SSTI

Server Side Template Injection

Challenges

How to prevent server-side template injection vulnerabilities

The best way to prevent server-side template injection is to not allow any users to modify or submit new templates.However, this is sometimes unavoidable due to business requirements.

One of the simplest ways to avoid introducing server-side template injection vulnerabilities is to always use a "logic-less" template engine, such as Mustache, unless absolutely necessary. Separating the logic from presentation as much as possible can greatly reduce your exposure to the most dangerous template-based attacks.

Another measure is to only execute users' code in a sandboxed environment where potentially dangerous modules and functions have been removed altogether. Unfortunately, sandboxing untrusted code is inherently difficult and prone to bypasses.

Finally, another complementary approach is to accept that arbitrary code execution is all but inevitable and apply your own sandboxing by deploying your template environment in a locked-down Docker container, for example.

Exploitation

https://portswigger.net/web-security/server-side-template-injection/exploiting#read-about-the-security-implications

Check this out
https://book.hacktricks.xyz/misc/basic-python/magic-methods
https://book.hacktricks.xyz/pentesting/pentesting-web/flask
https://pequalsnp-team.github.io/cheatsheet/flask-jinja2-ssti

Challenges
https://www.root-me.org/en/Challenges/Web-Server/Java-Server-side-Template-Injection

Solution:
Challenge Writeups:
http://dienpv-0pain.blogspot.com/2017/06/server-side-template-injection.html
https://hell38vn.wordpress.com/2019/07/11/root-mejava-server-side-template-injection-easy/

Writeups
https://medium.com/hackstreetboys/ritsec-ctf-2018-writeup-web-72a0e5aa01ad
https://medium.com/bugbountywriteup/x-mas-2019-ctf-write-up-mercenary-hat-factory-ssti-53e82d58829e
https://medium.com/server-side-template-injection/server-side-template-injection-faf88d0c7f34
https://hawkinsecurity.com/2017/12/13/rce-via-spring-engine-ssti/
https://www.betterhacker.com/2018/12/rce-in-hubspot-with-el-injection-in-hubl.html?spref=tw
https://0day.work/jinja2-template-injection-filter-bypasses/

https://medium.com/@david.valles/gaining-shell-using-server-side-template-injection-ssti-81e29bb8e0f9
https://owasp.org/www-pdf-archive/Owasp_SSTI_final.pdf
https://research.securitum.com/server-side-template-injection-on-the-example-of-pebble/
https://clement.notin.org/blog/2020/04/15/Server-Side-Template-Injection-(SSTI)-in-ASP.NET-Razor/
https://www.blackhat.com/docs/us-15/materials/us-15-Kettle-Server-Side-Template-Injection-RCE-For-The-Modern-Web-App-wp.pdf
https://gist.github.com/Yas3r/7006ec36ffb987cbfb98
https://ajinabraham.com/blog/server-side-template-injection-in-tornado
https://hell38vn.wordpress.com/2019/03/05/tamu-ctf2019-science-web/
https://subscription.packtpub.com/book/networking_and_servers/9781788626897/11/ch11lvl1sec78/ssti-in-the-wild

PayloadAllTheThings
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection