Informe Ejecutivo
Challenge técnico

Observability Sec
MELI

Jhony Alexander Henao Nava

¿ Qué vulnerabilidades se encontraron durante la prueba ?

HTML Injection

Tipo:
Vulnerabilidad aplicativo
Plataformas:
Linux, Windows, MacOS
Defensa ignorada:
Antivirus
Control de aplicación
Resumen:
Por medio de código ingresado en campos del sitio publicado se puede cambiar la manera en que es ejecutada la acción

Link Mitre

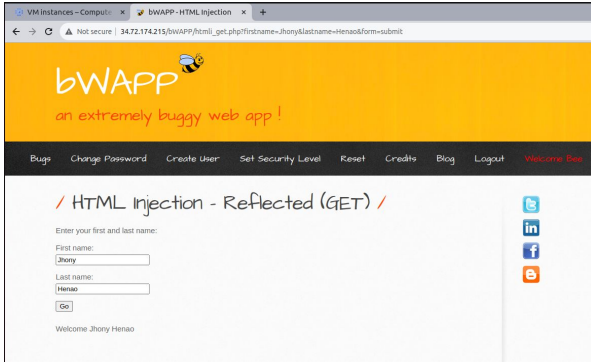
Endpoint Denial of Service

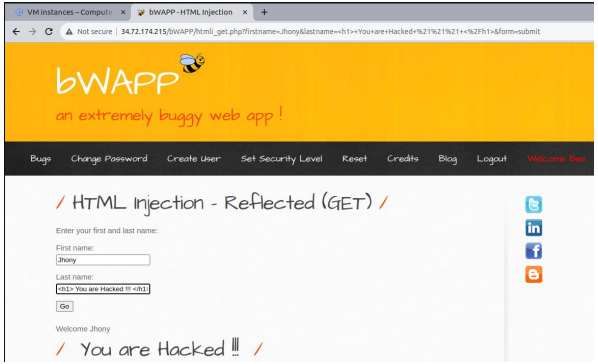
Tipo:
Degradación, disponibilidad
Plataformas:
Cloud, Linux, Windows, MacOS
Defensa ignorada:
FW, WAF, Rate limits
Resumen:
Por medio de envío de tráfico constante se busca degradar la respuesta del endpoint o dejarlo no disponible para consultas

Link Mitre

¿ Cómo respondió el endpoint ante la explotación y cómo se visualizó a nivel de Logs el ataque ?

HTML Injection

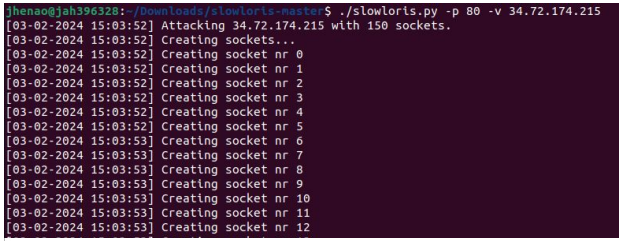


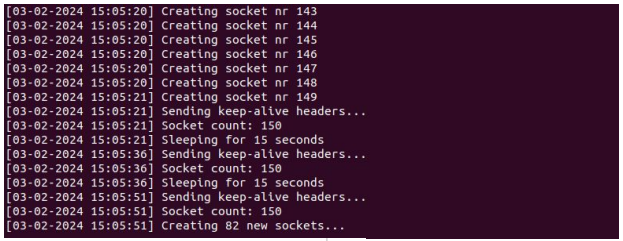


La inyección de HTML se realizó a un formulario publicado en el endpoint en el que se ingresaron etiquetas de HTML y se pudo cambiar el comportamiento del endpoint al incluir texto como un encabezado del sitio.

Date	Action taken	IP address	Method	Path	User agent	Query string
Feb 3, 2024 4:45:23 PM	Skip	181.51.80.143	GET	/bWAPP/htmli_get.php	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36	?firstname=Jhony&lastname=%3Ch1%3E+You+are+Hacked+%21%21%21+%3C%2Fh1%3E&for

Endpoint Denial of Service





La denegación de servicio se realizó por medio de una herramienta la cual envía peticiones http parciales al endpoint por lo que las conexiones se mantienen abiertas hasta degradar o bajar el servicio por completo.

Date	Action taken	IP address	Method	Path	User agent
Feb 3, 2024 4:43:25 PM	Skip	181.51.80.143	GET	/bWAPP/info.php	Screaming Frog SEO Spider/19.4
Feb 3, 2024 4:43:25 PM	Skip	181.51.80.143	GET	/bWAPP/training.php	Screaming Frog SEO Spider/19.4

¿ Cómo se pueden mitigar las vulnerabilidades ?

HTML Injection

- Validaciones a nivel de backend en el código de la aplicación (RegEx).
- Pruebas unitarias al endpoint donde se identifique éste tipo de datos ingresados.
- Configuración de un WAF con reglas habilitadas para identificar inyecciones de código en la aplicación.
- Habilitación de un agente XDR dentro de la instancia que ejecute la aplicación con el fin de poder detectar y remediar estos comportamientos atípicos encontrados.

Endpoint Denial of Service

- Validaciones a nivel de backend en el código de la aplicación (RackAttack, RateLimit).
- Pruebas de estrés al aplicativo identificando los valores máximos procesados por el endpoint sin llegar a degradar el servicio.
- Configuración de un FW o WAF con configuraciones habilitadas de DoS, DDoS y Rate Limit de acuerdo al tráfico esperado por cada endpoint protegido.

También se debería contar con un monitoreo del tráfico que procesa la aplicación en donde por medio de tableros y alertas se puedan encontrar éste tipo de ataques sobre la aplicación basado en respuestas, tráfico o comportamientos atípicos.

Date	Action	SourceIP	Hostname	Method	Path
2/1/2024 19:17	Block	181.51.80.143	test.direccionest...	GET	/bWAPP/htmli_get.php

QueryString
?firstname=Jhony&lastname=%3Ch1%3E+Hola+%3C%2Fh1%3E&form=submit

Anexos

https://github.com/jhonyhenao/Tech_Challenge