# nondiff-bacdoor

A bird flying in the sky

AI-generated content may be incorrect.

გვაქვს შემდეგი ტიპის საიტი. პირობაა შემდეგი: our website has been breached multiple times. now we even found a backup.zip in a public path and still can not find the backdoor.

საჭიროა ვიპოვოთ backdoor. backdoor არის რაიმე კოდი, რომელიც ვებსაიტს/სერვისს/სერვერს გააჩნია და მისი მეშვეობით შესაძლოა თავდამსხმელმა უფლებები მოიპოვოს სერვერზე. ის არ არის ვირუსი, თუმცა მისი გამოყენებით ბევრი რამის დაზიანებაა შესაძლებელი.

გავუშვათ dirsearch და ვნახოთ თუ რა სახის ფაილები გააჩნია სერვერს (ვებს)

(თუ dirsearch არ გვაქვს, დავაყენოთ sudo apt install dirsearch)

A screen shot of a computer

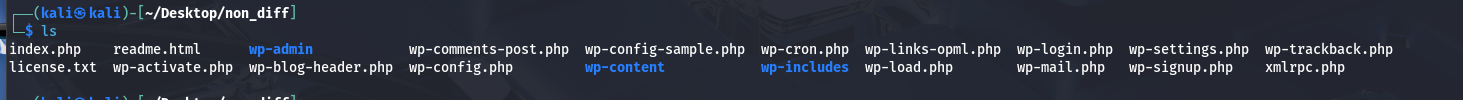
AI-generated content may be incorrect.



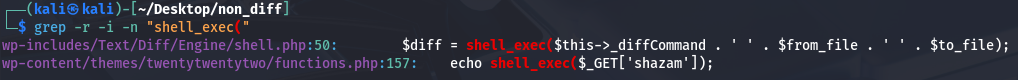
ნაპოვნია backup.zip ფოლდერი, ჩავწეროთ url-ში და ვნახოთ რა იქნება...



ენთერზე მარჯვენა ხელის დარტყმის შემდეგ ჩამოიტვირთება ზიპ ფოლდერ და ამოვაარქივოთ. გარდა ამისა, ჩვენ ვიცით რომ ბექში php გამოიყენება, ამიტომ მოწყვლადობის აღმოსაჩენად shell\_exec() ბრძანება გვჭირდება.



ამოარქივების შემდეგ ვხედავთ, რომ ბევრი ფაილია. დროის დაზოგვის მიზნით გამოვიყენოთ grep ბრძანება:

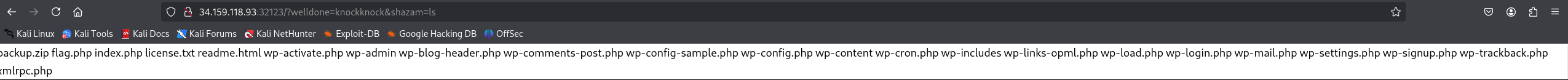


ფილტრაციის შედეგად გვაქვს ორი php სკრიპტი, სადაც exec არის გამოყენებული. დავუყვეთ და წავიკითხოთ ორივე:

A computer screen shot of code

AI-generated content may be incorrect.

ერთ-ერთ ფაილში get მეთოდს წავაწყდი, სადაც შემდეგი ლოგიკაა გაწერილი: http get მეთოდს სახელად welldone უნდა ჰქონდეს და მისი მნიშვნელობა knockknock უნდა იყოს, რათა shell\_exec-ის განხორციელება მოხდეს. გარდა ამისა, shell\_exec-ს მიეწოდება shazam (get მეთოდის სახელი) მნიშვნელობა.



A screenshot of a phone

AI-generated content may be incorrect.

შევაღწიეთ. ახლა საჭიროა flag-ის ძებნა და ამას ვიზამ შემდეგნაირად:



შედეგია:



ახლა ვუხმოთ cat ბრძანებას და ვნახოთ რა იქნება:



ბრძანება გაეშვა, თუმცა არაფერი გამოაქ. ინსპექტში, header-ში თუ ვნახავთ, არის გაწერილი შემდეგი ლოგიკა:



თუ 1 2-ის ტოლია, გამოიტანე ფლეგი. ფლეგი ისედაც ნაპოვნია უკვე, თუმცა გამოვიტანოთ ფრონტის მხარეს:

