

## 312-50v12 Dumps

### Certified Ethical Hacker Exam (CEHv12)

<https://www.certleader.com/312-50v12-dumps.html>



**NEW QUESTION 1**

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.

Which of the following techniques is employed by Susan?

- A. web shells
- B. Webhooks
- C. REST API
- D. SOAP API

**Answer: B**

**Explanation:**

Webhooks are one of a few ways internet applications will communicate with one another.

It allows you to send real-time data from one application to another whenever a given event happens.

For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.

What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered. The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data. Here's a visual representation of what that looks like:

A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.

Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the "payload." Here's an example of what a webhook url looks like with the payload it's carrying:

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase.

These notifications from the applications are usually sent through webhooks.

**NEW QUESTION 2**

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

- A. Docker client
- B. Docker objects
- C. Docker daemon
- D. Docker registries

**Answer: C**

**Explanation:**

Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers.

The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.

The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

**NEW QUESTION 3**

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

- A. DROWN attack
- B. Padding oracle attack
- C. Side-channel attack
- D. DUHK attack

**Answer:** A

**Explanation:**

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain?

Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

Operators of vulnerable servers got to take action. there's nothing practical that browsers or endusers will do on their own to protect against this attack. Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

A server is vulnerable to DROWN if:

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings. Its private key is used on any other server that allows SSLv2 connections, even for another protocol.

Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

How do I protect my server?

To protect against DROWN, server operators need to ensure that their private keys software used anywhere with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s.

Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more modern version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators are ready to take action to guard against the attack.

**NEW QUESTION 4**

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary In the above scenario.

- A. use of command-line interface
- B. Data staging
- C. Unspecified proxy activities
- D. Use of DNS tunneling

**Answer:** C

**Explanation:**

A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.

If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

**NEW QUESTION 5**

What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

- A. Vulnerability hunting program
- B. Bug bounty program
- C. White-hat hacking program
- D. Ethical hacking program

**Answer:** B

**Explanation:**

Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.

The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.

Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).

Who uses bug bounty programs?

Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.

Why do corporations use bug bounty programs?

Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.

This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.

It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program. This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.

Why do researchers and hackers participate in bug bounty programs?

Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job. It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.

What area unit the disadvantages of a bug bounty program for independent researchers and hackers?

A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.

In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash. Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.

In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.

Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).

What square measure the disadvantages of bug bounty programs for organizations?

These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)! If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.

Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).

Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies. The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.

This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.

This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

**NEW QUESTION 6**

Which file is a rich target to discover the structure of a website during web-server footprinting?



- A. Document root
- B. Robots.txt
- C. domain.txt
- D. index.html

**Answer:** B

#### NEW QUESTION 7

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. Netcraft
- C. infoga
- D. Zoominfo

**Answer:** C

#### Explanation:

Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

#### NEW QUESTION 8

Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unknornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

- A. 64
- B. 128
- C. 255
- D. 138

**Answer:** B

#### Explanation:

Windows TTL 128, Linux TTL 64, OpenBSD 255 ... <https://subinsb.com/default-device-ttl-values/> Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

#### NEW QUESTION 9

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment
- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

**Answer:** B

#### Explanation:

Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

#### NEW QUESTION 10

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture Is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-4: Orchestrators
- C. Tier-3: Registries
- D. Tier-2: Testing and accreditation systems

**Answer:** D

#### Explanation:

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization. Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter. For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all

intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary.

Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

**NEW QUESTION 10**

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

- A. .X session-log
- B. .bashrc
- C. .profile
- D. .bash\_history

**Answer:** D

**Explanation:**

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed. BASH\_HISTORY files are hidden files with no filename prefix. They always use the filename .bash\_history.

NOTE: Bash is that the shell program employed by Apple Terminal.

Our goal is to assist you understand what a file with a \*.bash\_history suffix is and the way to open it.

The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

**NEW QUESTION 12**

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

**Answer:** B

**Explanation:**

<https://tools.kali.org/information-gathering/hping3>

<http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf>

**NEW QUESTION 17**

What is the proper response for a NULL scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Answer:** F

**NEW QUESTION 21**

You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.

What Is the best Linux pipe to achieve your milestone?

- A. dirb https://site.com | grep "site"
- B. curl -s https://sile.com | grep "< a href-\`http" | grep "Site-com- | cut -d "V" -f 2
- C. wget https://stte.com | grep "< a href=\\`http" | grep "site.com"
- D. wgethttps://site.com | cut-d"http

**Answer:** C

**NEW QUESTION 25**

Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

- A. User-mode rootkit
- B. Library-level rootkit
- C. Kernel-level rootkit
- D. Hypervisor-level rootkit

**Answer:** C

**NEW QUESTION 28**

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

- A. True

B. False

**Answer:** B

### NEW QUESTION 33

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

**Answer:** C

#### Explanation:

[https://en.wikipedia.org/wiki/Internet\\_Relay\\_Chat](https://en.wikipedia.org/wiki/Internet_Relay_Chat)

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients.

IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well.

You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls.

[https://en.wikipedia.org/wiki/Application\\_firewall](https://en.wikipedia.org/wiki/Application_firewall)

An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based.

Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.

Network-based application firewalls

Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.

Host-based application firewalls

A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

### NEW QUESTION 34

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

- A. False-negative
- B. False-positive
- C. Brute force attack
- D. Backdoor

**Answer:** B

#### Explanation:

<https://www.infocycle.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-an>

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

### NEW QUESTION 38

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application. What kind of Web application vulnerability likely exists in their software?

- A. Cross-site scripting vulnerability
- B. SQL injection vulnerability
- C. Web site defacement vulnerability
- D. Gross-site Request Forgery vulnerability

**Answer:** A

#### Explanation:

There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one

searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

**NEW QUESTION 41**

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

- A. Reconnaissance
- B. Maintaining access
- C. Scanning
- D. Gaining access

**Answer:** D

**Explanation:**

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're → • Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table a used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. • Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

**NEW QUESTION 45**

What is the following command used for?

```
sqlmap.py-u  
„http://10.10.1.20/?p=1  
&forumaction=search" -dbs
```

- A. Creating backdoors using SQL injection
- B. A Enumerating the databases in the DBMS for the URL
- C. Retrieving SQL statements being executed on the database
- D. Searching database statements at the IP address given

**Answer:** A

**NEW QUESTION 50**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 312-50v12 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/312-50v12-dumps.html>