enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/time/nmap.txt 10.10.10.214
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-05 01:42 EDT
Nmap scan report for 10.10.10.214
Host is up (0.28s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 0f:7d:97:82:5f:04:2b:e0:0a:56:32:5d:14:56:82:d4 (RSA)
|   256 24:ea:53:49:d8:cb:9b:fc:d6:c4:26:ef:dd:34:c1:1e (ECDSA)
|_  256 fe:25:34:e4:3e:df:9f:ed:62:2a:a4:93:52:cc:cd:27 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Online JSON parser
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.51 seconds
```

going for complete port scan

no other ports are open

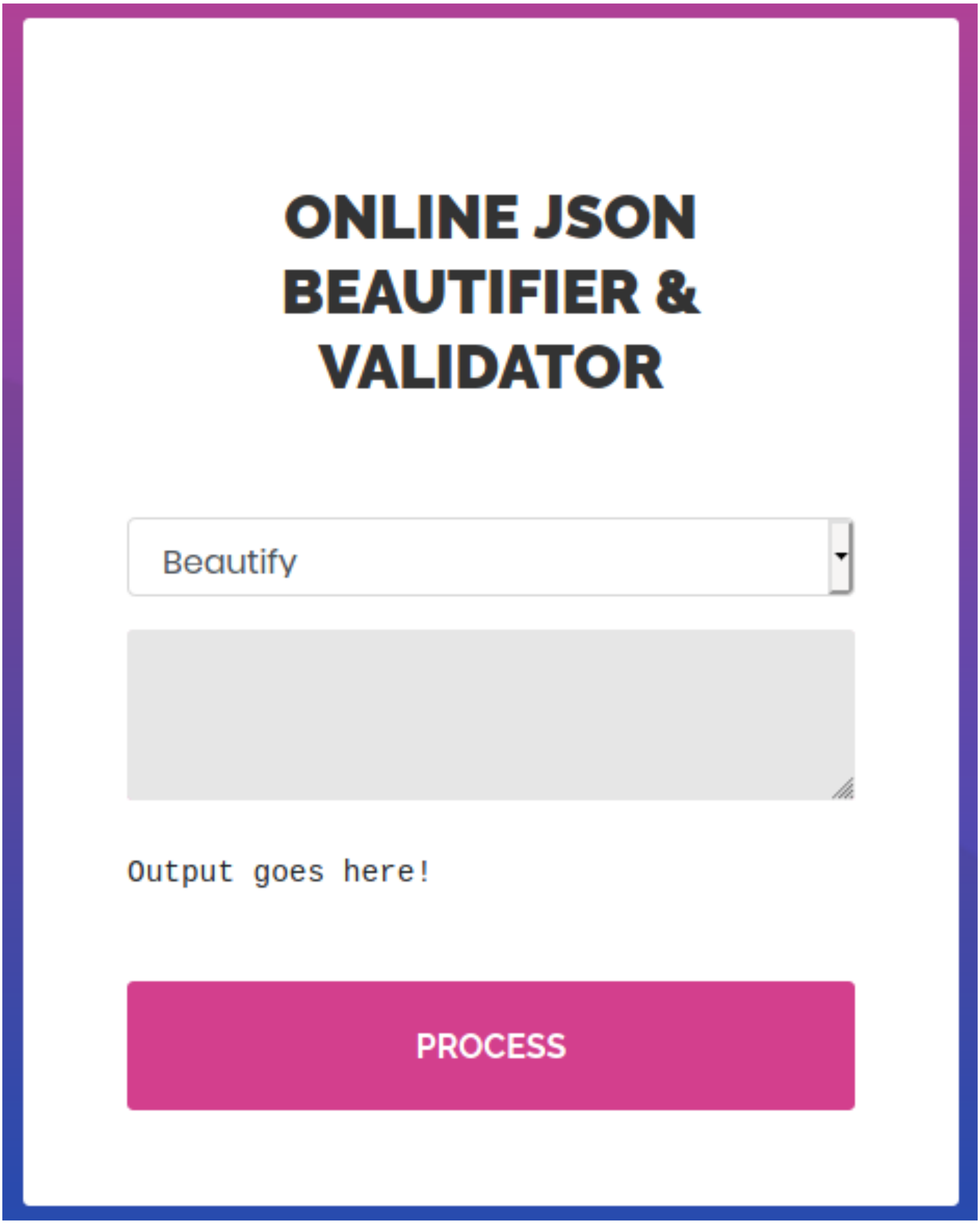
lets run the vuln script

we can see thet open ports are

```
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1
```

```
80/tcp open  http    Apache httpd 2.4.41
```

so everything seems fine with ssh lets see whats in port 80

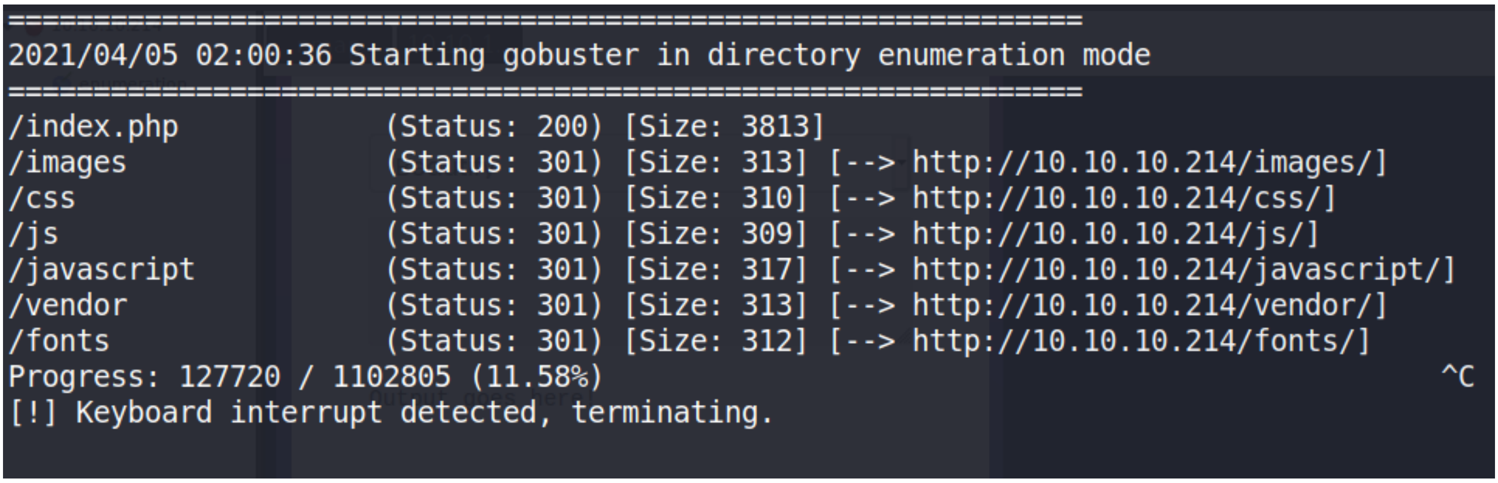


ONLINE JSON BEAUTIFIER & VALIDATOR

Output goes here!

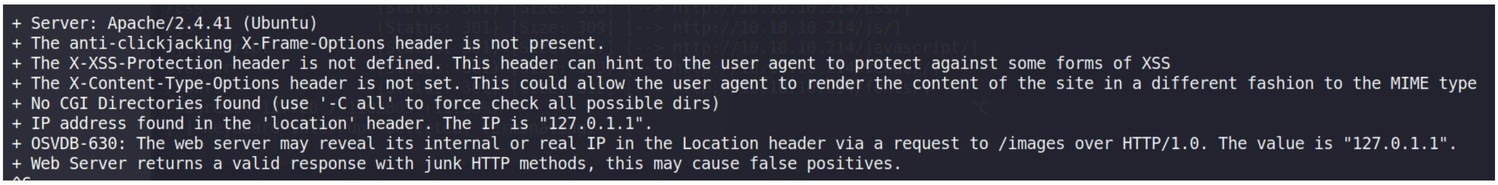
we see a online jason parser

and here we have gobuster result



```
===============================================================
2021/04/05 02:00:36 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 3813]
/images               (Status: 301) [Size: 313] [--> http://10.10.10.214/images/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.10.214/css/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.10.214/js/]
/javascript           (Status: 301) [Size: 317] [--> http://10.10.10.214/javascript/]
/vendor               (Status: 301) [Size: 313] [--> http://10.10.10.214/vendor/]
/fonts                (Status: 301) [Size: 312] [--> http://10.10.10.214/fonts/]
Progress: 127720 / 1102805 (11.58%)                                                ^C
[!] Keyboard interrupt detected, terminating.
```

and the nikto result

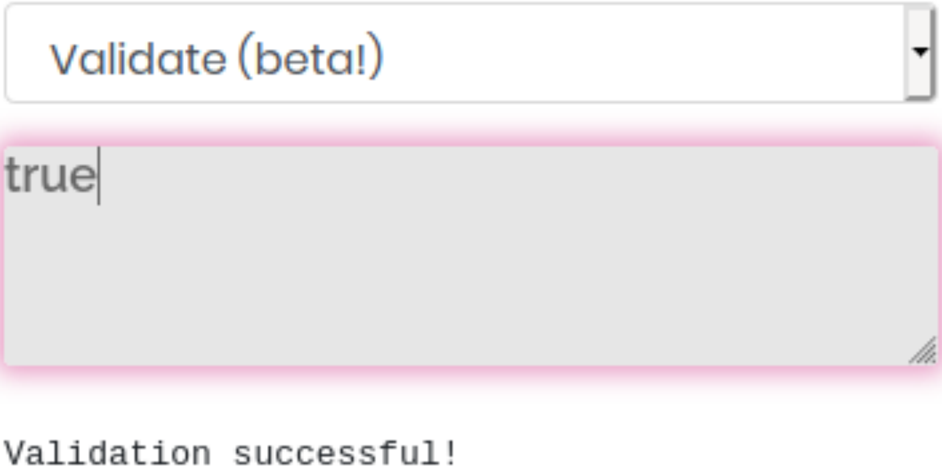


```
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

here we see that a loopback ip is running in the machine

no domain based routing

going to the webpage

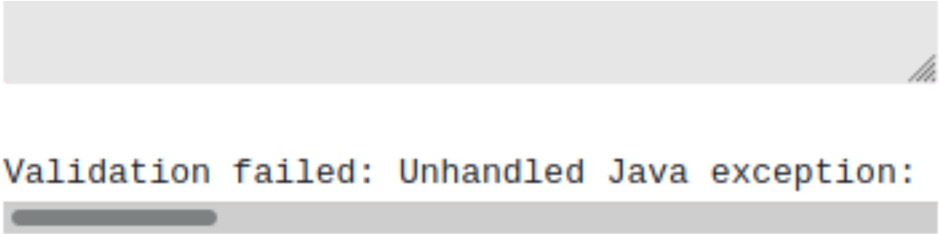


Validate (beta!)

true

Validation successful!

in validation if we give true, false or null it says validation sucessfull and any other input returns java exception



```
Validation failed: Unhandled Java exception:
```

Validation failed: Unhandled Java exception: com.fasterxml.jackson.core.JsonParseException: Unrecognized token 'admin': was expecting ('true', 'false' or 'null')

this has no vulnearable frameworks no vulnerable directories and no extra hints in page sources so i think this exception is the only way to get any shell