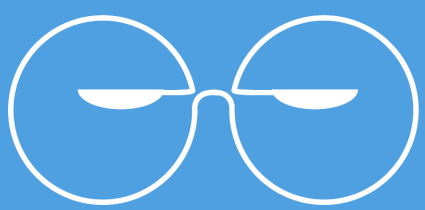
APPSEC engineer

A Beginner's Guide to Careers in AppSec

CONTENTS

WHY SHOULD I PICK A CAREER IN SECURITY



Here's a question we get asked a lot:

"Why should I pick a career in security?"

Information security is one of those industries that isn't just growing incredibly fast, it also has profound implications on every aspect of our modern, data-driven economy. Valued at USD 188 billion in 2023 according to Gartner, the AppSec market is expected to grow beyond USD 288 billion by 2027 according to analysts.

Information Security is more important than ever

In 2023, we saw not one, but two of the biggest cyberattacks of the last decade, and thousands more data breaches that have collectively cost companies, and governments billions of dollars. According to an IBM report, the average cost of a data breach was USD 4.45 million, a 15% increase over the last three years.

Organizations today are more aware than ever of the looming threat of a cyberattack, but they're nevertheless struggling with managing risk and reducing the impact of security breaches. Previously ignored concepts like threat modeling and DevSecOps are taking center-stage as companies recognise that security isn't a box you check at the end of production, it's an active, continuous element of the development process.

How competitive is the Information Security job market?

In the US, Glassdoor pegs the national average salary of a security engineer at around $150,000, well above what a network engineer or developer can expect to make at around $100,000. Despite this, in a 2023 report by ISC2, the global cybersecurity skills gap is nearly 4 million, and it's growing every year.

> **Security is expected to be a $288 billion industry in 2027. Despite this, there's a shortage of nearly 4 million cybersecurity jobs around the world.**

Security is expected to be a $288 billion industry in 2027. Despite this, there's a shortage of nearly 4 million cybersecurity jobs around the world.

But there's a reason for this. AppSec is still sometimes seen as a 'less-than-critical' part of software development, which means unless the company can afford it, a lot of businesses aren't willing to spend on training their employees. And new hires often don't have the kind of real-world practical experience that's critical for an AppSec professional.

It's a classic chicken and the egg problem, except no one seems to be able to find any more chickens, and the incubator to hatch new eggs is too expensive.

This all sounds rather discouraging, but what we're actually trying to do is set your expectations. Application security is a young and exciting field that's constantly changing, and you get the opportunity to work on groundbreaking projects and solve complex problems every single day.

If you're reading this ebook, you're already on your way to starting an exciting new career in this field. We've compiled some of the best pro-tips, advice, and guiding principles from some of the industry's leading experts on everything you need to know about how to start your career in application security

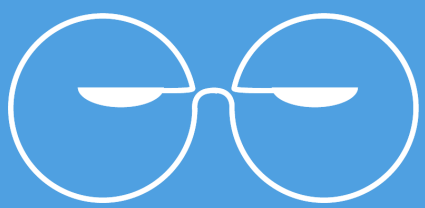
Q. What are the most important skills I need to get a job in Application Security?

For starters, you will need good social and communication skills. If you can't get along with the software developers, you won't get anywhere. And if you can't explain how to fix things or why something is important, again, you won't be able to succeed in this area. The art of persuasion is used often in the field of application security, if you want to excel.

I would also say that technical skills (how to install a tool, how to pick the best tool, how to run it and get good results), and how to build a program at an organization, would be the other two main skills you want to have. You can always learn a new tool, but understanding how to decide what type of tool, when to use it, and how to use it, are skills that will take you a lot further.

- Tanya Janca, Founder & CEO, We Hack Purple Academy

8 THINGS TO FAST-TRACK YOUR APPSEC CAREER



It's easy to think of your career as a distant goal you won't have to think about for a long time. But that won't just happen overnight. To get where you want to be tomorrow, you need to consistently put in some serious work today.

Instead of trying to figure all that out for yourself, we've compiled a list of all the things you could start doing today, without any fancy subscriptions or equipment. These are some of the most practical ways to build towards a career in security, and you're going to see both short-term results and long-term gains.

1. Learn about the OWASP Top 10

This is one of the first things pretty much anyone in security will tell you to do. Every year, the Open Web Application Security Project (OWASP) compiles a list of the ten most common and highest-risk vulnerabilities that affect applications and networks around the world.

The OWASP Top 10 is a great way to set a baseline knowledge about the most critical vulnerabilities out there. Reading about each of the vulnerabilities will help you understand how attackers exploit various weaknesses in an application's defence systems.

2. Workshops, whitepapers, and resources from cloud providers

Major cloud providers like AWS, GCP, and others offer tons of extremely detailed and useful resources on lots of different aspects of cloud and application security. Some of these are academic whitepapers and reports, while others are more hands-on security workshops where you build and test services and features.

Pretty much all of these are available for free, so it's super easy for you to just jump in and get started.

3. Stay up-to-date on current events in AppSec

This one might sound kind of basic, or even obvious, but it helps a lot more than you realize (even for an established security pro).

"Always, always keep your ear to the ground when it comes to what's new in the industry," says Abhay Bhargav, CEO of we45. "And I don't just mean read a blog post every now and then. Make it a habit to stay as current as possible. You can be prepared to ride a future trend before it even hits. And you'll be coming up with solutions no one else would have known about."

4. Learn with OWASP Projects

OWASP Projects are an insanely useful library of open-source community-driven projects meant to help people find resources for their security initiatives.

These are some of our favourite OWASP Projects for beginners:

OWASP Cheat Sheet series
The Cheat Sheet is a collection of over 65 high value information on specific application security topics.

OWASP WebGoat
WebGoat is application made deliberately vulnerable so you can use it to practice various security tests, exploits, and tools.

OWASP Security Knowledge Framework
The SKF is an extensive knowledge base you can use to learn how to integrate security by design in an application. It even has examples and best practices on how to prevent attackers from exploiting your apps.

5. Understand the tech you're trying to secure

It's impossible to effectively fortify an application without understanding the underlying technology it's built on. For example, if you're working on a cloud-native app, it's crucial to know how cloud architecture works on a fundamental level.

As a security engineer, your job will be to figure out all the ways an attacker can find to exploit your app. Knowing how your app works from the inside out can help you map user and abuser stories to their corresponding security test cases and mitigations.

6. Learn how to code

Here's one of the biggest misconceptions in the world of security: developers make apps, and AppSec engineers break apps. In reality, you'll be spending a lot of time with developers figuring out not just why their app is exploitable, but the most efficient way to secure it.

To do that effectively, it's important to learn how to code. You'll have the ability to troubleshoot issues while testing, and it can help you understand what a particular code block is supposed to do.

Beyond that, it gives you have a level of technical fluency when you talk to the developer who actually built the app, making for rapid, efficient collaboration.

7. Take part in competitions

Participate in every hackathon and capture-the-flag competitions you can find. A potential employer isn't just looking for the courses you've taken or the degrees under your belt.

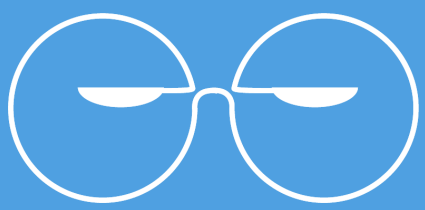
Your resume is going to look a whole lot more interesting if you can show them that you've been active in AppSec events that show off your technical skills. You're sending a clear message that you're someone who takes on challenging problems and is willing to put the extra effort to sharpen your skills and be active in the AppSec community.

8. Hone your skills with some bug bounty hunting

In 2022, Google paid security researchers over USD 12 million through their Vulnerability Rewards Program. Even so, it's not so much about the money as it is about what a successful bug bounty can do for your resume.

"It's a great way to show a potential employer that you really know your stuff," says Sudarshan Narayanan, Senior Manager of Technology Consulting at EY. "It sends them a message: 'I found a problem where no one else thought to look, and that was for Google. Hire me and I can do the same for you.'"

LET's GET ONE THING STRAIGHT: AppSec =/= Hacking



If movies are to be believed, hackers are these uber-cool tech wizards, fingers flying across their keyboards, unintelligible green on black lettering streaming across their screens as they break their way into every database and 'mainframe' known to mankind.

They're the sneaky ninjas that can penetrate any defensive walls, the finger that tips over the first domino, resulting in a chain reaction that collapses the economies of entire nations.

At least that's how we *want* people to see us.

There's just one problem. Real hacking is nothing like that. Security engineers don't just break an app to make it fail, they do it so they can understand how to build it back up. Only this time, they need to make it more secure than it was before.

The un-sexy side of security

If you were getting into application security hoping for cool stories to tell your friends over a beer, I'd hate to burst your bubble, but it's a lot more similar to a normal engineer's job.

That doesn't mean it's not fun, though! We're not trying to get you down, We're just setting realistic expectations here.

But now that you're aware of the nature of your future career, what can you expect your job to be like? Well, for starters, there's a surprising amount of collaboration you'd have to do with the other divisions in product engineering.

As an AppSec engineer, one of your most critical responsibilities would be to communicate your security findings with the developers on your team. You'll not only be showing them what vulnerabilities you found in their code, but also help them in fixing them in time for the next release. Additionally, you might even need to give them helpful pointers on how to avoid security flaws like that in the future.

This is where it helps to know how to code, so you should seriously consider developing that skill if you haven't already.

Offensive vs. Defensive AppSec

Broadly speaking, (and kind of oversimplifying) there's two main sides to application security. Offensive security is where you're acting as the malicious outsider trying to access data and privileges you're not supposed to have. The other is Defensive security, where you're the ones that built the app and are trying to find ways to harden it against those attackers. And that's the actual 'security' part of Application Security.

Offensive security is really more a means to an end, the 'end' here being more robust defensive measures for your application. It's a way for engineers to simulate attack scenarios as an outsider trying to find their way in, and using that information to build stronger fortifications. You need the former to learn how to better do the latter.

At the end of the day, employers want someone who can straddle both worlds with equal ease. After all, they say you can't hire a saint to catch a sinner.

Q. Is it necessary to be a programmer before getting into AppSec?

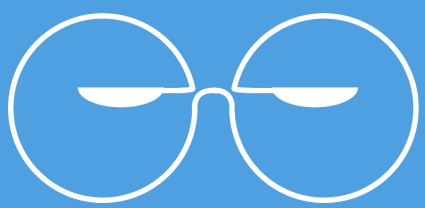
There is a common phrase that I've heard many times over the past few years and it goes something like this: "A hammer can be used to build a house or destroy one."

The difference between building and destroying comes down to intention but also ability and knowledge. When I look at an Application Security team and what the intentions and goals are of that team, it comes down to enabling the engineering of software in a secure manner. This will require the ability to understand development environments, how code is written so you can perform code reviews, how software is built and tested, and how applications are run in a production environment.

As an Application Security professional, your ability to understand the developer mindset, their problems and constraints, and how you can work with them to bring security into the SDLC will greatly increase your effectiveness in the Application Security industry.

- Derek Fisher, Vice President of Application Security at Envestnet

APPSEC ISN'T JUST 'APPLICATION SECURITY'



AppSec isn't just 'application security' anymore

Back in the good ol' days, every team in the product engineering pipeline had their own separate responsibilities. Developers did the coding, DevOps engineers handled the pipelines and operations, and security professionals were there to find vulnerabilities in the system.

These teams were generally siloed off, with not a whole lot of overlap between them. But all that's changing now.

Applications are huge and complex, more so today than ever before. All those moving parts make it necessary for teams to start automating and codifying more mundane tasks, ensuring human or team-based dependencies don't hold back the pace of development. It's why we're seeing the rise of Infrastructure as Code, Threat Modelling as Code, and largely automated security scans. Literally everything is code these days.

If this is starting to sound intimidating to non-programmers, relax. This doesn't mean you're suddenly expected to be able to develop an algorithm to predict the flight path of a space shuttle in the Cow Programming Language (look it up, it's hilarious). But it does mean you're going to have to get out of your comfort zone as an application security engineer.

How good are you at multitasking?

These days, developers are having to not just build apps but also consider the deployment, the environment it runs in, and all kinds of operational concerns that were traditionally the sole domain of DevOps engineers. The development process itself is hugely influenced by the cloud provider, hosting environment, and tech stack each engineering team uses.

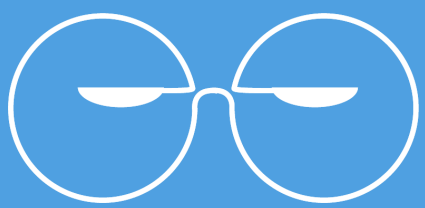
As an AppSec engineer, you'll have to start thinking about that, too. You'll need to ask important questions: Are your developers writing secure code? If not, what can they do differently? What's the most secure way to deploy your application on Kubernetes? How does hosting the app in AWS change your security risks? Is it running securely, or can an attacker initiate a container breakout during runtime and get access to the data?

You're even going to come across unique situations no one's ever encountered before because they don't use your organization's hosting or tech stack. And almost none of these questions are cut-and-dried; you're going to find yourself collaborating with people in every team to figure out the solution to a complex problem. Who knows? Your findings could potentially change your organization's development methodology. Trust us, we're only saying this because we've actually seen it happen in the real world.

The more you learn about product engineering, the deeper the rabbit hole goes. But that's also what makes it so exciting. You can be at the forefront of a technological renaissance and have interesting new challenges to overcome every day. AppSec is not just about securing software anymore. It's about transforming the way we look at product development on a fundamental level. If that doesn't sound incredible to you, we don't know what does.

.

EMPLOYERS NEED PEOPLE WITH EXPERIENCE



It's usually not enough to just take a course in a particular field of security, get certified, and call it a day. AppSec is an industry that values skill over everything else, and being able to demonstrate that skill is absolutely critical if you're looking to get noticed. Practical learning is the fastest way to level up your abilities, because it ensures you learn how security works *and* how to implement it in the real world.

But don't stop at just learning. Application security is like a game of problem-solving, and the only way to get good at it is to actually solve more problems. Whenever you learn something new, you need to practice that skill, applying it in a scenario where you can get tangible results. See how hands-on learning works in AppSecEngineer.

What should your resume look like?

One thing you should know about AppSec is that most people in the industry don't really care about your academic background. While security research is an incredibly important field of study, it's hardly a requirement when you're thinking about a career in AppSec.

But on the flip side, the security industry shares a lot of the same well-meaning scepticism and peer-reviewed scrutiny that you see in academia. They can be a tough crowd to please.

Security evangelist Per Thorsheim believes that you are not a security professional "until other security professionals start to refer to you as being one." In other words, your credentials don't make you an AppSec pro. It's the process of actually working with your hands to solve real-world security problems that defines how people see you in the industry.

Having all the theoretical security knowledge in the world won't matter if you can't put it to good use. And that's critical when you're looking for a job in security. Practical experience is basically a necessity for a career in AppSec.

How do you get experience in AppSec?

If you read the '7 things you could be doing to fast-track your AppSec career', your best starting point would be to...well, *do stuff.* Whether you're practicing how to compromise OWASP WebGoat, taking part in capture-the-flag competitions, hackathons, and even doing bug-bounties.

But what if you're a beginner? If you're just starting out in security and you want to level up your knowledge AND skills *fast*, you should really try out AppSecEngineer (shameless plug, we know). Seriously though, we have some of the best hands-on labs, cyber-ranges, and security exercises in the industry. While you watch our videos, you're also practicing what you learn.

What's so cool about these labs is that they're modelled after real-world security scenarios that *we've actually seen happen before.* It's simply the most authentic way to level up your AppSec skills while still gaining valuable experience for a job.

Most of all, though, be in the know of AppSec news. It's still a relatively young industry, and an incredibly dynamic one. Opportunities to learn and gain experience in even the smallest of ways can help. If you can show your potential employer that you're proactively seeking out new challenges and opportunities, you're already way ahead of a lot of the competition.

Q. Can I switch careers to AppSec without having a technical background? What are some things I would need to know?

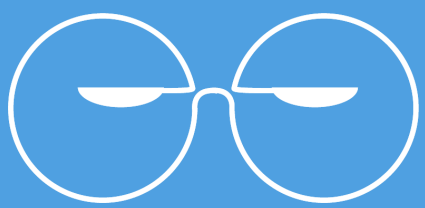
Yes you can!

One of the hardest jobs - and, in my opinion, harder than finding/learning secure code - is training and motivating developers to fix security vulnerabilities in the code, and sometimes even explaining why a security vulnerability should be fixed to avoid compromise.

A non-technical person with good understanding of human psychology and how to motivate people to do the right thing when it comes to fixing security bugs can be a great asset to a technical Application Security team.

- Ashish Rajan, Co-Founder of Kaizenteq & Host of Cloud Security Podcast

SWITCHING CAREERS ISN'T AS HARD AS YOU THOUGHT



I know what you might be thinking: you're already a developer, or an IT professional, or maybe none of those! Switching careers can be pretty scary, especially if you don't have a ton of prior experience in that field. But it's not as daunting a proposition as it might seem to be at first.

For starters, there's a lot of scope for a wide variety of career paths for someone getting into AppSec today. You're not restricted just to pen-testing and hacking anymore. In fact, one of the most highly-valued skills of an AppSec professional is the ability to communicate security risk to non-technical people. It can range from teaching developers how vulnerabilities crop up in insecure code, to demonstrating the business impact of security weaknesses to executives.

Skills a developer can use

You're also looking at helping teams achieve DevSecOps, where secure engineering practices are integrated seamlessly into a DevOps pipeline. This is the ideal jumping-off point for a lot of developers into security, because they can directly apply their knowledge of building apps in an agile pipeline to figuring out implementing security measures in the process.

Take automation for example. Automation is the cornerstone of any sophisticated, modern DevOps pipeline. It's critical for companies that want to scale up their development efforts without sacrificing speed. Continuous Integration and Delivery (CI/CD) is one of the most sought-after skills in AppSec engineers, according to Indeed.com.

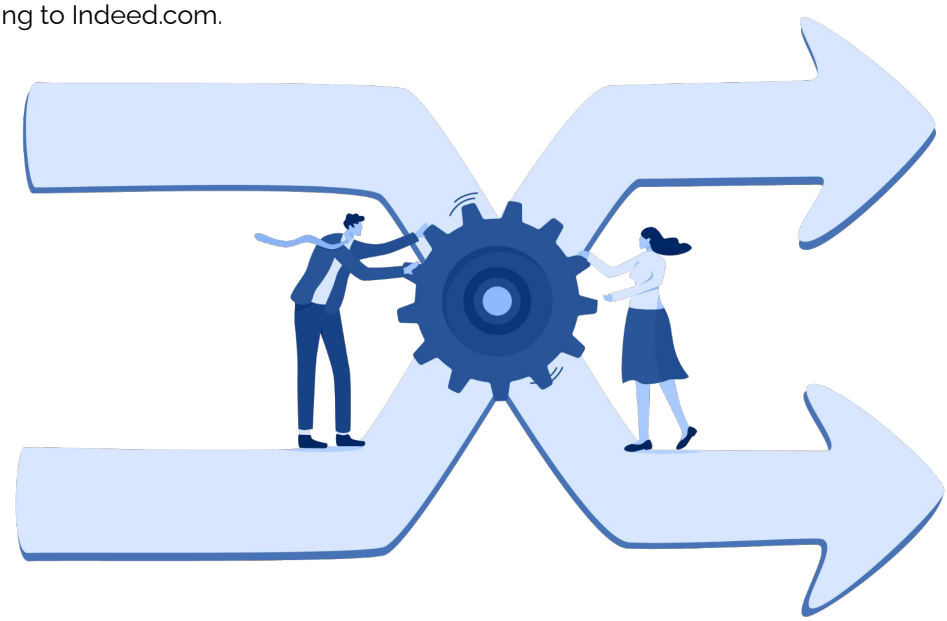
Be at the bleeding-edge of security

If that doesn't sound exciting enough for you, you could always try your hand at the *really* cutting-edge side of AppSec: Containers, Kubernetes, and Cloud Security. This is where it's all heading. A decentralized network of rapidly scalable cloud-based technologies that have all but spelled an end to the era of unwieldy monolithic apps.

Security for containers, Kubernetes, and cloud-native apps pose some of the most unique challenges that we've seen in AppSec in years. As more apps and data head for the cloud, companies are going to need more and more people to help secure all of it. That's where you'll come in.

As these emerging domains of product engineering go more mainstream, the technologies will continue to evolve and change at an unprecedented pace. Innovations are happening on a constant basis, especially with the runaway popularity of technologies like generative AI. To keep pace with the industry is anything but easy, and getting ahead is even harder. But the rewards for bringing your A-game are totally worth it.

Today, security engineers who can work on AWS, Azure, Kubernetes, and other platforms are some of the most valuable in the industry. You can be sure that if you bring the goods, there's a spot for you on their team. Trust us when we say: staying ahead of the curve is *always* a good thing.



Q. What's the first thing you'd tell someone interested in a career in AppSec?

For security professionals who want to explore the world of application security, I think it is very important that they have an appreciation for what developers go through as software is written and deployed via the software development lifecycle (SDLC).

There really is no excuse for any AppSec professional to not have the basic understanding of how applications are built and deployed. Pick a language that appeals to you, jump right in, and take some courses on how to write your first application.

If you can honestly sit down with a developer and say, "I may not be able to program as well as you, but I understand the processes you go through in order to deploy our software", you'll be able to empathize with the development team, and even get a tad bit of street cred from developers as you learn how to conduct code reviews, interpret static analysis results, and identify vulnerabilities that can be remediated long before production.

- Mark Willis, CISO, Bluescape

There's never been a better time to get into AppSec

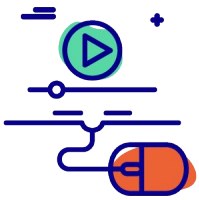
Application Security has only just begun to step out of the shadow of its bigger cousins in development, and we're only now seeing how absolutely indispensable it is for the kind of cloud and software-centric lives we're leading today.

If you're looking for a career in a field that's seeing a meteoric rise in demand and has no chance of going obsolete for a long, long time...well, this is it, folks.

AppSecEngineer is designed to give you everything you need to kickstart your AppSec career. Some of our courses in cutting-edge fields of AppSec like Kubernetes, Cloud Security, and DevSecOps can't be found anywhere else.

Learn secure coding in over 8 languages, and test your skills with hundreds of Challenges. Implement everything you learn in our hands-on labs and cyber ranges, and practice until you've mastered it.

You've come to the right place, at the right time. The only way to go now is forward.



Courses

Playgrounds

Challenges

Community

Become an AppSecEngineer