



# Application security highlights from the 2015 HP Security Research Cyber Risk Report

Misused application security features trouble both the Web and mobile applications



**86%**  
Web applications with issues involving **authentication, access control, and confidentiality**



**72%**  
Last year's rate

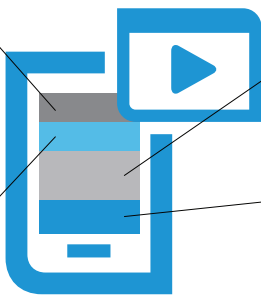


**97%**  
Mobile applications affected by these issues

Mobile applications have unique security issues

**80%**  
of mobile applications unintentionally reveal potential benefits to malicious attackers

**71%**  
store data in an insecure manner



**66%**  
don't protect data via encrypted communication or other means

**31%**  
can reveal geolocation

Fundamental application security errors in coding are still occurring

Appsec vulnerabilities also exist outside the application code



**52%**  
Web applications experience issues with input validation, including cross-site scripting, SQL injection, and other vulnerabilities

**48%**  
Mobile applications with input validation vulnerabilities



**82%**  
Web applications with vulnerabilities related to server misconfiguration, improper file settings, outdated software versions, and other issues of insecure deployment and security testing.



**70%**  
Mobile applications impacted by these application security issues



Even perfectly coded software can be dangerously vulnerable when misconfigured

Critical web security vulnerabilities impact almost half of all Web applications

Web applications:



**48%**  
have cross-frame scripting



**37%**  
have cross-site scripting



**47%**  
have unprotected file issues due to Web server misconfigurations

Newer technologies create new avenues of attack



The Internet of Things (IoT) expands the attack surface

**23%**

Developers planning work on connected devices within the next six months

Conclusions

- ✓ Applications are still vulnerable to well-known attacks.
- ✓ Vulnerabilities allowing unauthorized access to files and directories are prevalent.
- ✓ Consider liabilities related to application deployment along with code-based vulnerabilities.
- ✓ Organizations that systematically perform software security testing significantly reduce risk.
- ✓ A layered approach to mobile and web application security provides much more assurance than a single technology.

Recommendations



**Assess**  
Create an application security gate to assess all applications before they go into production.



**Assure**  
Implement an SSA program that measures risk and improvement, incorporates threat intelligence, and enforces compliance.



**Protect**  
Monitor and protect high-risk applications in production.

See how companies are building Software Security Assurance (SSA) programs at: [hp.com/go/fortifyssa](http://hp.com/go/fortifyssa)

