AKIMBOCORE

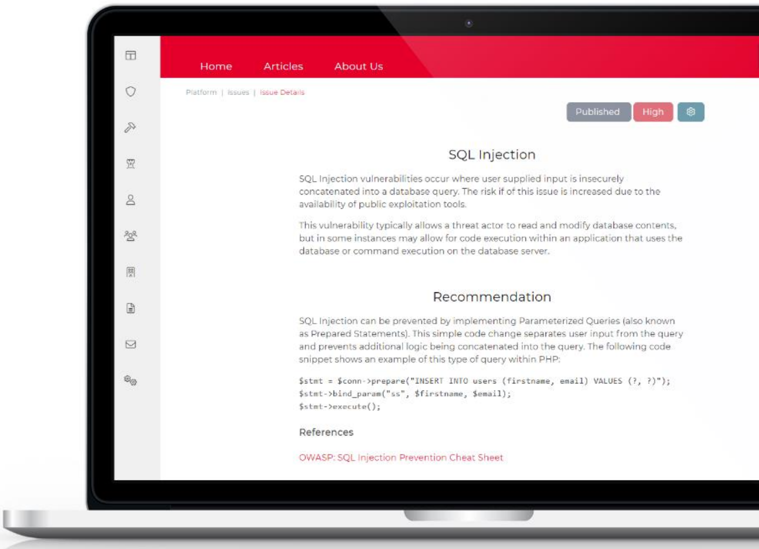
Vulnerability Management Platform

Keeping track of all the information relating to your organisation's security stance can be difficult, additionally securely sharing and discussing that information with your team and external partners can be frustrating. Our vulnerability management platform is a powerful and flexible web platform that allows you to do just that.

Our platform allows you to create, import, and manage information about assets and their security vulnerabilities easily from any device. It can also notify you when an team member or an external security provider publishes a new vulnerability on your systems, so that you're informed quickly about developments.

Whether you're using an Akimbo Core security testing service, a third-party service, or handling everything internally – our platform is designed to be easy to use and secure.

With multi-factor authentication on login, transport layer security to protect everything in transit, and a granular permissions model to control who can view or edit things.



SQL Injection

SQL Injection vulnerabilities occur where user supplied input is insecurely concatenated into a database query. The risk if of this issue is increased due to the availability of public exploitation tools.

This vulnerability typically allows a threat actor to read and modify database contents, but in some instances may allow for code execution within an application that uses the database or command execution on the database server.

Recommendation

SQL Injection can be prevented by implementing Parameterized Queries (also known as Prepared Statements). This simple code change separates user input from the query and prevents additional logic being concatenated into the query. The following code snippet shows an example of this type of query within PHP:

```
$stmt = $conn->prepare("INSERT INTO users (firstname, email) VALUES (?, ?)");
$stmt->bind_param("ss", $firstname, $email);
$stmt->execute();
```

References

OWASP: SQL Injection Prevention Cheat Sheet

Security Testing

Our platform-first approach to security reporting gives you a continuously updated view of your organisation's security stance. If you're using our continuous security testing service then, we continuously update your organisation's risk via our web platform. With work conducted, new issues found, and where you should focus your attention for maximum effect.

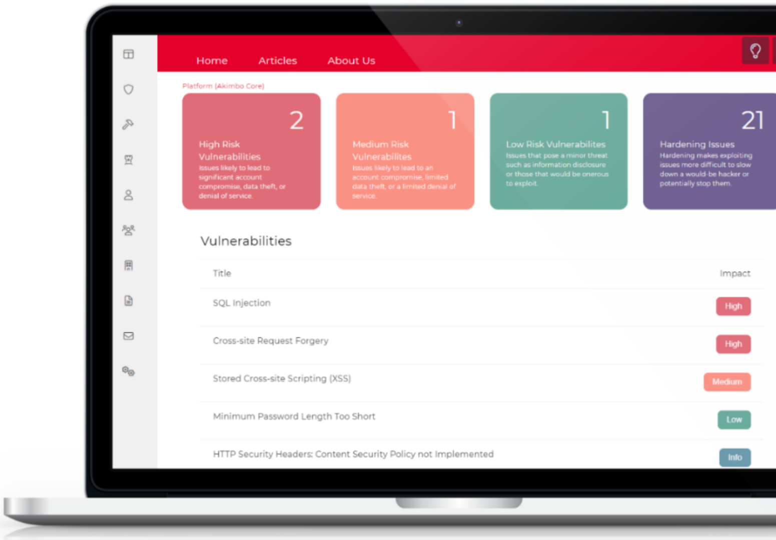
You can view vulnerabilities as soon as they are confirmed. You can communicate directly with the testing team, such as to request additional information or to request a retest of a remediated issue. You can view a high-level report of the state of your systems, ideal for management meetings - or you can drill down into the technical detail needed to remediate a complex issue.

You can view a high-level report of the state of your systems, ideal for management meetings – or you can drill down into the technical detail needed to remediate a complex issue.

Our Dashboard

Our platform gives you a single location to track vulnerabilities, assets, hardening issues and more.

For offensive teams it gives a list of in-scope systems for security testing. For defensive teams it gives a list of issues to be remediated and allows you to communicate within the team to collaborate and schedule remediation activities. For security leaders it gives an overview of security improvements over time and the current risk level today.



Platform (Akimbo Core)

2 High Risk Vulnerabilities
Issues likely to lead to significant account compromise, data theft, or denial of service.

1 Medium Risk Vulnerabilites
Issues likely to lead to an account compromise, limited data theft, or a limited denial of service.

1 Low Risk Vulnerabilites
Issues that pose a minor threat such as information disclosure or those that would be onerous to exploit.

21 Hardening Issues
Hardening makes exploiting issues more difficult to slow down a would-be hacker or potentially stop them.

Vulnerabilities

Title	Impact
SQL Injection	High
Cross-site Request Forgery	High
Stored Cross-site Scripting (XSS)	Medium
Minimum Password Length Too Short	Low
HTTP Security Headers: Content Security Policy not Implemented	Info

ASSIGNING TASKS

There’s no “I” in team, so we’ve developed our platform to work well with teams of any size.

You can assign vulnerabilities to specific staff for remediation, message team members to discuss issues, and securely share issue details with those in your organisation that need to know.

NOTIFICATIONS

With new security issues being found constantly, it’s difficult to keep track of them all or get any other work done.

That’s why we’ve set our platform up with configurable notifications, so that you can tell us what “critical” means to your business, and we’ll make sure to alert you to those issues without overloading you about minor details.

Continuous Security Testing

If you're looking for a security testing methodology that allows for your assets to be continuously tested for weaknesses - we also offer a Continuous Security Testing service. We use Penetration Testing techniques to continuously assess your external risk profile, alerting you to changes on your attack surface or the threat landscape. Combining this with bespoke automation to strike a balance between frequency and depth of testing.

OUR APPROACH

Akimbo Core began working in 2019, to address the weaknesses in the traditional approach to security testing. With companies relying on approaches that lead to a long mean- time-to-detection and that don’t take the whole organisational context into account — we wanted to do something different.

That’s why we take a platform-first approach to security and continuous security testing.

GET IN TOUCH

0161 327 1941
info@akimbocore.com
@AkimboCore