Is your web app under attack?

Web applications often process sensitive information, including credit cards, personally identifiable information and proprietary data. Applications are a vital business function, but with that functionality comes risk.

Web application attacks are the leading form of cyber crime and are responsible for 29.5% of all breaches.[1]

58% of IT professionals surveyed report that they are now seeing more attacks on application layers than on the servers.[2]

How many apps are not being tested?

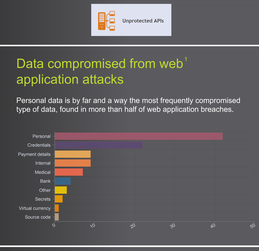
83% of organizations have released code before testing or resolving security issues.[3]

The main reasons for not testing enough[4]

- Uncertainty over how much to test
- Senior managers do not see the benefit
- Limited budget
- Limited expertise

Average vulnerabilities per site[5]

Average vulnerabilities per site varies from 5 (in Manufacturing) to 32 (in IT). As the chart indicates, the Retail, Education and IT industries suffer the highest number of vulnerabilities – including serious vulnerabilities – of any other industry studied.



OWASP top 10 most critical web application security flaws

Research has found that as many as 60 percent of applications do not pass the OWASP top 10 when first assessed.

60%

- Injection
- Broken authentication
- Cross-site scripting
- Broken access control
- Security misconfiguration
- Sensitive data exposure
- Insufficient attack protection
- Cross-site request forgery
- Using components with known vulnerabilities
- Unprotected APIs

Data compromised from web application attacks[1]

Personal data is by far and away the most frequently compromised type of data, found in more than half of web application breaches.

Average time to detect flaws[5]

Critical	High	Medium	Low
316 DAYS	507 DAYS	463 DAYS	270 DAYS

Examples of breaches[6]

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

Equifax failed to patch its Web applications against a flaw in Apache Struts framework, which resulted in the breach of personal data of nearly half of the US population (143 million people).

Data breach exposes US workers with high-level security clearance

In September 2017, files containing personal information on US citizens who have classified security clearances were leaked. A cache of around 9,400 job application files were held on an Amazon Web Services S3 storage server that required no password to access.

Wordpress blogs defaced in hack attacks

In February 2017, tens of thousands of WordPress blogs had been attacked and defaced by criminal hackers after a privilege escalation vulnerability was disclosed. Multiple public exploits were shared and posted online, fuelling over 1.5 million attacks.

An Instagram hack hit millions of accounts

In August 2017, six million Instagram accounts were exposed online after a flaw in the password reset option in the Instagram mobile app exposed mobile phone numbers and email addresses.

Web application penetration testing

Web application security testing should be part of an organization's risk assessment phase before launching live services, and repeated on a regular basis to deal with emerging and new vulnerabilities.

- User authentication testing performed to verify accounts cannot compromise data.
- Analyses web applications for flaws and vulnerabilities, such as Cross-site Scripting (XSS).
- Securely configure web browsers and identify features that can cause vulnerabilities.
- Safeguard web server security and database server security.

Choose which test you need

At IT Governance, we offer two levels of penetration test to meet your budget and technical requirements:

Level 1

Identifies the vulnerabilities that leave your IT exposed. Combining a series of manual assessments with automated scans, our team will assess the extent of your system or network's vulnerabilities, allowing you to evaluate your security posture and make more accurate budgetary decisions.

Purchase our quick and fixed-priced penetration tests online.

Buy online

Level 2

Involves attempting to exploit the identified vulnerabilities to see whether it is possible to access your assets and resources. This more thorough assessment of your security posture enables you to make more accurate decisions about investing in securing your business critical systems.

Please contact us for further information.

Contact us

For more penetration testing information or to request a quote, visit our website by clicking here.

References

1. Data Breach Investigations Report, Verizon (2017)
2. Five Lessons from an Application Security Pro, Veracode (2017)
3. State of Software Security, Veracode (2017)
4. The Cost of Web Application Attacks, Ponemon Institute (June, 2015)
5. Web applications Security Statistics Report, Whitehat Security (2016)
6. How Penetration Testing Can Prevent Web Application Attacks, IT Governance Blog, (October 2017)