Bài này thật sự rất khó và mới với người kiểm thử web như mình.

Nó nghiên về chuyên cryptography hơn.

Cùng tìm hiểu nào!

Mô tả:

Tôi đã gửi 2 lời mời sinh nhật đến tất cả những người bạn của tôi. Tôi sẽ biết nếu chúng bị mất vì 2 lá thư nhìn rất giống nhau, thậm chí chúng có chung 1 mã hash nhưng vẫn hơi khác 1 chút. Bạn sẽ không tin nó đã làm tôi mất bao lâu để tìm sự xung đột. Bằng mọi cách, hãy xem bạn có được mời không bằng việc gửi 2 PDFs đến trang web của tôi.

Hint1: 1 trang PHP làm thế nào có thể kiểm tra những qui tắc trong phần mô tả?

Nó là lỗ hổng file upload nhưng không thể thực thi web shell được.

Bạn chỉ cần để content-type là application/pdf và gửi 2 file là bypass được.

Nếu gửi 1 file php 🡪 báo lỗi không phải pdf.

Nếu gửi 1 file pdf quá lớn 🡪 báo lỗi tập tin quá lớn.

Mình thử gửi 2 webshell giống nhau 🡪 báo lỗi tập tin giống nhau.

Nếu gửi hai file khác nhau 🡪 báo lỗi mã MD5 không giống nhau.

Lúc đầu mình đọc phần mô tả thì không hiểu gì. Mãi mới biết tôi là ứng dụng web, muốn xem được mời không (flag), mình phải gửi 2 file pdf khác nhau, nhưng chung 1 mã hash (MD5).

Thực tế, 2 tập tin có chung mã MD5 là giống nhau. Nhưng vẫn có những xung đột trong hash này.

Kẻ tấn công có thể lợi dụng nó để tạo 1 file tốt và xấu (hash md5 giống hệt nhau).

Thử tìm kiếm: How I made two PHP files with the same MD5 hash

Bạn sẽ có 2 file php như vậy, upload và lấy flag thôi.

**FLAG: picoCTF{c0ngr4ts\_u\_r\_1nv1t3d\_73b0c8ad}**