Lab: nodiff-backdoor

IP მისამართზე შესვლისას, პირველ რიგში უნდა გამოვიკვლიოთ მაქსიმალურად მეტი რამ ამ საიტის შესახებ. კვლევის ერთ-ერთ მეთოდს წარმოადგენს Dirsearch. მისი გამოყენების შედეგად რამდენიმე ქვესაქაღალდე იქცევს ყურადღებას, ერთ-ერთია backup.zip. როდესაც ამ მისამართს მივმართავთ გადმოიწერს დაარქივებულ ფაილს. ფაილის ამორაქივების შემდეგ ვხედავთ რომ ის იყენებს PHP-ს. ამიტომ ვეძებთ არსებულ სისუსტეებს, რაც შეიძლება რომ გამოვიყენოთ. კოდში, backdoor-ის სახით, შეიძლება დატოვებული იყოს ისეთი კოდის ფრაგმენტი, რომელიც გაშვებადია. ერთ-ერთ გაშვებად კოდს წარმოადგენს shell\_exec. კოდში grep –r “shell\_exec(“ ბრძანებით ვნახულობთ რომ ასეთი ფრაგმენტი არსებობს. ამ ფრაგმენტის გაანალიზებით ვხვდებით რომ როდესაც გავაგზავნით GET request-ს სადაც welldone=knockknock გაეშვება ის რასაც ასევე ჩვენ გადავცემთ shazam პარამეტრის სახით. DirSearch ის დროს ასევე შევამჩნიეთ flag.php ამიტომ მოდი ვცადოთ მისი წაკითხვა. /?welldone=knockknock&shazam=cat flag.php ერთი შეხედვით არაფერი მოხდა თუმცა request წარმატებული იყო. თუ ჩვენ მაინც შევამოწმებთ inspect elements ჩვენ დავინახავთ ჩვენს flag-ს.