# Bolt

34.159.78.95:30626 URL-ზე გადასვლის შემდეგ ვნახავთ, რომ აწყობილია მარტივი CMS (A content management system (CMS) is computer software used to manage the creation and modification of digital content (content management)) საიტი.

საიტი იყენებს bolt-ის CMS, ამას ვადგენთ მრავალი გზით. მაგალითად საიტის ბოლოს მითითებლია bolt. გარდა ამისა, F12 ღილაკის დაჭერით, ვაწყდებით path-ებს (img, a …) სადაც Bolt path არის მითითებული.

ტეგებში path-ის მითითებისთვის ჯერ გადავიდეთ საიტის რაიმე გვერდზე, რადგან home page-ს არ გააჩნია ისეთი tag, რომელიც src-ს ითხოვს (path).

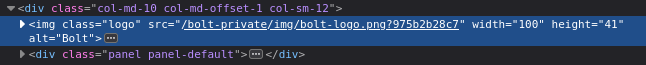
გადავედით sub1-ში:

A computer screen shot of a program

AI-generated content may be incorrect.



Bolt-public რეპოზიტორია? ვებსაიტს გააჩნია private (administrator privileges) და public (Client accessibility). როგორც წესი, admin პრივილეგიაზე რომ გადავიდეთ, შსაჭიროა მივუთითოთ დახურული (private) path.









Img url-ის ცვლილებამ შედეგამდე ვერ მიგვიყვანა, თუმცა გამოვიყენოთ მისი path საძიებო ველში და მსგავსი ოპერაციები განვახორციელოთ:  
34.159.78.95:30626/bolt-public/img/bolt-logo.png?975b2b28c7

34.159.78.95:30626/boltprivate/admin

[34.159.78.95:30626/bolt](http://34.159.78.95:30626/bolt)

საბოლოოდ, მივედით დასკვნამდე, რომ საძიებო ველში admin არა, თუმცა bolt-ის მითითებით შევძლებთ გადასვლას და შევეცდებით ადმინისტრაციული პრივილეგიების ხელში ჩაგდებას.

A screenshot of a login form

AI-generated content may be incorrect.

Brute force-ის შედეგად, აღმოვაჩინე, რომ admin/password არის input-ებში შესაყვანი.

დაგუგვლის შედეგად, არმოვაჩინე, რომ bolt php\_ზე არის დაწერილი. ცხადია ჯერ მოწყვლადობა უნდა ვიპოვო და შემდეგ შევეცადო php სკრიპტის გაწერა.

File manager სექციაში, იტვირთება გარკვეული გაფართოების ფაილები (php არა).

ატვირთვის შედეგად შეგვიძლია ფაილის გაფართოების გადაკეთება. საქმე გვაქვს MIME ტიპის ოპერაციასთან. MIME – Multipurpose Internet Mail Extension არის, რომელიც სერვერზე ატვირთული ფაილის გაფართოებაზე მიუთითებს. შეგვიძლია ეს მოწყვლადობად გამოვიყენოთ, ცხადია თუ სერვერი ამგვარი ტიპის თავდასხმისთვის დაცული არ არის. ავტვირთოთ რაიმე .txt ფაილი და შემდეგ php-ით გადავაკეთოთ.



A screenshot of a phone

AI-generated content may be incorrect.

შევეცადოთ php-ის გამოყენებით რაიმე ლინუქსის სკრიპტი გავწეროთ და გავგზავნოთ სერვერზე...

A screenshot of a computer code

AI-generated content may be incorrect.

დროა გადავაკეთოთ php გაფართოებად და ვნახოთ რა შედეგი იქნება.



A screenshot of a computer

AI-generated content may be incorrect. test.php ფაილზე დაჭერით გადავდივართ მოცემულ გვერდზე. ახლა საჭიროა დავუყვეთ ყველა დირექტორიას და შევეცადოთ flag მოვძებოთ. Flag როგორც წესი, root დირექტორიაშია მოთავსებული, ამიტომაც მანდედან დავიწყებ 😊

Php სკრიპტის გადაკეთებისთვის მოგვიწევს ფაილის txt\_ად გადაკეთება და ისევ გადმოკეთება. Php ფაილში უშუალოდ სკრიპტს ვერ გავწერთ...

A screenshot of a computer code

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect. flag ნაპოვნია, ახლა წავიკითხოთ.

A line of black lines

AI-generated content may be incorrect.

ვეცადოთ გადავიდეთ root დირექტორიაში და ისე წავიკითხოთ ფლაგი.



A screenshot of a computer

AI-generated content may be incorrect.

