Web Server Hardening

Business Case Study and Report

While certain project details have been adapted to protect confidentiality, they reflect the knowledge, challenges, and approach we bring to every collaboration.

grow

Service area:
Cybersecurity

Client type:
Professional Services

Challenges and Objectives

Challenges

The client’s website, hosted on a cloud-based VPS, had never undergone a structured security review. There were concerns about potential exposure of sensitive contact forms, outdated software, and access control gaps. Without a dedicated IT team, they needed a practical, guided approach to hardening their environment.

Objectives

- Reduce the attack surface of the organization’s cloud-hosted web server
- Identify misconfigurations or vulnerabilities in the current setup
- Implement security best practices aligned with industry standards
- Document the process for internal knowledge and future audits
- Educate internal staff on secure hosting practices

Our Approach

We started with a security assessment using automated tools and manual inspection. Then, we defined a hardening checklist tailored to the client's environment (Ubuntu + Apache + WordPress), aligned with CIS Benchmarks and OWASP guidelines. Our process included:

01

Securing SSH access and enforcing strong authentication

02

Enabling firewalls and intrusion detection tools

03

Reviewing third-party plugin/code exposure in the CMS

Solution Highlights

Firewall rules (UFW) implemented to restrict traffic

Auto-updates for system packages and CMS core enabled

Plugins and themes purged to reduce unnecessary exposure

SSL configuration reviewed and improved (A+ on SSL Labs test)

Results

- Reduced server vulnerability score (from 61 to 91 using baseline tools)
- 80% decrease in unauthorized login attempts within 2 weeks
- Improved uptime monitoring and alert configuration
- First version of their “Server Security Handbook” completed

“We thought we needed a whole IT department to improve security.

Grow made it understandable and manageable.”

— Managing Partner

Before & After: Server Exposure

BEFORE

Score: 61/100

12 High-Risk Issues
SSL Grade: B
Unmonitored Attacks

3 Weeks

AFTER

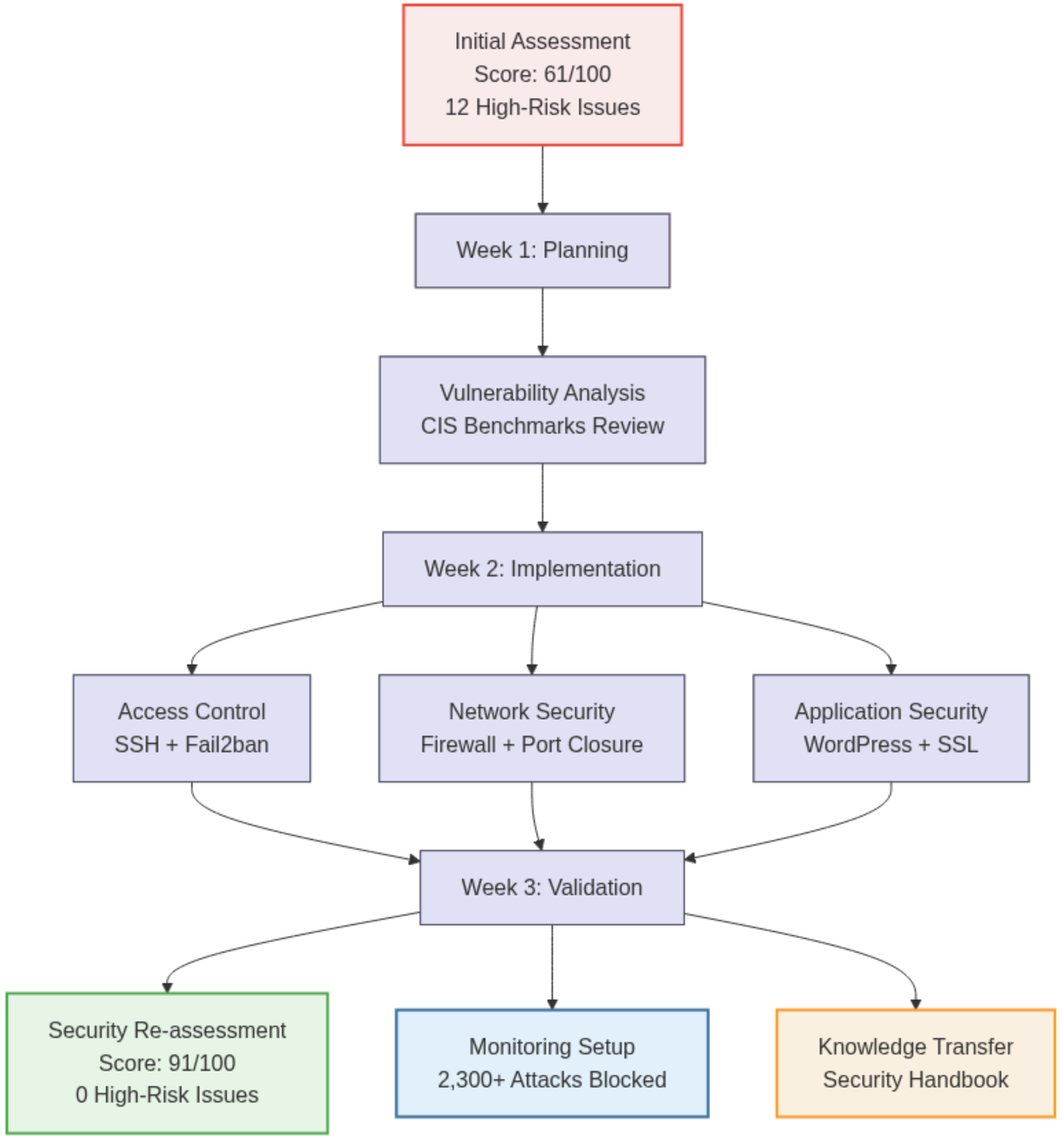
Score: 91/100

0 High-Risk Issues
SSL Grade: A+
2,300+ Attacks Blocked

Key Achievements

- ✓ 49% Security Score Improvement
- ✓ SSL Labs A+ Rating Achieved
- ✓ Team Trained + Security Handbook Delivered

grow's Approach



Get In Touch

Email

info@iniciativagrow.com

Social Media

@iniciativagrow

Call us

(+507) 6318-3683