PROJECT PROPOSAL

GOOGLE SUMMER OF CODE 2022

OWASP FOUNDATION ModSecurity Core Rule Set - Machine Learning Plugin Integration

- Deepshikha Sinha

TABLE OF CONTENTS

About Me:

- ★ **Name:** Deepshikha Sinha
- ★ **University:** Indian Institute of Technology (BHU), Varanasi
- ★ **Year:** 1st year
- ★ **Degree:** Bachelor of Technology (BTech)
- ★ **Email:** deepshikha.sinha.che21@itbhu.ac.in
  i.deepshikha.sinha@gmail.com
- ★ **Github:** deepshikha-s
- ★ **Linkedin:** Deepshikha Sinha
- ★ **Phone:** +91 8762132716
- ★ **Address:** HAL 2nd Stage, Bangalore, Karnataka, India
- ★ **Time Zone:** IST (UTC +5:30)
- ★ **Skills:** Python, Javascript, Content Writing
- ★ **Languages:** English, Hindi (fluent and comfortable in both languages)

I am Deepshikha Sinha, a first year undergraduate student, currently doing my BTech at IIT (BHU), Varanasi.
The idea of open-source projects has fascinated me for quite some time now. I'm drawn towards open source by the fact that I will get to contribute to projects which are solving real-life problems and work with expert experienced people. Open-source communities are very welcoming and provide me with a very good environment to expand my skill set and to contribute to projects which are developed for the good of the community. Ever since I attended the first workshop on open-source projects, I have actively been on the lookout for opportunities to contribute and interact with people. Google Summer of Code would be an excellent opportunity for me to apply my current skills to contribute to projects and expand my skill set. The best part is not only do I get to learn a lot and interact with new people, I get to collaborate on projects which have a global impact.
I have developed an interest in machine learning and artificial intelligence. I'm currently exploring its wide applications and I'm looking to dive deeper

into it. I am also a cyber security enthusiast and I have been reading about the latest cyber vulnerabilities and means to counter them which regularly come up.
I have significant experience in Python and Javascript.I have been using Git and Github for quite some time now. Although my primary interest lies in machine learning, I'm also interested in software development.

Why me?

I believe that I am the right choice for this project due to the following reasons:

1. I have developed the right level of knowledge and skills to successfully complete this project. This would also be an excellent opportunity for me to apply my knowledge and hone my skills. This would also allow me to learn new things and develop new skills. Working under the guidance of and along with experts and active contributors will be an opportunity for me to learn a lot of new things which cannot be taught in any course.

2. I have chosen to apply to this project because this is where my interests lie. I am deeply interested in machine learning and I feel very strongly about cyber security. I believe with the increased use of technology in our daily lives, it is important to be aware of the associated threats that arise and find ways to counter those threats. Modsecurity along with the OWASP Core Rule Set helps in protecting web applications from cyber attacks by blocking malicious requests. When integrated with machine learning, the performance of the firewall will only improve. The opportunity to contribute to a project where I can pursue my interests and work for a cause I feel very strongly about is the best opportunity I could have asked for.

3. The OWASP CRS community is a really nice community. For a first year undergraduate student, the thought about interacting with such experienced people could be intimidating at first. However,this was

not the case for me due to the community. The OWASP community has been very welcoming and I never felt hesitant to ask any questions. The mentors are very supportive and always respond promptly. Their guidance for this proposal has been very helpful and insightful for me. For the short duration in which I have been associated with this community, I have really enjoyed the way the community works and I would definitely want to be a part of the community and further contribute to the projects after the completion of this project.

Familiarity With the Required Software:

I am quite familiar with the software required for the project. I have set it up on my pc (Linux version 18) and have been using it since late February. I'm currently using OWASP CRS v3.3 with Modsecurity 2.9.3. I have gone through the documentation very thoroughly and have tried to experiment by changing several settings.

Prior Coding Experience:

I have been working with python for the past 4 years. I learnt python on my own when I started grade 10 and had formal training in it in grades 11 and 12 as it was part of my course. I have also done a project using python and pygame for grade 12. The code for my project is available on github. I have also taken part in PES Codewars when I was in grade 12. Along with my teammates, we made it to the finals.
As a part of my college course, I am taking up a course on C++ this semester.
I have also worked a bit with Javascript

For this project, I have learnt Lua scripting too. Since the beginning of March, when I decided that I would like to work on this project, I have spent time everyday learning it and I'm currently making good progress.
My other projects can be found on my Github handle.
I have a dual boot pc with windows 10 and Linux version18 installed. I have been using the python IDLE, PyCharm, VS Code for python. I have also used Intellij Idea and Android Studio for other development. Although I have been using these, I am flexible with software to use and I can switch over to whichever software the organization and project requires me to. I will be able to switch over very easily as I am usually very quick to grasp new software.

Availability and Commitments:

I do not have any other commitments this summer (May 2022 - September 2022). I do not plan on taking up any internships or other activities this summer as I want to keep myself available for this project. During this time, I will devote a minimum of 25 hrs per week or more depending on the project requirements to work on this project.
I am available the entire day on weekends and plan to spend at least 6-7 hrs per day over the weekends and holidays and 2-3 hrs per day on the remaining days. I also plan to keep a 1 day buffer every week to make sure the deadlines are met despite unforeseen issues like runtime errors which take time to solve. I will keep the rest of the time available for discussions with the mentors and the community. I'm flexible with timings and can work with significant overlapping time zones between India, Europe and USA in this project. I will keep the mentors and community updated on my progress. I will inform them about my progress on a weekly basis and update my work on Github on a daily basis. I can alter the frequency depending on the mentors' preference.
Due to the COVID-19 situation, our college is currently online and we haven't been called on campus yet. If we are called back on campus during this period, I would not be able to put in a lot of time for a day or two as I would have to travel and get settled in college. I will make up for these two

days either by completing the task beforehand or by spending 2-4hrs extra the next day. As of now, we have no intimation as to when we would be called on campus. I will keep the mentors informed about this.
In addition, I will be having my college exams from July 6 - 12 and hence I would be able to denote 10-15 hrs that week. I will compensate for the remaining 10-15 hrs by working 5 hrs extra for 2-3 weeks. I assure you that this will not affect the time I'm willing to devote for my project.

Preferred Working Method:

I am comfortable working under a mentor remotely. For the past two years, all our classes have been online and I have been working under the guidance of my teachers remotely. As mentioned above, I would be uploading my work on a daily basis and giving my mentors a progress report weekly or at a frequency preferred by the mentors.
I am very comfortable with English and I can definitely work closely with a supervisor whose native language is English.

Past Contributions:

I have started exploring open source very recently and I have made the following contributions to this project:

- Pull Requests
- Issues raised

Pre-GSoC:

I will get a time of 1 month between the time of submission of this proposal and the community bonding period. I will be using this time to complete any left out groundwork (if any) which is necessary for this project.
As mentioned above, I have been learning Lua but I haven't yet implemented any project in that. I would like to do this over this month.

I would like to implement a few machine learning algorithms to increase my first hand experience with machine learning.
I would also spend time testing the crs more extensively and contribute to the codebase.

Synopsis

With the increase in use of technology and the internet, the risks associated with the internet are also increasing at a very high rate. Hence, it is necessary to have a system in place to protect our systems from such risks. The risk of malicious attacks is especially higher when browsing the internet. Thus, there is a need for an external system to intervene and block any unauthorized requests to the web server. A web application firewall(WAF) does just that. Modsecurity follows the OWASP Core Rule Set(CRS) rules to detect any vulnerabilities. This helps make web browsing more secure. The CRS has different Paranoia Levels which represent different security levels. At higher paranoia levels, the system has a stricter set of rules to block malicious activities. However, at such high paranoia levels, many genuine requests also get blocked as they resemble malicious activities. These are known as false positives. Such a large number of false positive detections hinders the user experience and as a result, they may stop using CRS and compromise security. Hence, it is important to reduce the number of false positive detections. As the data isn't labeled, using an appropriate unsupervised learning algorithm is the best possible way to achieve this. With the existing proposal by Floriane Gilliéron as a basis, I would work on an unsupervised learning algorithm for the machine learning plugin and aim to get it integrated as an official plugin. I will also add additional features to the plugin.

Objective:

➔ Write a new Machine Learning framework for CRS (Core Rule Set)
➔ Develop a machine learning plugin with performance improvements

➔ Integrate the machine learning plugin and get it registered as an official plugin.
➔ Write documentation of the plugin for the benefit of students as well as the community.

Deliverables:

1. **Plugin Integration:**

   I will implement an ML algorithm in the form of a plugin which follows the general plugin architecture for the CRS. Currently, the machine learning rule gets triggered only when the anomaly score generated by the CRS crosses a threshold value. I will generalise this so that the ml rule gets triggered for all requests irrespective of whether it is suspicious or not. This will help in the reduction of false positives and false negatives.

2. **ML Plugin Development:**

   Once a functional ML plugin for reduction of false positives is ready, I will work on adding an ML algorithm which will detect whether a particular request is an attack or not. This will act as a reference for further machine learning research.

3. **Documentation:**

   I will write documentation for the features I add on a regular basis. Every week, I will write the documentation of the work done over that week before I submit my weekly report to the mentors. This will ensure that all the features of the plugin are documented and nothing is missed.

Approach:

I will create a new repository to keep all the files for the machine learning plugin.
The repository will contain the following files:

- ➔ machinelearning-before.conf
- ➔ machinelearning-after.conf
- ➔ machinelearning-config.conf
- ➔ <machine learning scripts>
- ➔ mainscript.py

The project will be done in two phases:

- ➔ Phase 1: Integrating a machine learning plugin
- ➔ Phase 2: Adding ML Algorithm for Detection of Cyber Attacks

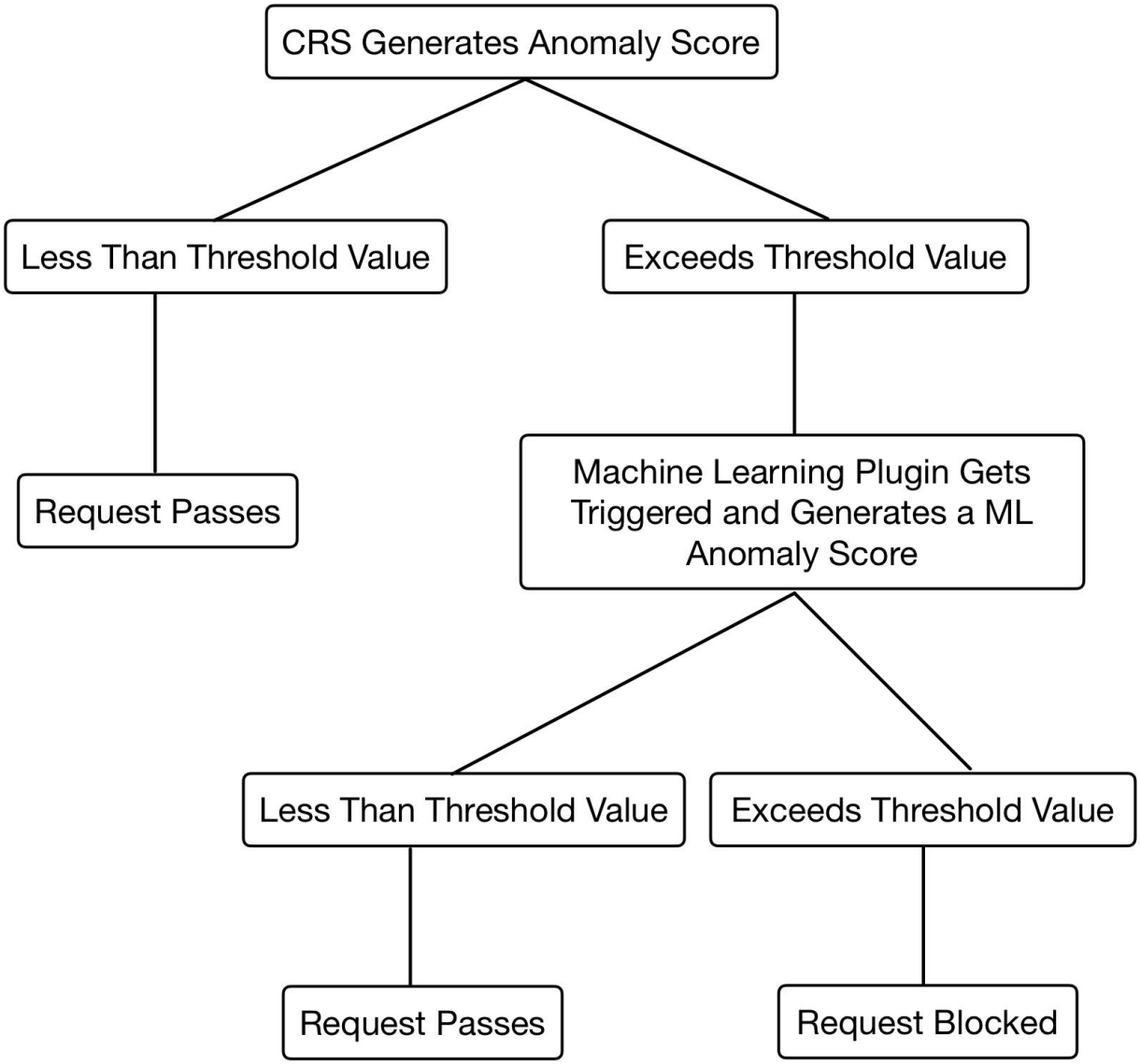
Phase 1:

The file machinelearning-config.conf will be used to configure the machine learning plugin. The machine learning plugin will have a default configuration for the detection of false positives. Once the plugin is configured with this setting, the CRS and the machine learning algorithms will generate anomaly scores. If both the anomaly scores cross the threshold value, then the request will be blocked. The implementation will be as follows:

1. After the plugin configuration, the CRS will generate an anomaly score as per the existing CRS rules.
2. If this value exceeds the threshold value, the ML algorithm gets triggered.
3. Once triggered, the ML algorithm will generate an anomaly score.
4. Based on this score, the request will be either blocked or allowed to go through.

The machine learning rule will be called in the machinelearning-after.conf file through a script.
The Machine Learning algorithm used here will be similar to the one used in the existing proposal. Unsupervised learning techniques will be used to train the algorithm as the data set is not a labeled dataset. In particular, the

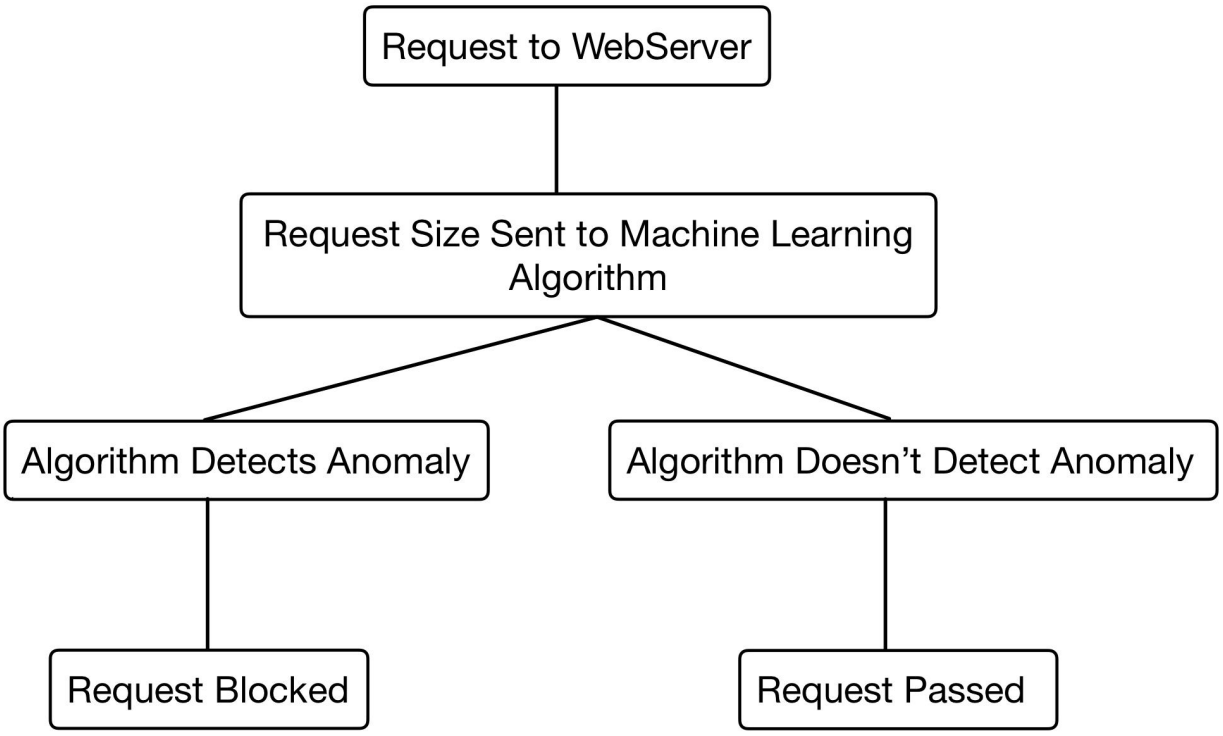
isolation tree method will be used. While usual learning algorithms would look for ‘normal’ data points and learn from that, the isolation forest method works differently. Instead of looking for the normal data points, it looks for the anomalies in the dataset as these are much easier to find. It does so by recursively partitioning the data into smaller clusters based on certain attributes. The points which need the smallest number of partitions to be isolated are the anomalies. This algorithm will also generate an anomaly score according to the formula. This anomaly score will be used to decide whether the request should be blocked or not.


CRS Generates Anomaly Score
Less Than Threshold Value
Exceeds Threshold Value
Request Passes
Machine Learning Plugin Gets Triggered and Generates a ML Anomaly Score
Less Than Threshold Value
Exceeds Threshold Value
Request Passes
Request Blocked

Phase 2:

Once the functional plugin is ready, I will work to develop an ML algorithm which would help detect whether a particular request is an attack or not. To do this, the algorithm will look at the size of the request. Whenever a request is made to the server, the algorithm will look at the size of the server. Using the size of the requests, the algorithm will determine whether the request is an attack or not. This will also use the isolation forest method to detect the anomalies (requests which could possibly be attacks) based on request size. Since the requests which could be attacks can be detected using various criteria, request size being one of the criteria, this algorithm could be used as a base for similar algorithms for other criteria.
The implementation will be as follows:

1. Once the plugin is configured with this setting, as soon as a request is made, the lua script will first extract the necessary data and feed it into the algorithm.
2. Based on the data received, the program will check whether the request is an anomaly or not.
3. If the algorithm marks it as an anomaly, the plugin will trigger the CRS blocking rule to block the request.


Request to WebServer
Request Size Sent to Machine Learning Algorithm
Algorithm Detects Anomaly
Algorithm Doesn’t Detect Anomaly
Request Blocked
Request Passed

Timeline:

I intend to follow the following timeline:

Time	Target
Proposal Evaluation Period [evaluation by organisation] (April 19 - May 19)	● Get existing prs merged ● Resolve issues and bugs (if any) ● Continue contributing to the project. ● Keep learning and dive deeper into the codebase ● Explore alternative approaches to the project ● Stay connected with the community
Community Bonding Period (May 20 - June 12)	● Interact with the community ● Interact with the mentors, discuss the proposal and implement their suggestions ● Try to look for more ways to enhance the ml algorithm ● Learn more about the structure and workflow of the repositories. ● Decide and finalize approaches to the chosen ideas.
Week 1 (June 13 - June 19)	● Work on completing the Isolation Forest algorithm for false positive detection
Week 2 (June 20 - June 26)	● Connect the machine learning algorithm with the CRS and make it functional

Week 3 (June 27 - July 3)	• Merge the algorithm with the CRS as a plugin and get the plugin officially registered.
Week 4 (July 4 - July 10)	• Work on extracting the size of the request from the request sent to the web server
Week 5 (July 11 - July 17)	• Write the machine learning algorithm to detect the anomalies in the requests sent to the web server.
Week 6 (July 18 - July 24)	• Complete the machine learning algorithm
Evaluation Period 1 (July 24 - July 29)	• Submission of project status report for initial evaluation • Review documentation for false positive detection
Week 7 (July 30 - August 5)	• Connect the algorithm to the CRS and test on actual requests.
Week 8 (August 6 - August 12)	• Tuning the algorithm to get the anomaly scores
Week 9 (August 13 - August 19)	• Minor adjustments to add the algorithm to the plugin.
Week 10 (August 20 - August 26)	• Testing to generate data and train the algorithms to enhance its accuracy and efficiency
Week 11 (August 27 - September 4)	• Additional time for fixing bugs and other minor issues (if any)
Final Submission Period (September 5 - September 12)	• Final round of testing • Review documentation • Submit final work and work report

Expected Results:

By the end of the project the following would be done:

1. The machine learning plugin would be integrated to the CRS as a plugin and it would run parallel to the CRS.
2. Apart from the reduction in false positives, the plugin would also have an additional detection rule.
3. The plugin would also be able to detect malicious payloads.

Post GSoC:

By the end of the project, I hope to be a part of the OWASP community. After the completion of Google Summer of Code 2022, I would be more than happy to make regular contributions to the CRS and other OWASP projects. I want to dive deeper into the field of cyber security. Further, I would love to take part in more meetings and interact with the community. While being associated with OWASP, I have learned a lot of things in a very short duration of time. I'm really thankful to the community who have been very helpful and played an integral role in my growth.

References and Acknowledgements:

Acknowledgements:

I would like to thank Mr. Felipe Zipitria and Mr. Christian Folini for their guidance and support for this project. They actively answered all my questions and provided valuable feedback on my proposal.
I would also like to thank the OWASP community for their help and support.

References:

- ➔ https://github.com/coreruleset/coreruleset/pull/2067
- ➔ https://coreruleset.org/20210519/a-new-attempt-to-combine-the-crs-with-machine-learning/