



Best Practices for Application Security

10 Ways to Protect Your Cloud, Mobile
and Web Apps from Hacker Attacks



Introduction

As the number of websites reaches over 255M and Internet users reach 2B, hackers continue to relentlessly attack at Cloud, Mobile and Web applications. Exploiting SQL Injection, Cross-Site Scripting, Session Hijacking, Weak Passwords, and other vulnerabilities, hackers are targeting application vulnerabilities. No organization is safe. Universities, banks, government agencies, retailers, high-tech companies, and social networking sites like Twitter and Facebook have all been victims of repeated attacks. Organizations have lost billions of dollars because of these breaches. Hactivism and cyber terrorism have become mainstream and the number of people behind them is growing.

In spite of these breaches, most corporations are doing very little to secure their Cloud, Mobile and Web applications. With network infrastructure pretty secure, albeit not perfect, hackers are putting their efforts toward going after the weakest link – Cloud, Mobile and Web applications. Many application vulnerabilities have a public exploit and even when patches are available, most companies still haven't deployed these patches.

People have good intentions, but the task of securing applications can seem daunting and cause them to delay patch initiatives. The problem is that these vulnerabilities in Cloud, Mobile and Web applications represent serious risk. In a study conducted by the Ponemon Institute, 72 percent of respondents test less than 10 percent of their applications, even though 73 percent admitted that they have been hacked at least once in the last 24 months.

What You Can Do

Following are 10 Cloud, Mobile and Web application security best practices. These are all important and not necessarily in any specific order.

1. Know your apps

We find that in a lot of cases companies don't even know how many Cloud, Mobile and Web applications they have or where they all are. Maintaining an inventory of your applications is important. You'd be surprised by how many rogue applications are out there. There are many solutions available to locate your applications.

2. Prioritize your apps

Not all apps are created equal. Once you know what apps you have, you should categorize them as critical (external facing with customer information), serious (external or internal containing some sensitive information), and normal (less exposure). You still need to have a plan to test them all, but categorization allows you to test them at optimal levels. For example, you can test the most critical applications with a full robust suite of attacks, serious ones with some common attacks, and the normal ones with a few basic tests.

3. Build awareness internally

Many of your employees have no clue what application security means. There are many resources to educate the various constituents within an organization. In many of the awareness training sessions we have done, we find that most employees in the information security group are at least somewhat knowledgeable about these issues. But, once you go beyond that to developers, QA, line of business managers and executives, the knowledge drops quickly.

4. Bust those myths

You should bust some of the myths around application security. For example, SSL does not protect you from hackers exploiting your web vulnerabilities and neither does a network firewall or IDS. Once people understand this, be aware of the buzz word vendors. Many of them say they can detect application security vulnerabilities even though their solutions are focused on a completely different set of problems.



5. Create a plan

You need to have an application security plan that takes into account identifying application risk and what to do once vulnerabilities are detected – block and/or fix. The plan should consist of your goals (compliance, brand protection, not getting fired, etc.), which apps you want to secure first, how are you going to test them (manual testing, using a managed service provider, using on-premise software, using a cloud solution, etc.), who should be involved in the process on an ongoing basis, and how much it would cost. Having a solid plan can help you justify the cost of ongoing protection of your organization's most important information assets.

6. Use a quantitative score for prioritization of vulnerabilities

Assuming you have the budget and you have started testing your applications for vulnerabilities, you will find that almost every application will have hundreds of vulnerabilities. This can be overwhelming and demoralizing. But if you prioritize these vulnerabilities based on some kind of quantitative score, the task becomes much more manageable for InfoSec and for development.

7. Interim protection

Vulnerabilities typically don't get fixed overnight. With developers already under pressure to get their Cloud, Mobiles and Web applications out on time, they have to make time for security. Until you fix these vulnerabilities, you have to protect your infrastructure. You can do this by configuring your web application firewalls (WAF) for specific vulnerabilities and by removing some functionality.

8. Don't forget production applications

Most people focus only on applications that are going through the development lifecycle with new code or changes to an existing application. And, yes it's important to test those. However, majority of your apps are already in production and could be seriously vulnerable. You can't afford to wait for the next set of changes to test for vulnerabilities.

9. Celebrate

If you don't celebrate your small wins, your team will feel de-moralized. After each application you secure with no critical vulnerabilities, celebrate. For passing a compliance audit, celebrate. For doing better than other business units, celebrate.

10. Test continuously

There are hundreds of new application vulnerabilities every month. You have to use a continuous testing process to detect new vulnerabilities. If you don't follow a continuous process, your applications will be at risk.

Trends show that attacks on Cloud, Mobile and Web applications are increasing in frequency and sophistication. Hacking is a lucrative career and these applications are an easy target as they offer an easy point of entry. Take some easy steps to reduce your application risk by eliminating known application vulnerabilities. With so many applications to choose from, hackers will seek the path of least resistance – don't make that your Cloud, Mobile and Web applications.



About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.

Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic’s security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic’s expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic’s security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.