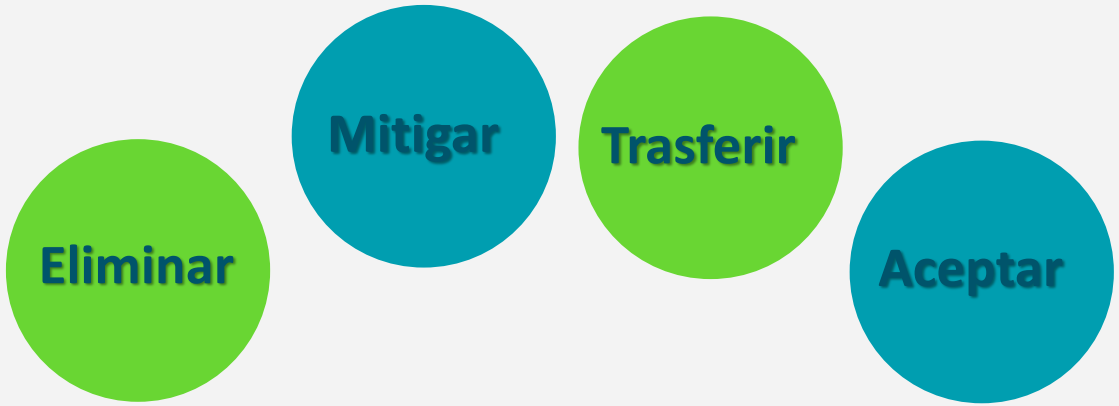
Estructura efectiva de reportes e impacto al negocio

El impacto al negocio se refiere a las consecuencias (tangibles y mensurables) que un evento o actividad puede tener sobre una empresa, como la pérdida de ingresos, el daño a la reputación o el aumento de gastos.

Riesgo = Amenaza x Vulnerabilidad x Activo

Riesgo = Probabilidad x Impacto



Likelihood severity occurs	Potential Severity Rating: Minor	Moderate	Significant	Catastrophic
Very Likely	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Unlikely	Very Low	Low	Moderate	High
Rare	Very Low	Very Low	Low	Moderate

IMPACTO != RIESGO

Una cadena de cines ofrece descuentos por reserva de grupo y tiene un máximo de quince asistentes antes de exigir un depósito. Los atacantes podrían modelar este flujo y probar si pueden reservar seiscientas butacas y todos los cines a la vez con unas pocas solicitudes, lo que provocaría una pérdida masiva de ingresos.

IMPACTO != RIESGO

- AMENAZA
- PROBABILIDAD
- ACTIVO
- IMPACTO
- RIESGO

IMPACTO != RIESGO

• AMENAZA	**Fraude y denegación de inventario.**
• PROBABILIDAD	**Alta — el flujo es fácil de modelar con herramientas de automatización**
• ACTIVO	**Sistema de reservas en línea de la cadena de cines**
• IMPACTO	**Alto - Económico**: pérdida de ingresos por bloqueo de cientos de asientos no pagados. **Operativo**: indisponibilidad de reservas reales por clientes legítimos. **Reputacional**: pérdida de confianza del público y potencial cobertura negativa en medios.
• RIESGO	**Alto / Crítico** — la combinación de alta probabilidad y alto impacto genera un riesgo crítico.

IMPACTO != RIESGO

La confianza ciega de una aplicación en los frameworks puede generar consultas que aún sean vulnerables (por ejemplo, Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE
custID='" + request.getParameter("id") + "'");
```

En ambos casos, el atacante modifica el valor del parámetro 'id' en su navegador para enviar: `' UNION SLEEP(10);--`. Por ejemplo:

```
http://example.com/app/accountView?id=' UNION SELECT SLEEP(10);--
```

Esto cambia el significado de ambas consultas para devolver todos los registros de la tabla de cuentas.

IMPACTO != RIESGO

- AMENAZA
- PROBABILIDAD
- ACTIVO
- IMPACTO
- RIESGO

IMPACTO != RIESGO

- AMENAZA
- PROBABILIDAD
- ACTIVO
- IMPACTO
- RIESGO

Alta — el patrón de concatenar request.getParameter("id") en una cadena de consulta es una vulnerabilidad común y trivial de explotar con acceso a la URL.

Reporte Ejecutivo

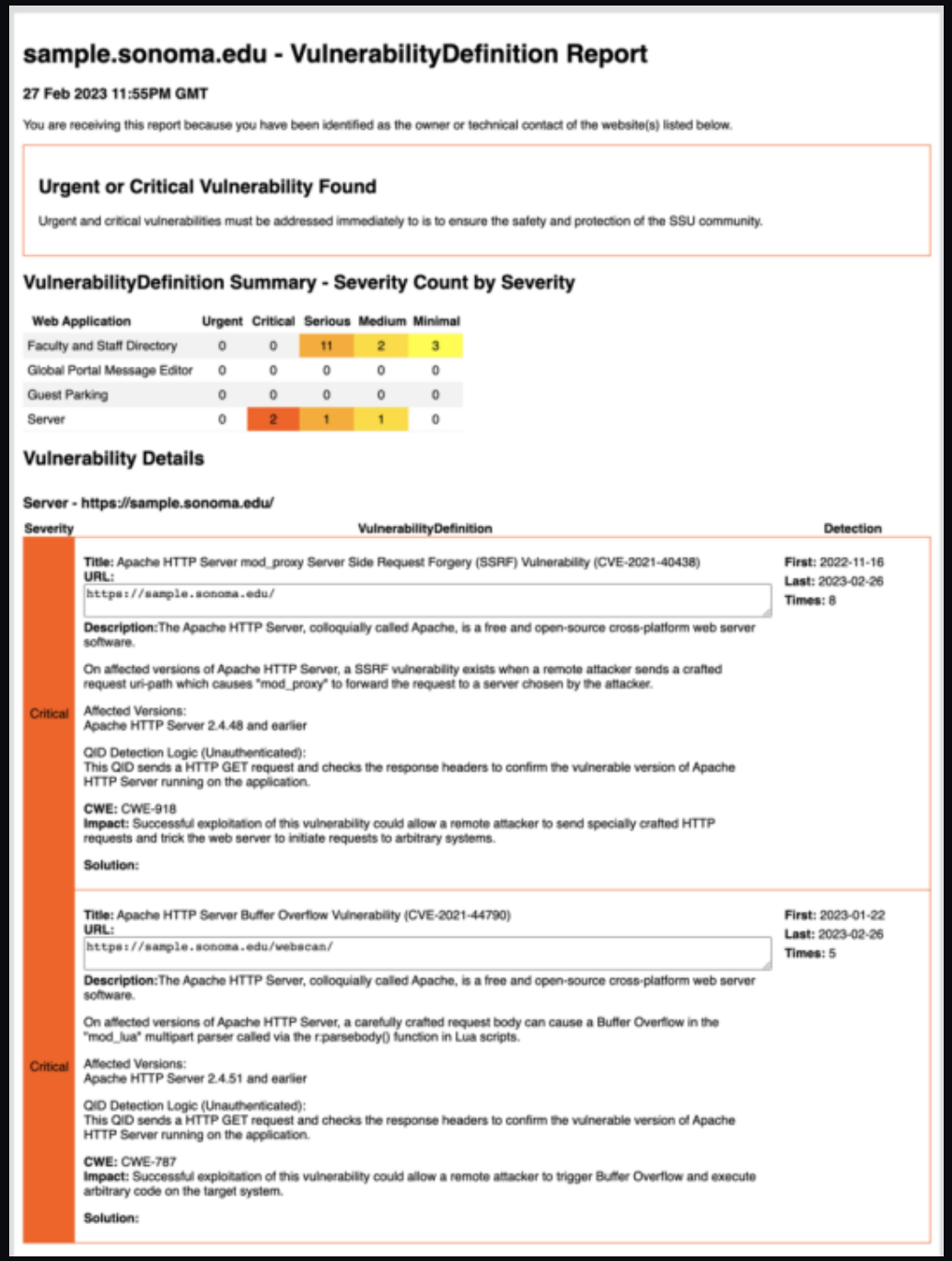
Report prepared by:

AWESOME CONSULTING CO.

Project	ABC Pentest
Date	June 1 2020 - June 10 2020
Test Type	Penetration Test
Team	Leonard McCoy, James Kirk

Node	Issue	Severity
1.1.1.1	Blind SQL Injection	Critical
10.0.0.1	.NET assemblies were not obfuscated	Critical
10.0.0.2	Apache Web Server ETag Header Information Disclosure Weakness	Medium
10.0.155.157	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low
10.0.155.160	Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	High
173.45.230.150	Firewall Detected	Info

- INTRODUCCIÓN
- Información del proyecto
- Consideraciones
- Disclaimer
- Introducción
- Objetivo
- SUMARIO EJECUTIVO
- Postura de seguridad
- PERFIL DE RIESGO
- RESULTADOS
- Postura y perfil de riesgo asignados
- CONCLUSIONES
- Resumen de Vulnerabilidades
- Gráficas



sample.sonoma.edu - VulnerabilityDefinition Report

27 Feb 2023 11:55PM GMT

You are receiving this report because you have been identified as the owner or technical contact of the website(s) listed below.

Urgent or Critical Vulnerability Found

Urgent and critical vulnerabilities must be addressed immediately to is to ensure the safety and protection of the SSU community.

VulnerabilityDefinition Summary - Severity Count by Severity

Web Application	Urgent	Critical	Serious	Medium	Minimal
Faculty and Staff Directory	0	0	11	2	3
Global Portal Message Editor	0	0	0	0	0
Guest Parking	0	0	0	0	0
Server	0	2	1	1	0

Vulnerability Details

Server - https://sample.sonoma.edu/

Severity	VulnerabilityDefinition	Detection
Critical	**Title:** Apache HTTP Server mod_proxy Server Side Request Forgery (SSRF) Vulnerability (CVE-2021-40438) **URL:** https://sample.sonoma.edu/ **Description:**The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software. On affected versions of Apache HTTP Server, a SSRF vulnerability exists when a remote attacker sends a crafted request uri-path which causes "mod_proxy" to forward the request to a server chosen by the attacker. Affected Versions: Apache HTTP Server 2.4.48 and earlier QID Detection Logic (Unauthenticated): This QID sends a HTTP GET request and checks the response headers to confirm the vulnerable version of Apache HTTP Server running on the application. **CWE:** CWE-918 **Impact:** Successful exploitation of this vulnerability could allow a remote attacker to send specially crafted HTTP requests and trick the web server to initiate requests to arbitrary systems. **Solution:**	**First:** 2022-11-16 **Last:** 2023-02-26 **Times:** 8
Critical	**Title:** Apache HTTP Server Buffer Overflow Vulnerability (CVE-2021-44790) **URL:** https://sample.sonoma.edu/webscan/ **Description:**The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software. On affected versions of Apache HTTP Server, a carefully crafted request body can cause a Buffer Overflow in the "mod_lua" multipart parser called via the r:parsebody() function in Lua scripts. Affected Versions: Apache HTTP Server 2.4.51 and earlier QID Detection Logic (Unauthenticated): This QID sends a HTTP GET request and checks the response headers to confirm the vulnerable version of Apache HTTP Server running on the application. **CWE:** CWE-787 **Impact:** Successful exploitation of this vulnerability could allow a remote attacker to trigger Buffer Overflow and execute arbitrary code on the target system. **Solution:**	**First:** 2023-01-22 **Last:** 2023-02-26 **Times:** 5

Reporte Técnico

- INTRODUCCIÓN
- Objetivo
- Metodología empleada
- Reconocimiento
- Identificación y comprobación de vulnerabilidades
- Alcance
- SUMARIO TÉCNICO
- Metodología de Riesgo
- Listado de Vulnerabilidades
- Recolección de información
- Narrativa de ataque
- Detalle de las Vulnerabilidades y
- REMEDIACIONES