SOP: Automated CI/CD pipeline security testing framework for self-configuration and expanding. Test every build with the same accuracy as the last one and expand on your tests with every iteration.

Introduction

We want to solve the problem of automating pentesting while also relieving the cost strain and the complexity. Outsource your security testing now and sleep better knowing you are secured by a team of professionals on every single build without having to pay the cost of a full test but rather, the cost of electricity it costs your servers to run (which you usually already have in the form of a dev pipeline) and the initial set up costs.

What do you get?

You get the full code and it is open source to you but of course also offer the possibility to push security and feature updates which you can subscribe to separately as a package deal or even just take 1 specific update you'd like. We will also be providing you with a standard list of payloads plus tests that tailor to your company, all included in the initial setup fee.

The updates to these lists can also be subscribed to separately, in case you just want to use the software and tests we made internally without worrying too much about new feature or security updates since you might only be running our software internally.

We can even train your staff on how to easily create new test case in a simple txt file. All they do is add the attack vector and the expected status code of the response + part of the text that is unique to the page we are expecting. (For example
"Wesley" – "200" – "Welcome Wesley"

Will test if we can enter the text Wesley and get a response with status code 200, with the text "Welcome Wesley" on the page.

A last feature we have is that you can name your test cases for a prettier and easier to understand test report. Please make 1 file per test (per thing you want to test) that contains the attack vectors like mentioned before. Name it the way you want your test cases to be named in the report.

Your reports will by default come in HTML, and MD form:

Test	Status
Assert the the exclude list is not empty	OK
Assert the the include list is not empty	OK
Assert the the repo list is not empty	OK
All the items in the include list should be in the repo list	OK

Extra services

But wait there is even more, we can custom tailer these checks to what you company needs for small extra fee such as:

- Add better reporting options, Standard reporting in the console and in an HTML file are included.
- Add more checks to the module, for example, add the possibility to check screenshots of a website and see if they compare to what we get. You then tell the location of the screenshot and the framework will do the rest for you
- Added cucumber functionality if you'd like to expand on the test itself

- A ghost browser to confirm exploits such as XSS with a true PoC and even screenshot
- Web testing with selenium. Please be aware though, this can be a big extra cost and needs to warrant the ROI since most can be with API testing for moderately big companies
- We can implement our framework in your company after signing of an NDA or you can install it yourself fully in conjunction with a professional senior team member of The XSS Rat.
- Endpoint processing, where you enter the endpoint + it's checks + it's test data into an XML file and use that instead of the limited TXT file. The TXT file can not add their own endpoints seeing the complexity of the task for now, but might get that future added later on. Adding endpoints by a senior of The XSS Rat is usually a short endeavor as we properly document the procedure to do so to limit the time it takes to add 1 endpoint. Usually 1 hour suffices but there are no guarantees, it all depends on the request method, complexity of the request and parameters.
- Everyone can fully adept the script as it becomes their right to use after purchasing for a one time fee, updates can be bought and new versions will not come free as we will not make new version for a small feature. We will also push free features where possible. But the core MVP needs to be met and then everyone can pick their own required modules with the help of an account manager/senior at The XSS Rat.

What comes in the box?

- Automated command injection testing
- Automated SQL injection testing
- Automated NoSQL injection testing
- Automated Mass assignment testing (Being able to change parameter should no be able to change.
- A module to make the requests (python file)
- A module per endpoint (python file)
- An example of how to call the tests per endpoint within that file
- We use the unit test framework
- You will get an HTML report and a MarkDown report
- You will get a full pentesting report, written by a senior, containing

o Per issue found

§ Title + severity

§ Description

§ Pre-requisites

§ Steps to reproduce

§ Actual result

§ Expected result

§ Impact

§ Steps we performed to clean up our exploit after testing

§ OPTIONAL: Remediation steps

§ OPTIONAL: Ways to retain access

o OWASP top 10 Compliance (fail/pass per item based on issues found)

o SANS CWE top 25 compliance if applicable

o General advice for the company

o Comparison of metrics up to 3 previous reports (See trends in your security before it hits production) with potential to grab more historical storage for a small fee. This is 10 Previous reports for people who the full updates + features packages and we include a detailed analysis per first report, quarterly report after that and/or big release)

o A conclusion written by a senior after analyzing your results if you have a subscription package, any which one includes this. For a small fee this can also be grabbed on hourly basis with a minimum of 15 minutes at a rate of 125$/h. This will be done by a senior, always, though a medior /junior might follow along after signing the proper NDAs to learn. Only 1 person's hours are billable at a time of course so you will never be billed for us training someone on these reports.

o You get a Senior and a Junior or medior at least who will work with you and the teamlead/project manager on our side to get things fit for your needs and implemented in your workflow. We are all for custom work as no 2 companies are the same but we've found a formula for automating the most boring and repetitive tasks which will often cost the most money.

So what about the price?

Everything here is based on the MAXIMUM SIZE COMPANY AND ASSIGNMENT/SCOPE. THIS IS THE MOST EXTREME CASE OF OUR PRICELIST. PLEASE REQUEST A FREE MEETING AT info@thexssrat.com AND INCLUDE brandon@thexssrat.com. We will help you with a custom quote, usually the same day even because we work in different timezones and can cover a big portion of the world in terms of time.

Please note, we can employ testers from all over the world quickly so we can also scale up quickly. It's better to slow low and slow, use it for a while and see what extra's you need than it is to start going 200% all in from the start since we do offer all this in module form, and you should take advantage of that modularity. It will help you create a better fit solution for your needs. It's much easier to add a module than to remove one that might have been integrated for a while and we do not want to waste your money on tests we do not think you will get value from.

- Basic set up for a Jenkins pipeline

o About 2 weeks work: $ 16 000

o Includes setting up script, adepting to your endpoints + setting up reporting

o Includes small training for your staff for up to 12 people on how to use the technology - 1h

o Includes documentation on how to use

o Includes 4 types of attackers per endpoint. You can define your own endpoints and parameters in a CSV file. We will do an initial set-up to ensure everything works.

o Includes 2 reports, in MD and HTML

- Full source of the framework at the moment in time with the latest version of the software
- You will always get free critical security patches. High, medium and low are optional and for you to install. We will only PUSH high impact security patches.
- A written-out checklist of all the things we would recommend starting with to test (based on impact, severity and occurrence rate)
- A helpdesk line where we offer 4 hours of free phone support per month for the non-subscriber packages and 10 hours of free phone support for package members. For customers that have bought everything, including all updates, they get a 15 hour phone or zoom meeting support.
- We can perform remote support on your server if you give us a user account with the correct rights. This can be done by of our staff in your downtime and is always planned in accordance with you.
- We expect to release 1 feature of small to medium size every month to increase the support we can offer for different technologies. Roadmap will come soon. These features do require payment, except for our QoL (Quality of Life) updates such removing x,y or z from a report to make it look better
- We expect to deliver 1 major release every 6 months that includes an engine rework which will make the previous version outdates. Still perfectly useable and supported at that point, but it might be missing a major feature like .net integration for which you can grab an expansion pack specifically or even skip entirely if you don't need it http://dot.net for example.
- We will keep supporting and updating your software back to a working state, should things brake due to our fault (Note this does NOT include changes in features, workflow or technology on the clients end) for at minimum 2 years. However we can not guarantee modified code will keep on functioning and might have to revert to our default code in case of catastrophic crash, so always make backups if you make changes yourself.
- The 3 oldest reports with history analysis per release

- EXPANSION: Fully train us in making things – 16 hours – 1500$/12 people max

- EXPANSION: Extra people, can also be with other expansions – x h = 125$/person/training day of 8h

- EXPANSION: Reporting – 24h extra – Grab a fully, custom written and comprehensive report that comes with coding so you can make adjustements in the source and generate new reports, your way! We will go through the initial design process with you and create that first custom report, so you know what to do. We will pair up with someone from your team for direct training on your side and Peer reviews that happen with a stakeholder from both sides. – 2000$

- EXPANSION: Add cucumber + Selenium for UI, End-to-End testing – Most critical functionality only – Is very flakey, if 1 identifier of an element on screen changes, we need new maintenance - +- Tripe the cost of the project and add 30% buffer. High level estimations can be acquired through Wesley or Brandon

- EXPANSION: Maintenance module – We can commit periodic maintenance, in which we check a couple of metrics to ensure our framework is still performing optimally and to see if we can make suggestions to improve speed for example. These metrics are –

1500$/mo :

o Speed per test case from first bit sent to last bit received – Custom local only monitoring

o Speed test per run from first bit sent to last bit received – Custom local only monitoring

o CPU usage of test cases if allowed by customer – Custom local only monitoring

o Memory usage of test cases if allowed by customer – Custom local only monitoring

o CPU usage of test runs if allowed by customer – Custom local only monitoring

o Memory usage of test runs if allowed by customer – Custom local only monitoring

o Queries duration if any are performed – Custom local only monitoring

o Counts of test cases, runs, and amount of crashes + crash information (Anonymous – sent on to our servers to help you better and improve the product – WILL NOT INCLUDE ANY PERSONAL DATA , ONLY AFTER YOU APPROVE IT, ERROR MESSAGES WILL NOT CONTAIN SENSITIVE DATA IF SENT OVER NETWORK. A full list of messages that are logged can be requested with Brandon or Wesley. We can also use this to report issues with any potential 3rd party software we might be using such as selenium.

o Crashes + detailed error messages for analyzing with an “The XSS Rat” Senior/Technician. DO NOT SEND THIS OVER THE NETWORK BUT INSTEAD, HAVE A PROFESIONAL GRAB THESE FILES WITH YOU AND ENSURE THEY LAND UP ON THE PROTECTED DRIVE OF THE COMPANY AND NEVER ON THE PERSONAL HDD/SDD OF ANYONE WORKING NO THE PROJECTS. THIS CONTAINS HIGHLY SENSITIVE DATA.

o In some cases, A technician on the end of The XSS Rat might be given access to the server and be able to view these logs without the customer. At this moment or at the moment the server goes down, an email is ALWAYS send to the customer’s contacts (can be a list) but make sure you realise we are not responsible for removing fired employees. You are to explicitly contact us to do this and this service is free.

- EXPANSION: Customize framework - ??? – Custom quote, we adept to your needs in full

- EXPANSION: Feature packs subscriptions, you get all the updates which will realistically be 10 a year, about one a month including the latest and greatest features. We release 1 feature at a time to production when we can to give you guys new features in a faster timeframe while being to maintain the quality of work. You can also add the Expansion packs subscriptions. (See next bullet point) - 1500$/year

- EXPANSION: Expansions pack, when we do a complete core overhaul of the functionality or develop our tool in an additional language such as add LUA support, you can grab this for a discount if you already own the product currently or subscribe the Expansions pack which includes the Features pack. (5000$/year)

- EXPANSION: Single update/upgrade, security updates will 150$ per bug they cover, non-security yet critical business logic patches will cost 100$ per included features and non-critical patches are 50$ each. For the Expansion packs it will be 500$ per upgrade if you own the software already and 8000$ if we have to totally reinstall everything instead of upgrade it for you. This full reinstallation usually has to happen when a few patches have been skipped. Especially patches pertaining to data as they will most often break with continued releases or scenario test cases.

- EXPANSION: Have you tests designed by one of our Senior hackers – Depending on the size of the project – 125$ up to 250$ per hour since this also includes test case design techniques and coaching of your staff

- EXPANSION: Verify a page with a screenshot, allow them to have a certain error margin and if not within that margin, fail tests. This is a very visual, very flaky kind of test. Often done to test documents that are auto generated by a web app or API.