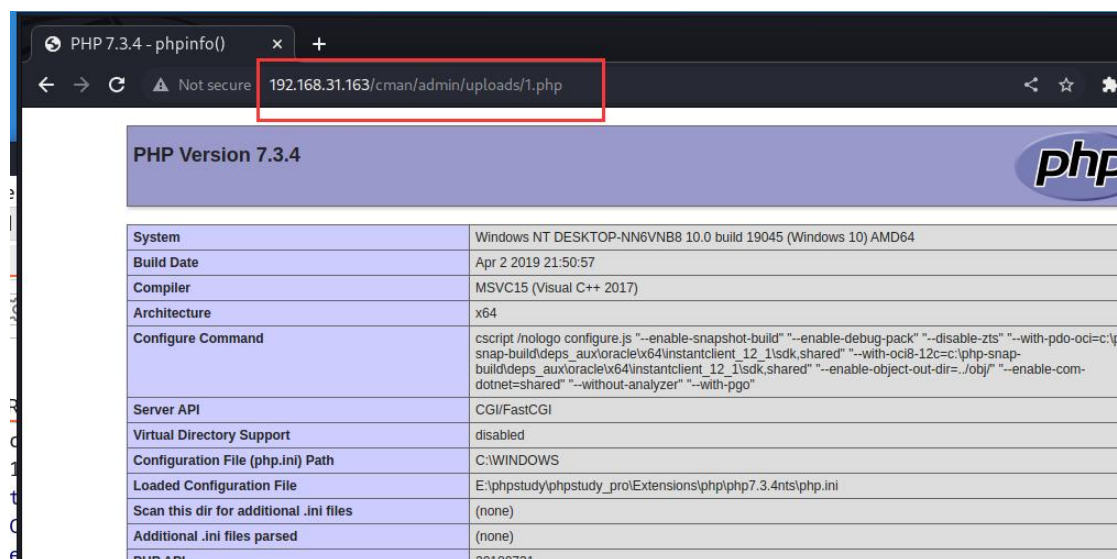
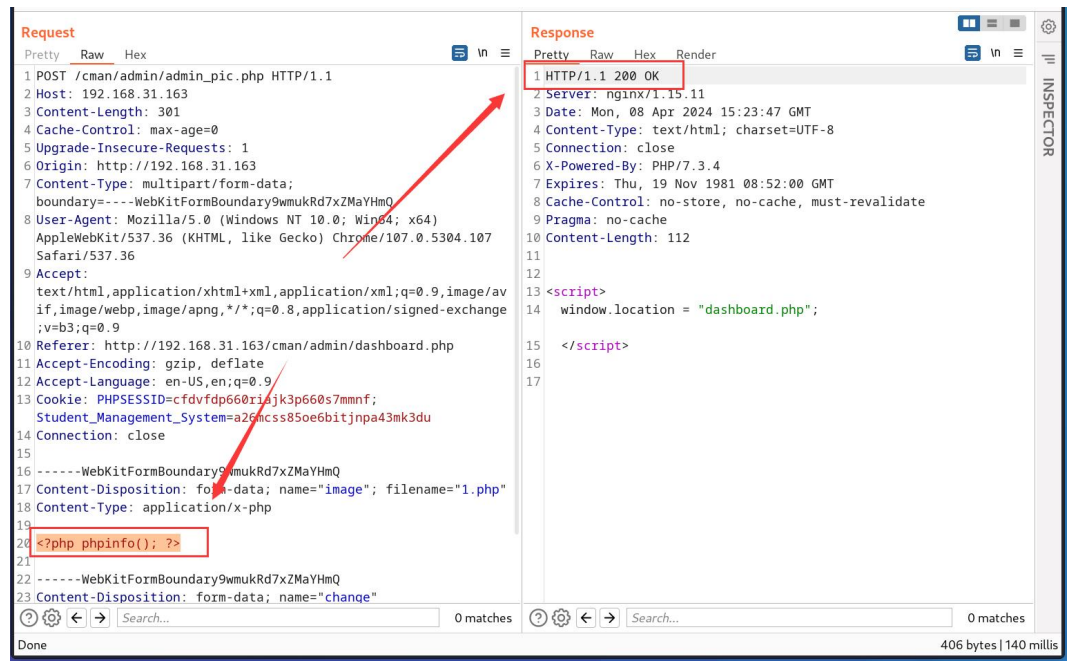


Arbitrary file upload vulnerability exists in image parameter of /admin/admin_pic.php file of Church Management System

Arbitrary file upload poses significant cybersecurity risks. Attackers can upload files containing malicious code to execute on the server, gaining system privileges and stealing sensitive data. They may also overwrite or delete legitimate files, disrupt system functionality, and abuse server resources. By bypassing authentication mechanisms, attackers can gain access to restricted resources, escalate privileges, and compromise the server.



Payload: image=<?php phpinfo(); ?>

Source Download:

<https://www.campcodes.com/projects/php/church-management-system/>