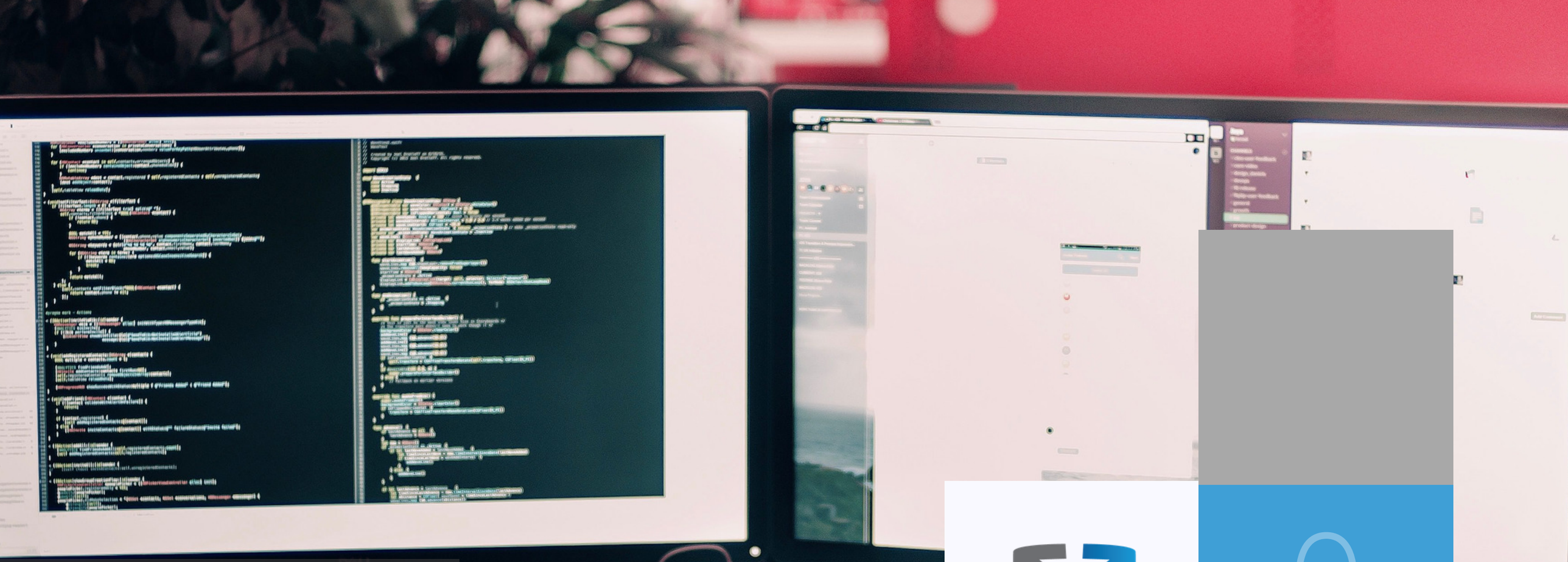

IBSS
Case Study

Penetration Testing

IBSS INC.
INTERNET BIOMETRIC SECURITY SYSTEMS

"Assess the security on the implemented authentication mechanism and perform an analysis on the current security state of their portal".

INDEX

- The challenge
- Requirements
- Process
- Results

Get in touch:

Saltillo, Mx - Eagle Pass, US

US 512 487 7554 info@clickittech.com

ClickIT SMART TECHNOLOGIES

The Blade platform is the easiest way for digital currency companies to enable real-currency payments and it’s becoming the fastest and most efficient way to handle traditional consumer payments & settlement.

- Security.
- Authentication.
- Deep analysis.

The Challenge

IBSS has an online webmail portal for which there's a proprietary authentication log in mechanism via voice and/or face recognition. IBSS wanted to assess the security on the implemented authentication mechanism as well as to perform a deep analysis on the current security state of the full portal.

Requirements

IBSS had the requirement to perform a Penetration Testing against the webmail portal in order to detect potential security vulnerabilities on their authentication log in mechanism as well as in the whole portal so that those could be mitigated as soon as possible, preventing further potential cyberattacks to the infrastructure/application and/or customer data.

The Process

The Penetration Testing is a time-bound strategy to actively help top management, system administrators and application owners to know and understand the actual security status of a certain application. The results presented are a picture of the application configuration at the time of the security assessment during the period of time where it was executed. A Penetration Testing was performed using black-box and white-box techniques, which means that available public information was used to attack the application as well as private data (defined and provided by the customer in order to deep-dive and fast-drive the security assessment). This is the most realistic approach since that would be the scenario for an external attacker in a real world situation.

The analysis always can be split into Application and Infrastructure. The Application side showed an overall Low Security level since some of the vulnerabilities found have a high risk level and high impact on the application and user’s information. It is evident that security programming and configuration were done following secure coding implementations, best practices & guidelines since several protection mechanisms against well-known attacks were found in various modules of the application, even though there are some other vulnerabilities that in specific scenarios are exploitable in order to take other user’s sessions, modify information without authorization and gain privileged access.On the other hand, the Infrastructure architecture reflects a High Security Level; configurations have been applied in order to harden the server, not other unnecessary services were found. The security assessment was performed by covering the following:

- Vulnerability Assessment:
  Discovery and vulnerability scanning to identify security vulnerabilities within the context of a LAMP environment.
- Security Assessment:
  Build upon Vulnerability Assessment by adding manual verification to confirm Proof of Concept.
- Penetration Testing:
  Simulate an attack by a malicious party. Using this approach will result in an understanding of the ability of an attacker to potentially gain access to confidential information, affect data integrity or availability of a service.

Technologies

- ZAP
- W3AF
- Burp
- Metasploit
- Kali
- NeXpose
- Nmap
- Snort
- Paros
- Fiddler
- Putty
- open source

Results

IBSS was able to identify several vulnerabilities* and their type (Application and Infrastructure) with defined risk levels (Informational, Low, Medium, High, Critical, Hazardous) in order to prioritize those and assign the required efforts to address them. ClickIT helped IBSS to reduce the risk of being attacked since we provided a wide range of vulnerability metadata in the final Penetration Testing report, such as the vulnerability list, vulnerability definitions, impacts, worst-case scenarios, URL details, steps to reproduce each vulnerability (screenshots included) and remediation recommendations.

* For security reasons and confidentiality, ClickIT is not allowed to disclose any details on the security state of IBSS.
** The risk of being attacked is always on; the perspective of being vulnerable can be reduced significantly by performing Vulnerability Assessments, security Assessments, and/or Penetration Testing in a proactive and regular basis.

About Us

Development

Web and Mobile Development for Ecommerce sites, Startups, Mobile and SaaS applications.

Security

Hardening and malware removal. Ask for a security assessment, ethical hacking and penetration testing.

DevOps

Continuous integration and Accelerate your Development productivity with IT automation.

Migrations

Migrate your aplication to the Cloud, or move your site to the hosting that suits you best.

Cloud Computing

Integrate your online business to the cloud today. Get the benefits that cloud computing can give you.

Optimization

Accelerate your application and CMS using caching layers, CDN technologies and tuning your LEMP services.

ClickIT
SMART TECHNOLOGIES

Need More Information?

Our Blog

Our Work