Penetration testing for web apps

AEC

Avoid application compromise and data leaks

During web application security testing, our tasks mainly focus on manual activities supported by the results from automated tools. This approach can reveal a broader spectrum of vulnerabilities that automated tests cannot, especially in business logic, complex communication links, authorization mechanisms or the possibility of exposing publicly available sensitive data. We have many years of experience with both simple static portals and extensive complex systems.

aec-security.eu

Penetration tests and vulnerability scans

One of the things the tests we conduct are aimed at is identifying security weaknesses that may occur within the configuration, during data processing processes, or through incorrect implementation. The tests also include checking the security of all functionalities, authentication and authorization mechanisms, business logic, how sensitive information is handled and other areas.

Penetration testing mainly involves the following steps:

- collecting available information,
- checking secure communication settings (e.g. using HTTPS, SSL),
- verifying the security of critical data flows,
- leaks of sensitive information,
- the possibility of misusing the app in an unauthorized manner and an attempt to take control of a legitimate user's account,
- checking the inputs entered by the user,
- the security of the technologies on which the systems are built (operating systems, web, application and database servers) and securely integrating them into the rest of the infrastructure,
- the possibility of an attacker abusing the available technology in the application and feasible attacks on the accounts/sessions of legitimate clients,
- non-destructive exploitation of generally known/found vulnerabilities, and more.

Penetration testing for web apps

When carrying out penetration tests, we rely primarily on the current OWASP Testing Guide methodology, using the techniques listed below.

Information Gathering

- a phase aimed at collating as much information as possible,
- using freely available tools (search engines, scanners, simple HTTP requests or specially adapted requests),
- leaking information, for example in the form of error messages or notifications about specific versions and the technologies used.

Configuration and Deploy Management Testing

- topology infrastructure and architecture analysis,
- a survey of the technical information such as source code, the HTTP methods enabled, administrative functionality, authentication methods and infrastructure configuration information.

Identity Management Testing

- verifying the mechanism for managing users and their roles,
- testing the parameters, identifying security flaws, vulnerabilities leading to direct compromise of user accounts.

Authentication Testing

- analysis of the authentication process' functionality and attempts to get round it.

Authorization Testing

- finding ways to bypass authorization rules and user rights settings,
- looking for ways to escalate allocated privileges.

Session Management Testing

- analysis of the possibility of stealing an authenticated user session,
- finding a possibility and carrying out a Man-in-the-Middle and similar attacks.

Data Validation Testing

- one of the most important parts of penetration testing - it tests the application's resistance to attacks such as SQL/Code Injection, Cross-Site Scripting, Local File Inclusion and others.

Error Handling Testing

- tests for leakage of sensitive information from often very detailed error messages,
- generation of non-standard inputs, both in size and content.

Cryptography Testing

- checking whether the application accepts outdated, defunct or completely inappropriate (no) cryptographic mechanisms for the given purpose.

Business Logic Testing

- probing all workflow functionalities and seeking a possibility to misuse them to carry out activities that are not in accordance with the given application's usage options.

Client Side Testing

- verifying how effective the application's mechanisms are at protecting users from specialised attacks that directly target the user and their browser,
- testing various kinds of client scripting language injections and manipulating the parameters managed by the browser.

Our strengths

- We are an established Czech security company that has been successfully operating on the market for over 30 years.
- We have more than 20 years of experience in the field of web application and platform security.
- We have the largest team of ethical hackers in the Czech Republic, one that is made up of more than 15 of our own employees.
- We hold CEH, eMAPT, CISSP, OSCP, OSCE and many other certifications.
- Our team is composed of specialists with experience from hundreds of web projects.
- We run our own hacking lab where we share our knowledge with the community, that being both in the design, architecture and the actual use and management of web applications.
- We listen to our clients and adapt our tests to their needs and the time they have available.
- We follow modern trends in web security and technology.
- We emphasize a manual approach whilst testing, which leads to more errors being detected, especially in business logic applications.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283