Bolt

# 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.

A screen shot of a computer

Description automatically generated







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.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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.



# 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.

Nondiff backdor

A screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A computer screen shot of a code

Description automatically generated

A computer screen with text

Description automatically generated

# 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

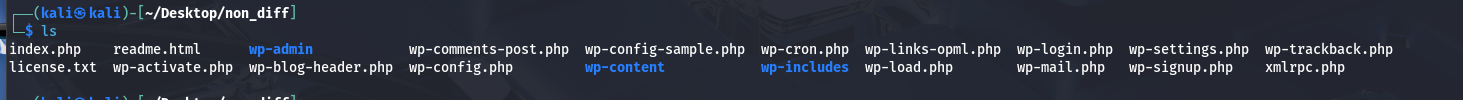
AI-generated content may be incorrect.



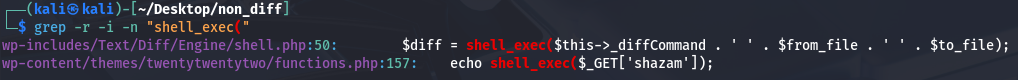
ნაპოვნია backup.zip ფოლდერი, ჩავწეროთ url-ში და ვნახოთ რა იქნება...



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:

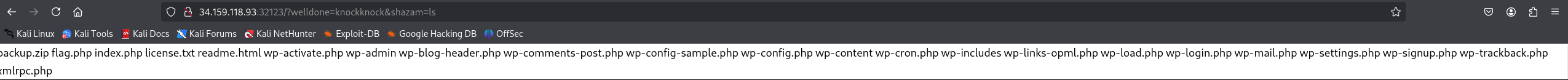


ფილტრაციის შედეგად გვაქვს ორი php სკრიპტი, სადაც exec არის გამოყენებული. დავუყვეთ და წავიკითხოთ ორივე:

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:



# LibSSH

ამოცანის პირობის თანახმად flag-ის ძებნა მოსახერხებელია CVE-ის მეშვეობით. CVE-Common Vulnerability and Exposure. Exploit არ არის ვირუსი ანდ რაიმე malware. ის არის მიდგომა, რომელიც სისტემაში არსებულ მოწყვლადობას იყენებს თავდასხმის განსახორციელებლად.

A screenshot of a computer

AI-generated content may be incorrect.

სატიზე გადასვლისთანავე გვაქვს ssh-ის ინფორმაციაზე. SSH არის დისტანციურად ჰოსტზე დაკავშირების მიდგომა, რომელიც აბსოლიტურად უსაბრთხოა. ჩემი ამჟამინდელი ინფორმაციით, SSH-ის ბოლო ვერსია არის 2.0. გარდა SSH-ისა, გვაქვს libssh-ის შესახებ ინფორმაცია. Libssh C-Library არის, რომელიც SSH-ის კონფიგურაცია/იმპლემენტაციას უზრუნველყობს. ამოცანის პირობის თანახმად, flag-ის ძებნა CVE-ის მეშვეობით შეგვიძლია. მოვიძიოთ LibSSH-ის ამ ვერსიაზე ინფორმაცია, მოწყვლადი ხომ არ არის?

A screenshot of a computer

Description automatically generated

მოცემულ საიტზე გადასვლით ვადგენთ, რომ 0.6 და უფრო ახალი ვერსიების libssh მოწყვლადია. გარდა ამისა, CVE-იც მოცემულია. მოვძებნოთ გით-ზე source code:

A screenshot of a computer

AI-generated content may be incorrect.

  
მოცემული სკრიპტი argv-ს მეშვეობით იღებს ჰოსტის მისამართს, პორტსა და ბრძანებას. თუმცა სკრიპტი იმუშავებს იმ შემთხვევაში, თუ ssh კავშირი გვექნება ჰოსტთან:



ახლა გვრჩება მხოლოდ დირექტორიებში ძრომიალი და ფლაგის ძებნა 😊

A close up of numbers

Description automatically generated



გარდა ამისა, მაქვს დაწერილი სკრიპტი, რომელიც 2-1-ში მუშაობს და არ გვჭირდება ცალკე ssh-ის გაწერა და ცალკე სკრიპტის გაშვება.  
<https://github.com/giolga/ssh-command-exec>  
მოცემული სკრიპტი:

>ქმნის socket-ს და უერთდება მითითებული IP:Port მისამართით

>იყენებს paramiko ბიბლიოთეკას SSH პროტოკოლის გასამართად

>უვლის აუტორიზაციის პროცესებს გვერდს. კერძდ კი, სერვერს ატყობინებს, რომ მომხმარებელი აწ უკვე ავტორიზებული არის

> იქმნება SSH სესია და შესაძლებელია კომანდების გაშვება

A screenshot of a computer

Description automatically generated

# Ellastic

A screenshot of a computer program

AI-generated content may be incorrect.

საიტზე გადასვლისთანავე ვაწყდებით JSON ტიპის ინფორმაციას. ამოცანის პირობის თანახმად elasticsearch-ის მოწყვლადობა უნდა აღმოვაჩინოთ. თუ დავხედავთ საიტს, შევამჩნევთ რომ Elasticsearch-ის ვერსია არის 1.3.4. ვცადოთ მოწყვლადობის პოვნა.

როგორც ჩანს ჩვენი ვერსია მოწყვლადია და გააჩნია CVE. მოვძებნოთ ჩვენი ვერსიისთვის შესაბამისი Common Vulnerability and Exposure: A grey rectangular sign with white text

AI-generated content may be incorrect.

<https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py>

დავადგინეთ, რომ ჩვენი ვერსიის CVE არის 2015-5531, ამიტომ ავიღოთ პითონ სკრიპტი და შევეცადოთ მოვძებნო მოწყვლადობა.

A screenshot of a computer

AI-generated content may be incorrect.



A computer screen with white text

AI-generated content may be incorrect.

პითონ სკრიპტი argv-ის წყალობით მოითხოვს საიტის ლინკსა და /etc/passwd-ის.

A screen shot of a computer

AI-generated content may be incorrect.

