulnerability databases were found ,these were then consulted when deciding what vulnerabilities to test

Methodology: Assigning Workloads

During the testing stage; the work was split up amongst the three team members. Two different types of WordPress sites were decided, which were set up with plugins that related to their respective purpose. The two chosen site types were:

- An e-commerce site
- A blog site

A group member was allocated to each site, and the third worked on vulnerabilities affecting the core of WordPress.

Methodology: Testing Stage

The three tasks in this stage were:

1. Scanning: Searching for and analyzing plugins
2. Hacking: Performing the exploits to ensure the vulnerability is present, so it can be documented.
3. Mitigating: Ensuring the vulnerability is fixed and cannot be exploited.

Once these tasks were completed for a given vulnerability, they were repeated for the next until the deadline we had given ourselves was reached.

Methodology: Documentation

Two tutorials were to be completed for this investigation, they are:

- A vulnerabilities Tutorial
- A Mitigations Tutorial

The steps required to test whether a vulnerability existed were placed into the vulnerabilities tutorial.

The steps required to mitigate the vulnerability were placed into the mitigations tutorial.

These are the finished products of the investigation.

Results

What was found:

- 11 vulnerabilities affecting WordPress and its plugins were found during this investigation. These were all documented in the form of a tutorial.
- For each of these vulnerabilities; a mitigation was presented, applied and documented.

The found vulnerabilities ranged in severity, from Information disclosure to script injections. The number and variety of the plugins found gives a good insight into the security surrounding WordPress.

Results: Agreement Met

As stated in our quality assurance section that was outlined in the plan that the project's success was to be based on three variables:

- The number of vulnerabilities the team find throughout this project
- The perceived severity of these vulnerabilities
- The number of fixes that the team find for the vulnerabilities investigated

Through evaluating these attributes it is clear that the team has met their goal.

Team Limitations

Although the requirements were met and the quality of the investigation was of a decent standard, there are still limitations to the work that was performed.

- The plugin vulnerabilities were focussed on only two variations of a site. This means that if the client used a different type of site to the two investigated, the plugins may not be relevant to them.
- There are 55 thousand plugins available, to test them all would be futile. Although, the papers produced at least give knowledge to the user on how they could begin testing other plugins they may use.

Conclusion

A detailed methodology was provided. Any detail that was relevant at any point of testing was included.

Tutorials were detailed and they contained a diverse range of vulnerabilities

The team managed to meet the requirements outlined in the client agreement. The project was delivered on time and included all the deliverables outlined in the agreement.

Conclusion: Reflection

Overall the communication was good between team members, communicated daily to provide updates on work.

Team members also consulted between each other when assistance was required.

The plan was followed, however at points the extra time outline in the plan was used.

By and large there seemed to be fewer vulnerable e-commerce plugins present in WordPress, due to their nature. This lead to a case where there was an uneven workloads

Conclusion: Future Work

If more resources were given, mainly time the team could potentially make the following improvements to the investigation:

- Investigate a wider range of plugins
- Launch an investigation into other popular CMS’s and compare their security to WordPress
- Improvements on the tutorial layout in the form of video walkthroughs

Questions?