UC-276

Akwaaba Web Server Security Project

IT 4893-W02 Capstone CRN83939 Cyber Team 1

Team: Cody Reese, Ron Southern, Ty Rogers, Jayland Vann, Taiyeb Choudhury

KENNESAW STATE UNIVERSITY

ABSTRACT & OUTCOMES

Our team engaged in a mock cybersecurity drill. Our objective was to take on the roll of cybersecurity consultants and to secure a mock business website. Afterwards, we were to engage in the active defense of our site from another team, while perpetuating attacks on that team's site.

Goals:

I. Secure a business website
II. Defend a site from cyber attack(s)
III. Perform a successful attack(s) on another team's website.

Outcomes:

I. Developed a comprehensive security policy
II. Documented site risks and vulnerabilities
III. Implemented security and configuration changes

PROJECT OUTLINE

Our team followed a regimented weekly schedule that focused on completing tasks in order to meet phase goals and this build towards a cohesive project and a secure site.

PHASE 1 – Analyze Business Site
- Perform Risk Assessment
- Propose Security Policy Plan
- Create Technical Plan

PHASE 2 – Secure Site
- Implement Security Changes
- Document activity within Change Log
- Deliver news w/ Implementation Plan

PHASE 3 – Defend and Attack
- Maintain Server Integrity
- Document attacks in Forensic Report
- Conduct Vulnerability Analysis

Gantt Chart: Task Breakdown

Project Name: Akwaaba Web Server Security
Report Date: 10/22/2022

Deliverable	Tasks	Completion %	Assigned To	28-Aug	4-Sep	11-Sep	18-Sep	25-Sep
				Milestone #1				
Project Plan	Setup Project Website	100%	Ron	5	5			
	Complete Gantt Chart	100%	Jayland		10	1		
	Draft Project Plan	100%	All		12			
	Finalize Project Plan	100%	Jayland		3	1		
Risk Analysis	Bring Site Online	100%	Jayland		0	2		
	Interrogate Servers	100%	All		0	10	15	
	Identify Open Ports	100%	Cody			4		
	Scrutinize User Account/Group	100%	Ty			4		
	General Vulnerability Check	100%	All			7.5	15	
	Conduct and Compile Research	100%	Ron			15	9	
	Finalize Risk Report	100%	Taiyeb			0	2	
Security Policy	Classify Systems & Data	100%	Ty				5	
	Classify User Accounts	100%	Cody				5	
	Determine Acceptable Use	100%	Ron				5	
	Determine Access Controls	100%	Taiyeb				4	
	Make Incident Response Plan	100%	Jayland				3	
Technical Plan	Research Security Solutions	100%	All				0	10
	Infrastucture Breakdown	100%	Ty					2
	Detail System Security Strategy	100%	Taiyeb					6
	Suggested Tech/Tools	100%	All					5
Milestone Meeting 1	Compile Document Info	100%	All					7
	Prepare Powerpoint	100%	All					7

Project Plan: Project Owner & Team

Roles	Name	Major responsibilities
Project owner	Donald Privitera	Provide project details, assist in directing work, grade milestones and final project.
Team leader	Jayland Vann	Organizing meetings. Informing team members of scheduling changes and delivery dates. Submitting group assignments.
Team members	Ron Southern	Capstone Project Website Upkeep
	Ty Rogers	Technical Tools and Strategies research; Documentation support
	Cody Reese	Technical Tools and Strategies research; Documentation support
	Taiyeb Choudhury	Develop Risk Assessment and Security Policy
Advisor / Instructor	Jack Zheng	Facilitate project progress; advise on project planning and management.

CONCLUSION

Security cannot be an afterthought. During the project there many times that we as team encountered an issue that could have been readily solved during the site's implementation. That's not to say that we encountered any problem that couldn't be solved, but if security had been an integral part of the planning phase of the server, there would not have a problem to begin with. Maintaining security should be a primary focus during the planning and implementation phase of any technical infrastructure project. With this mindset risk can be mitigated early on in project, and future headaches and late nights can be avoided. For our project, turnover is set to occur on November 20th. Deliverables are to include: a secure virtual machine and website, a full report on the entirety of the project, and all supporting documents created during the course of the project. Supporting documents include: Risk Assessment, Security Policy, Technical Plan, Implementation Plan, Change Log, Forensic Security Report, and Target Vulnerability Analysis.

CONTACT INFORMATION

Project Website
- https://sites.google.com/view/cs-capstone-team-1

Ron Southern
- Email: rsouthe2@students.kennesaw.edu

Taiyeb Choudhury
- Email: tchoud2@ students.kennesaw.edu

Ty Rogers
- Email: troger79@students.kennesaw.edu

Cody Reese
- Email:creese38@students.kennesaw.edu

Jayland Vann
- Email: jvann9@students.kennesaw.edu

RESULTS

DEFENSE

Vulnerability Testing Tools

Wappalyzer · OWASP Zed Attack Proxy · Nikto (a Practical Website Vulnerability Scanner) · NMAP.ORG · WPScan

Vulnerability and Risks

Vulnerable Login

I. Widespread reuse of passwords
II. User Credential Leak
III. No Captcha or 2FA
IV. Dictionary attack vulnerable

Enumeration Risks

I. Information on services and their versions available on site
II. Use of Xmlrpc allows for data gathering on user accounts

HTTP Security

I. HTTPS not utilized
II. Security Headers for XSS, Clickjack, MIME, and Request Forgery unset.

Other

I. Lack of IDS / IPS
II. Services not updated
III. No WAF for site
IV. Vulnerable to traffic-based attacks

System Classification

WordPress CMS: Earns its status due to well known default configurations, open Internet access and it's use of protected data

Apache Web Server: Vulnerable due to open requests from the Internet through unsecured channels.

RHEL OS: Open to external connections, but utilizes layered defense, firewall and password, to maintain integrity

MariaDB: Holds encrypted confidential information. Communicates with front-facing systems but remains strictly internal.

With Cybersecurity there are Do's, Don'ts, and D'OHs!

Server Changes

Login Changes
- Captcha added to all forms
- Custom Login URL
- Links to login disabled
- Login lockout enabled
- IP lockout enabled
- Complex, unique passwords created

Services Installed / Updated
- Installed IDS & IPS
- Services updated
- Installed Web Application Firewall
- Custom Plugin Installed

General Changes
- Xmlrpc disabled
- HTTP Security Headers utilized
- Browser directory listing disabled
- Access to some Web Server files removed

OFFENSE

Target Analysis

One of the foremost vulnerabilities that we found was in the enabled xmlrpc.php file. This file allows for remote management of a WordPress site through HTTP and XML encoded functions.

Brute Force Attack Functions
- system.multicall
- wp.getUsersBlogs

Mechanism
- Functions mutlicall and getUserBlogs used to perform mass login attempts

XSPA/Pingback DDOS Functions
- pingback.ping

Mechanism
- A self hosted server/ webhook/ vulnerable WordPress site can be leveraged as a vector to launch the attack

Penetration Toolkit

Burp Suite was used as a proxy to edit, test and send our forged HTTP requests to the target

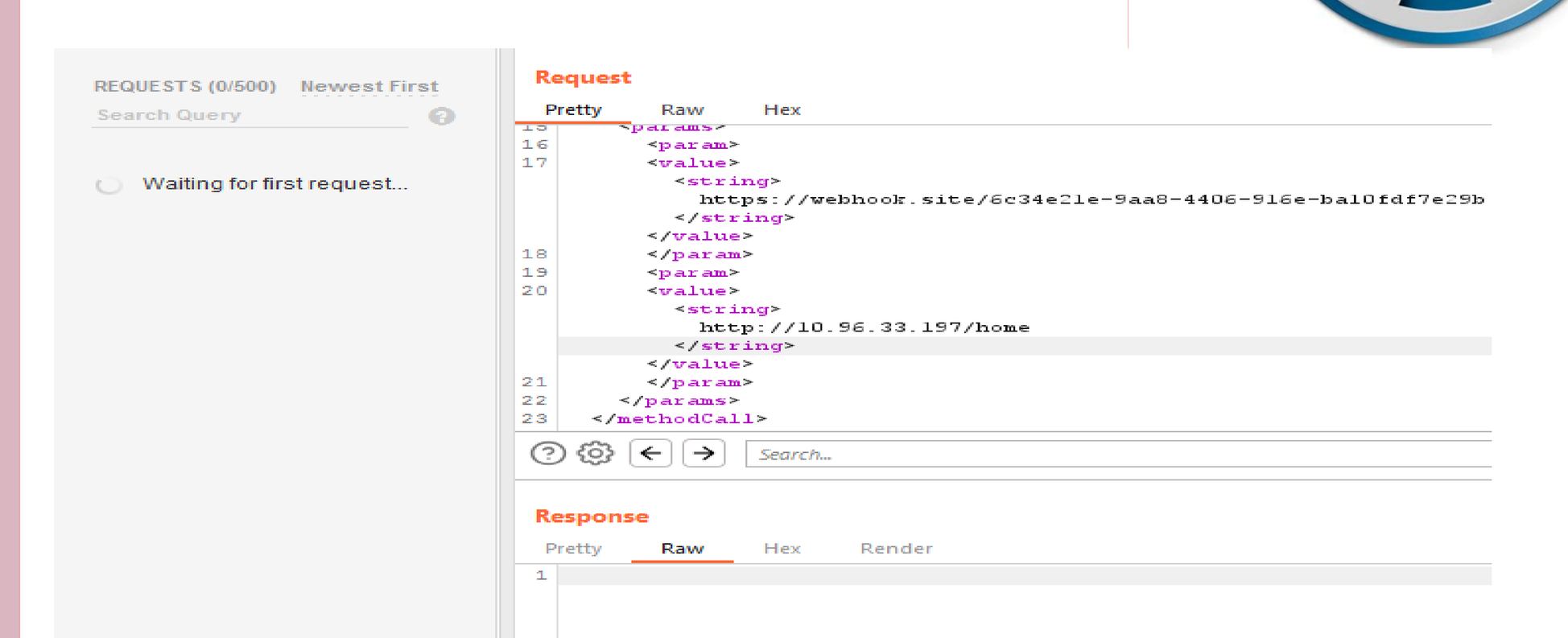
NEXT

During testing ngrok and socat were used together to create a self hosted server to receive returned pings from the target

NEXT

By utilizing the WP sites and posts of other teams we can amplify our potential DoS into a DDoS attack on our target.

Attack Execution



ATTACK FAILED

Why? We know the attack works when a faultCode of 0 wth no supplied faultString is returned. We couldn't get this to occur because we had issues getiting pingback responses from the target site to our server. We tried alternatives like Webhook.site and even tried a WordPress site we created but neither worked.