# PHP-unit

აღნიშნულ საიტზე გადასვლისას ვერ ვაწყდებით ჩვენთვის საინტერესო url\_ებსა და ლინკებს. ინსპექტში არაფერია.

ჩავატაროტ Web-Enumeration, რომელიც მოიცავს იმ რესურსების აღმოჩენას, რომელიც სერვერი იყენებს.

იმისთვის, რომ მოვძებნოთ ჩვენთვის რაიმე საინტერესო ინფორმაცია, ვუხმოთ ბრძანებათაგან სათნო dirsearch-ს, რომელიც brute force-ის მეშვეობით ეძებს ფაილებსა და ფოლდერებს, რომელიც ესა თუ ის სერვისი/სერვერი იყენებს. Dirsearch-ს ესაჭიროება დაყენება...



A screen shot of a computer

AI-generated content may be incorrect.

დაიწყო მუშაობა და ვხედავთ, რომ არის ასეთი ფოლდერი:  
A screenshot of a computer

AI-generated content may be incorrect.

(composer. json is a configuration file used in PHP projects that utilize the Composer dependency manager)

გვაქვს რამოდენიმე დირექტორია, თუმცა დავიწყოთ composer.json-ით. გამოვიყენოთ პროგრამათაგან სათნო Burp Suite და გადავიჭიროთ პაკეტები. მისი მეშვეობით შეგვიძლია აგრეთვე გავიგოთ რა OS-ზე არის სერვერი.



A screenshot of a computer program

AI-generated content may be incorrect.

გადავიჭირეთ პაკეტები, გავუშვათ repeater-ში და განვახორციელოთ ოპერაციები...

A screenshot of a computer

AI-generated content may be incorrect.

ვხედავთ, რომ სერვერი არის Debian ანუ ლინუქსი. phpUnit-ის ვერსია (PHPUnit is a unit testing framework for the PHP programming language.) არის 5.6.2. ვნახოთ თუ არის ის მოწყვლადი:

A screenshot of a computer

AI-generated content may be incorrect.

როგორც ჩანს ხაკერებმა იზარმაცეს და ბევრი მოწყვლადობა ვერ აღმოუჩენიათ მთელი ამდენი ხნის მანძილზე...

A screenshot of a computer

AI-generated content may be incorrect.

ახლა კი ვცადოთ და გავაყოლოთ Get მეთოდს php სკრიპტი.

ვუხმოთ ქეთინოს, რაულის, ომარიკოს, მაიასა და იას სახელების პირველი სიმბოლოების საძიებო ველს და დავსერჩოთ შემდეგი :  
Php exec script

A black background with white text

AI-generated content may be incorrect.



გითზე გადასვლის შემდეგ მითიტებული path მივუთითოთ repeater-ში:  


A close-up of a computer code

AI-generated content may be incorrect.

ვუხმოთ php სკრიპტსაც და დავიწყოთ ძებნა...

A computer code with numbers and letters

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A close up of a computer screen

AI-generated content may be incorrect.