

Unrestricted File Upload







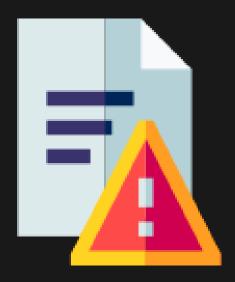






01

What is Unrestricted File Upload





What is Unrestricted File Upload

- It's a critical vulnerability that occurs when a web application allows users to upload files without any limitations or restrictions.
- The web application developer does not implement proper security checks and validation.















Q2
Risks of
Unrestricted File
Upload





Risks of Unrestricted File Upload

How critical is this

vulnerability?

- Denial of Service (DoS): Attackers could upload large files causing slowdowns or service interruptions.
- Malicious Code Execution: Attackers can upload files containing malicious scripts, or malware. These malicious files can be executed on the server, leading to unauthorized access and data breaches.
- And many more...













03

Hands-on Exploit





Hands-on Exploit

Time To Hack





Hands-on Exploit

- First, we'll upload a large file and see what is does.
- Second, we'll see how we can upload any type of file, even though it's supposed to only allow images.













Mitigations





Mitigations

How to prevent Unrestricted File Upload?

- Restricting file size, to prevent overloading the server
- Validate uploaded files thoroughly, checking file types and content.













05 Recap and Q&A



RESOURCES

https://portswigger.net/web-security/file-upload https://book.hacktricks.xyz/pentesting-web/file-upload

Book: Web Security for Developers

