


SMB File Upload -> Webserver Access

```
└─$ smbclient -U WORKGROUP\WORKGROUP \\\192.168.56.117\web\\
Password for [WORKGROUP\WORKGROUP]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D                0
..               D                0
03-comming-soon  D                0
aspnet_client    D                0
common-js        D                0
fonts            D                0
images           D                0
index.html       A                1481
```




If we are able to access an SMB fileshare with write access to a web-accessible directory,

SMB File Upload -> Webserver Access

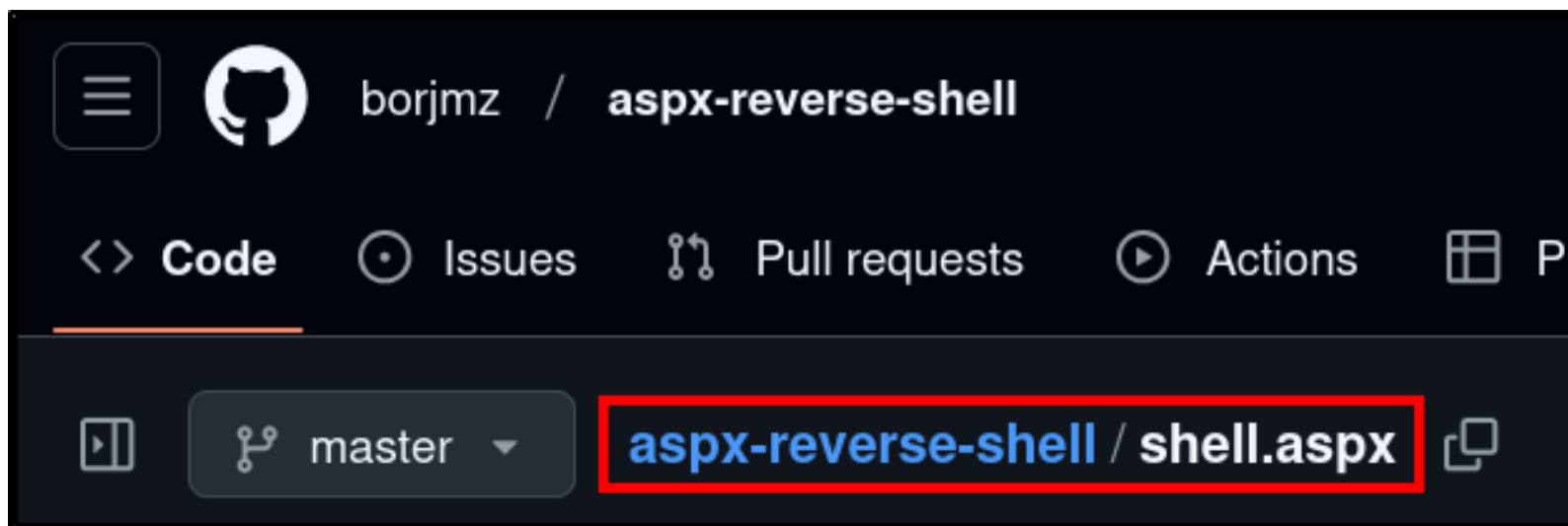
```
L$ smbclient -U WORKGROUP\WORKGROUP \\192.168.56.117\web\\
Password for [WORKGROUP\WORKGROUP]:
Try "help" to get a list of possible commands.
smb: \> dir
.
```

.	D	0
..	D	0
03-comming-soon	D	0
aspnet_client	D	0
common-js	D	0
fonts	D	0
images	D	0
index.html	A	1481



we could leverage these two conditions to gain Remote Command Execution on the server

SMB File Upload -> Webserver Access



Because this is a Windows web server, it's likely able to execute code written in .asp or .aspx files, so we can prepare such a file for upload

Privilege Escalation

SeImpersonate Privilege

```
Nombre de privilegio
=====
SeAssignPrimaryTokenPrivilege
SeIncreaseQuotaPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
```

The SeImpersonate privilege is a feature which allows a user to perform commands in the context of other users

Privilege Escalation

SelImpersonate Privilege

```
c:\windows\system32\inetsrv>whoami  
whoami  
iis apppool\defaultapppool
```

This privilege is typically associated with service accounts, like IIS, SQL Server, and with Administrator accounts

Privilege Escalation

SeImpersonate Privilege

```
Nombre de privilegio
=====
SeAssignPrimaryTokenPrivilege
SeIncreaseQuotaPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
```

Using SeImpersonate, attackers can elevate privileges to SYSTEM or Administrator level, either through Token Theft and / or Named Pipes

Selmpersonate – Potato Exploit

The Potato-family of Windows exploits all leverage the Selmpersonate privilege in different ways to achieve elevated access on Windows targets



Potato Exploit – DeadPotato



Which Potato exploit to use on a target largely depends on the version of Windows being used. In this case, we'll be using the DeadPotato variant