# Relatório de Segurança – Tópico 1.3

## Objetivo

Detectar comportamentos anômalos em entradas de usuários, como tentativas excessivas ou padrões maliciosos (XSS), para prevenir ataques e identificar possíveis invasores.

## Ações Realizadas

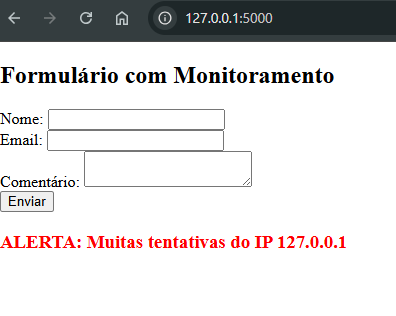
- Utilizado o framework Flask para criação de uma interface web com campos de entrada.  
- Utilizado o Loguru para registrar todas as requisições em arquivo de log.  
- Implementada contagem de tentativas por IP e detecção de padrões maliciosos no campo de comentário.  
- Configurado alerta visual (na tela) e por log para eventos suspeitos, como XSS e excesso de requisições.

## Testes Realizados

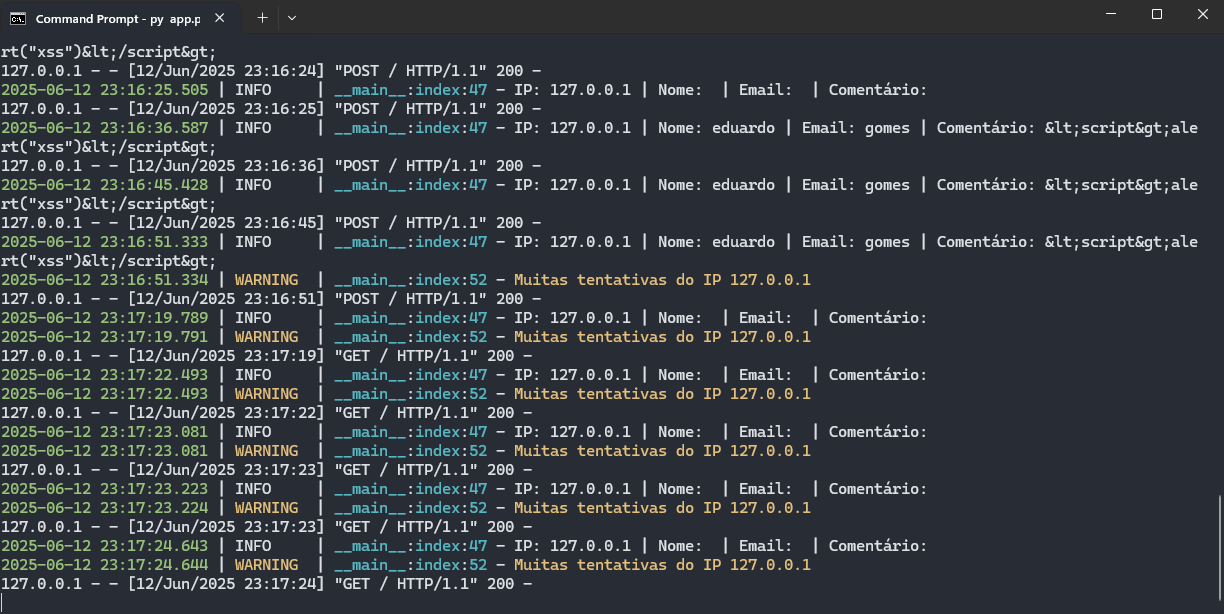
|  |  |  |  |
| --- | --- | --- | --- |
| Cenário | Entrada | Resultado Esperado | Resultado Obtido |
| Tentativas repetidas | 6 requisições consecutivas do mesmo IP | Alerta de excesso de tentativas | ALERTA: Muitas tentativas do IP 127.0.0.1 |
| Tentativa de XSS | <script>alert('xss')</script> | Detecção de XSS e bloqueio | Comentário sanitizado, alerta emitido em log |

## Capturas de Tela

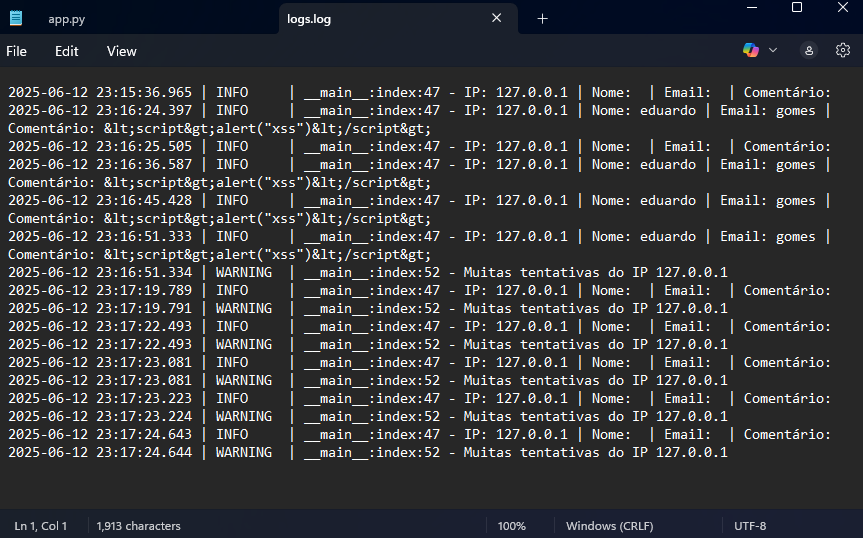
Abaixo, a evidência da interface web com alerta de múltiplas tentativas do mesmo IP:



Evidência do terminal mostrando múltiplas requisições com alertas de segurança:



Arquivo de log (logs.log) com registros detalhados das entradas e alertas gerados:



## Conclusão

O sistema foi capaz de detectar padrões de comportamento anômalos, emitindo alertas tanto na interface quanto nos logs.  
As técnicas implementadas demonstram boas práticas de monitoramento e resposta a incidentes, contribuindo para a segurança geral do sistema.