Tarefa realizada no dia: 26/04

Representando a atividade: **Cadastro Servidor- SQL Injection**

Duração dos testes: 1hora e 30 min

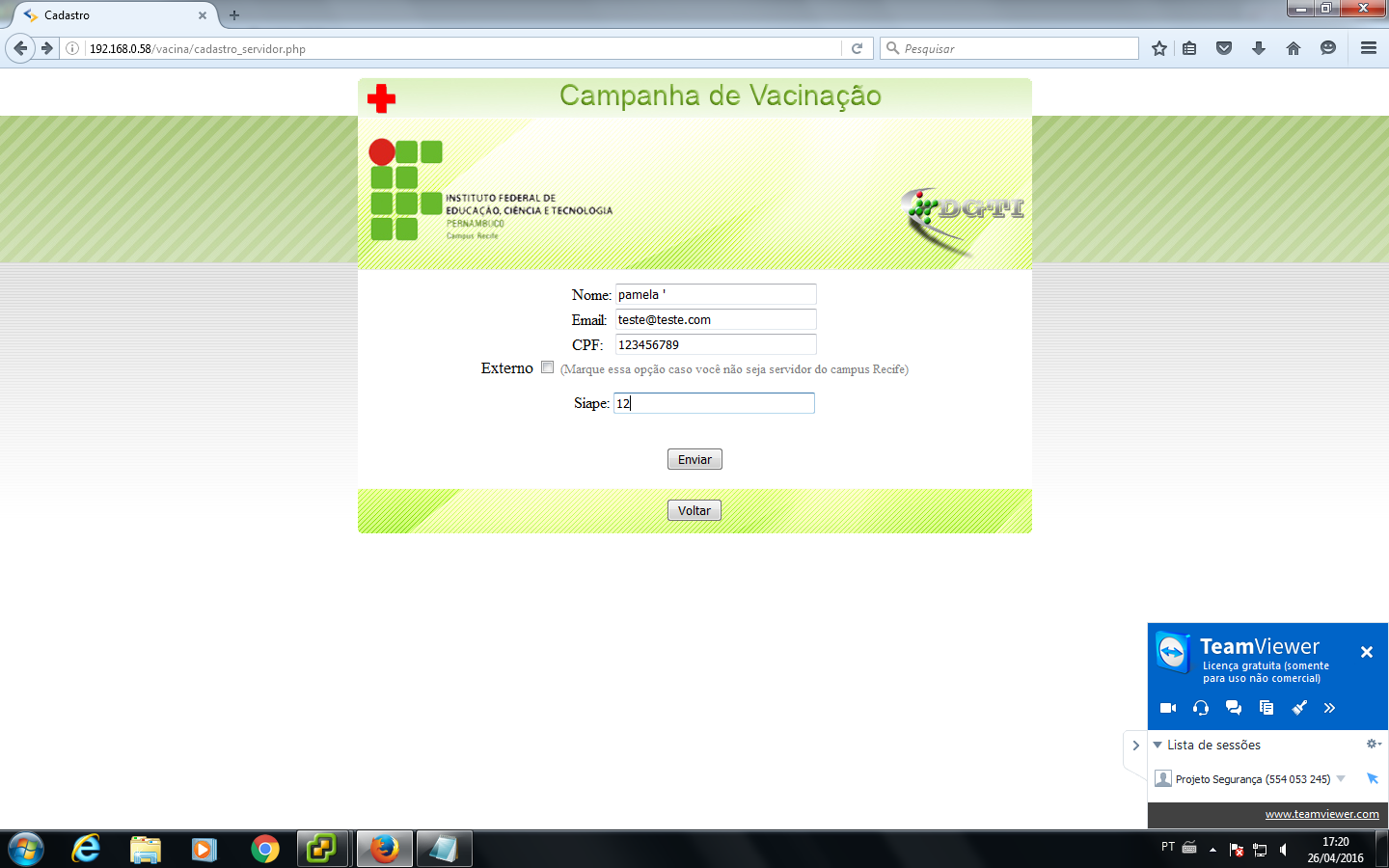
Duração total da atividade: 2 horas

**Objetivo**: Submeter entradas maliciosas no sistema através de injeção de códigos SQL na página de Cadastro Servidor de modo a fazer a aplicação web executar ações não autorizadas. Exemplos: expor dados de usuários cadastrados na base de dados e tipo de SGBD utilizado por essa base de dados.

**Resultados**:

**Tentativa 1:** Verificar se o campo Nome é vulnerável a injeção de código SQL fazendo uso da técnica de concatenação de aspas simples.

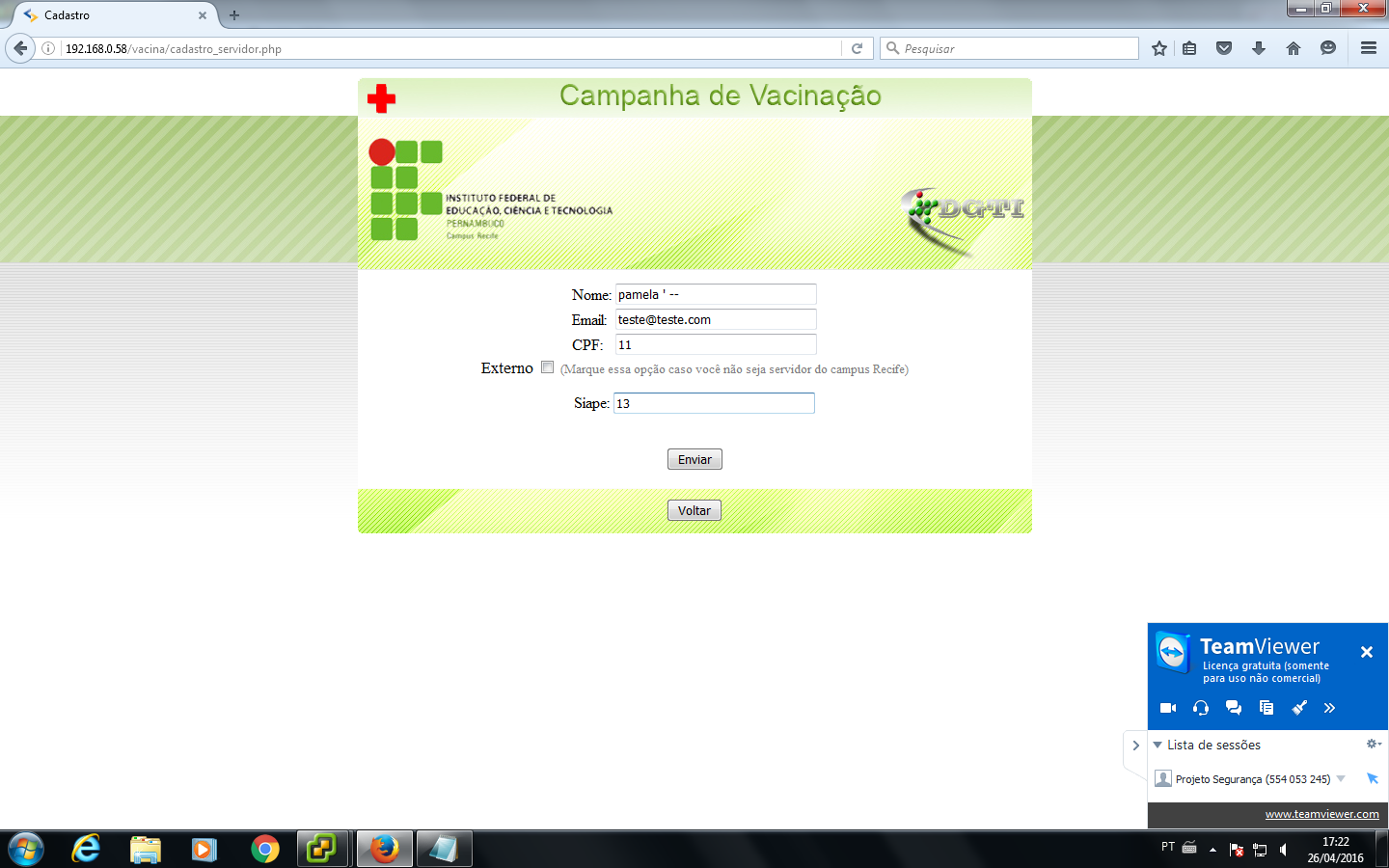
Entradas:



**Resultado**: Passou no teste. A aplicação está fazendo tratamento de dados de entrada não permitindo a injeção de instruções SQL através do campo de Nome.

**Tentativa 2:** Inserir uma string com uma distribuição adequada de aspa simples e comentários inline como entrada para o campo Nome para não provocar falha na instrução a ser executada no interpretador de SQL da aplicação. Dessa forma, tentar forçar o interpretador de SQL da aplicação a ignorar tudo que vier após o comentário inline.

Entradas:



**Resultado**: Passou no teste.

**Tentativa 3:** Desabilitar javascript e repetir tentativas 1 e 2.

Entradas:

Campo Nome

teste ‘

teste ‘ --

teste ‘ #

Campo Siape

1231 ; select \* from usuarios; --

; select \* from usuarios; #

**Resultado:** Passou no teste. Nada acontece página não realiza requisição.

Tentativa 3:

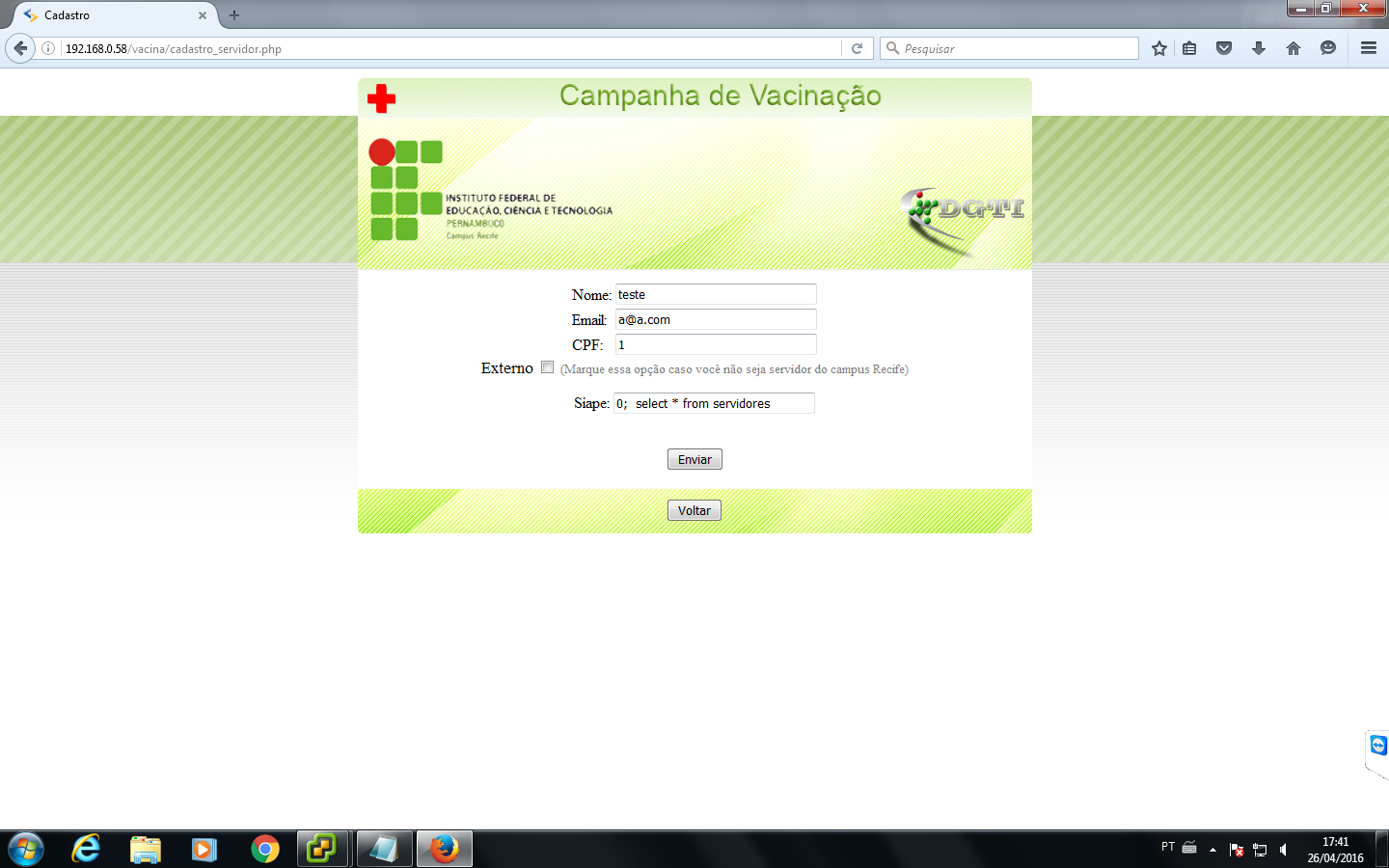
Verificar se o campo Siape é vulnerável.

Entradas

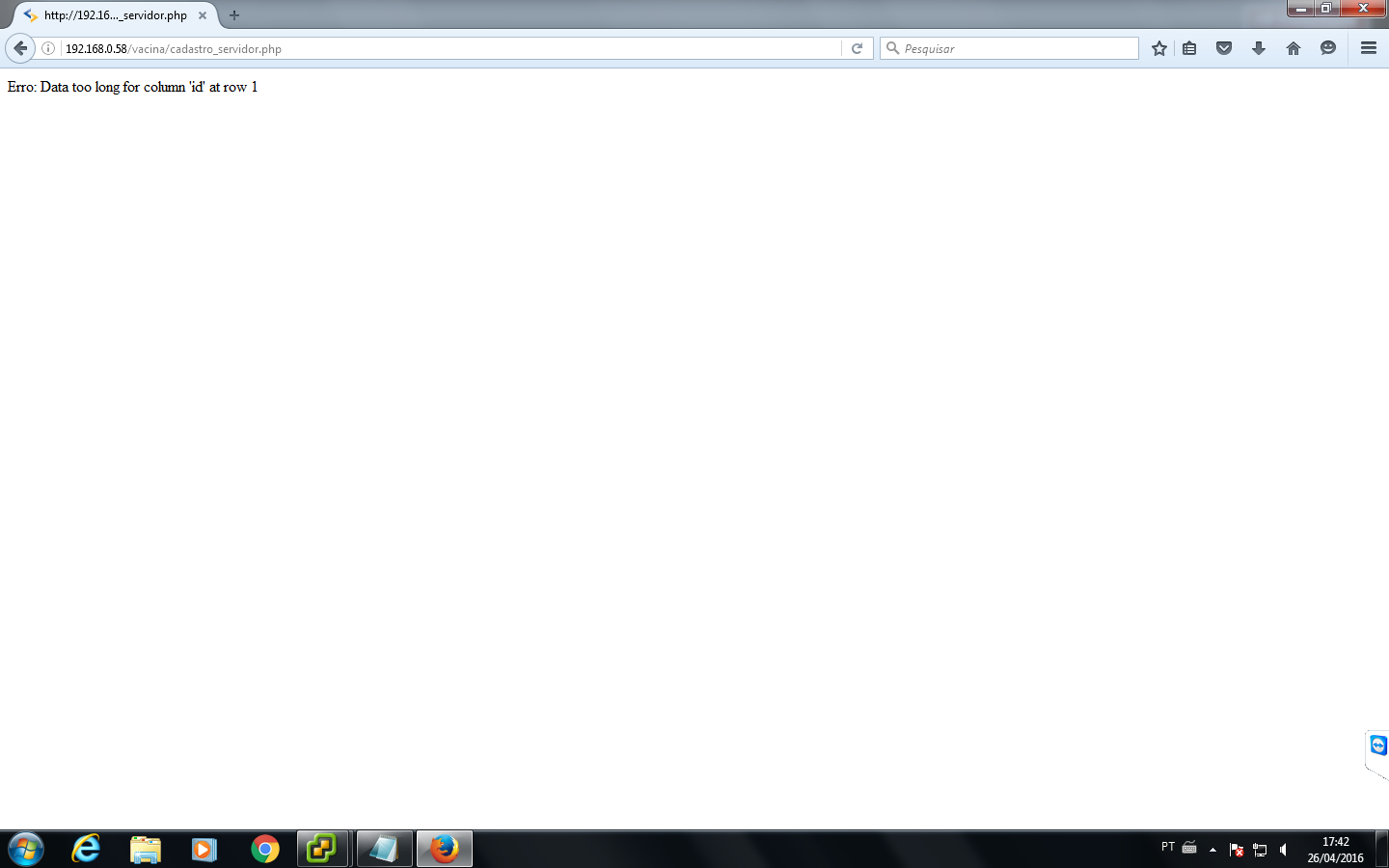
Campo Siape

1231 ; select \* from usuarios; --

; select \* from usuarios; #

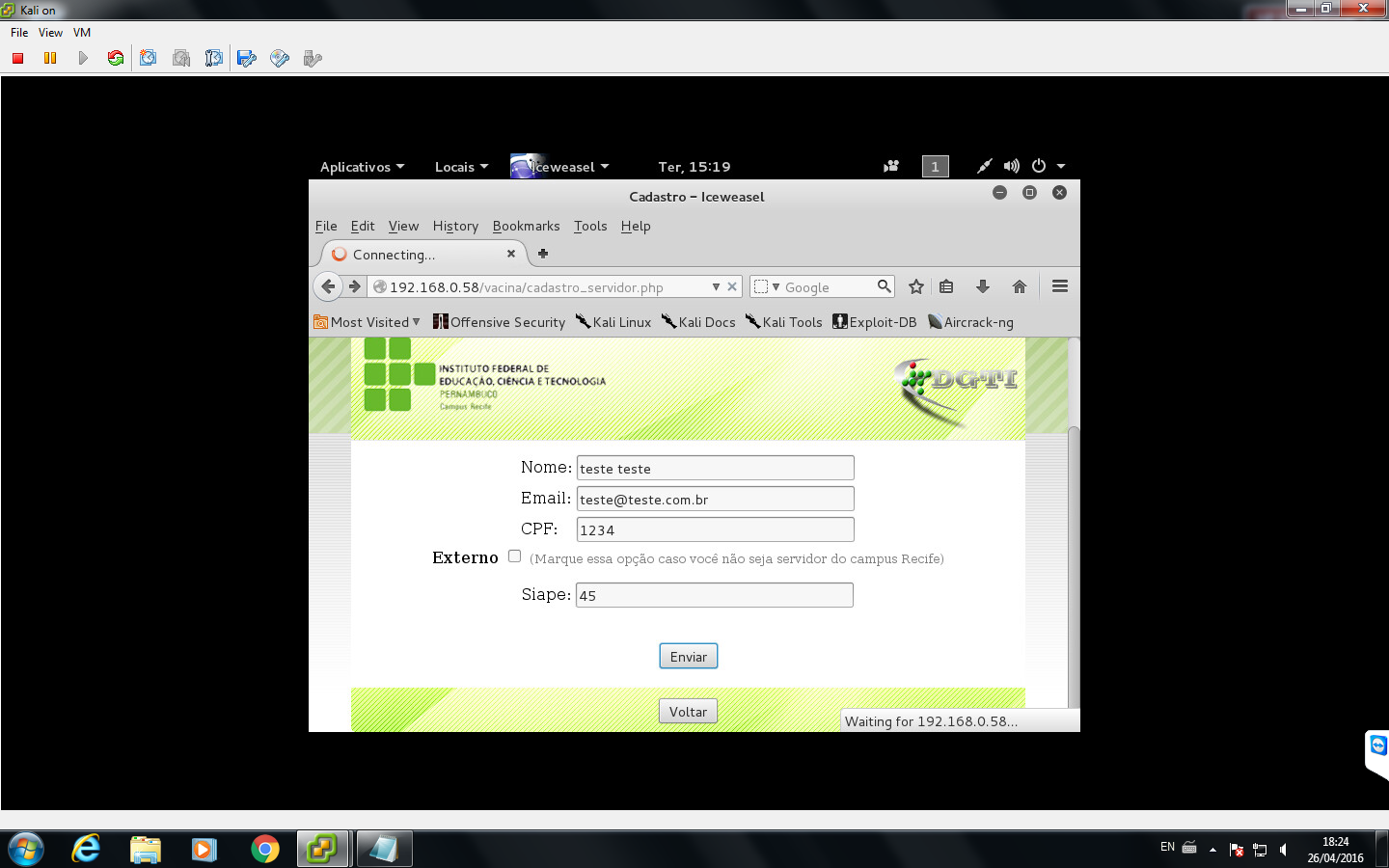


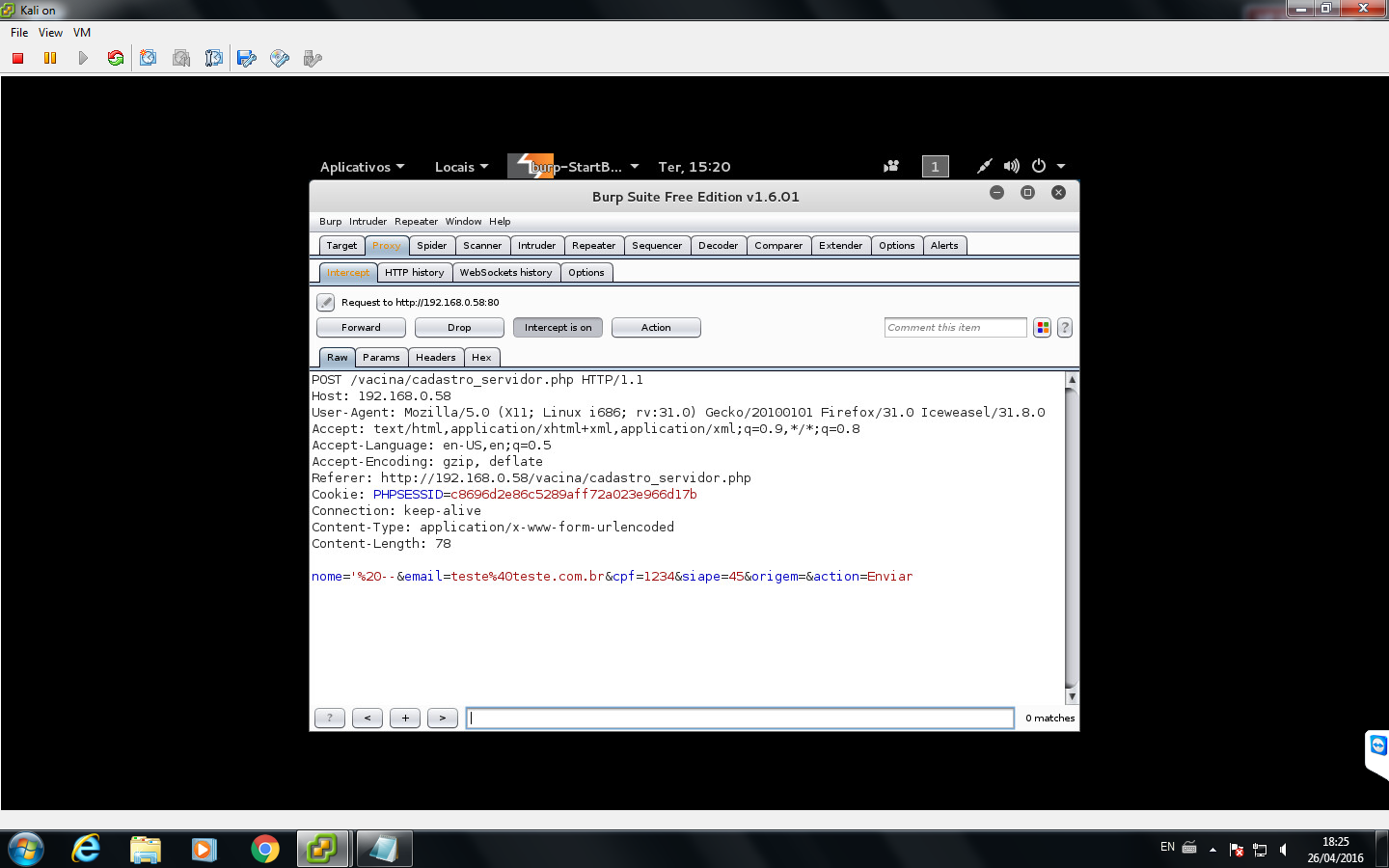
Resultado: Não foi possível descobrir dados de outros servidores cadastrados na base de dados. Entretanto devido a falta de tratamento adequado para dados inválidos no campo Siape, foi possível identificar que esse campo, no banco de dados corresponde a coluna ‘id’.

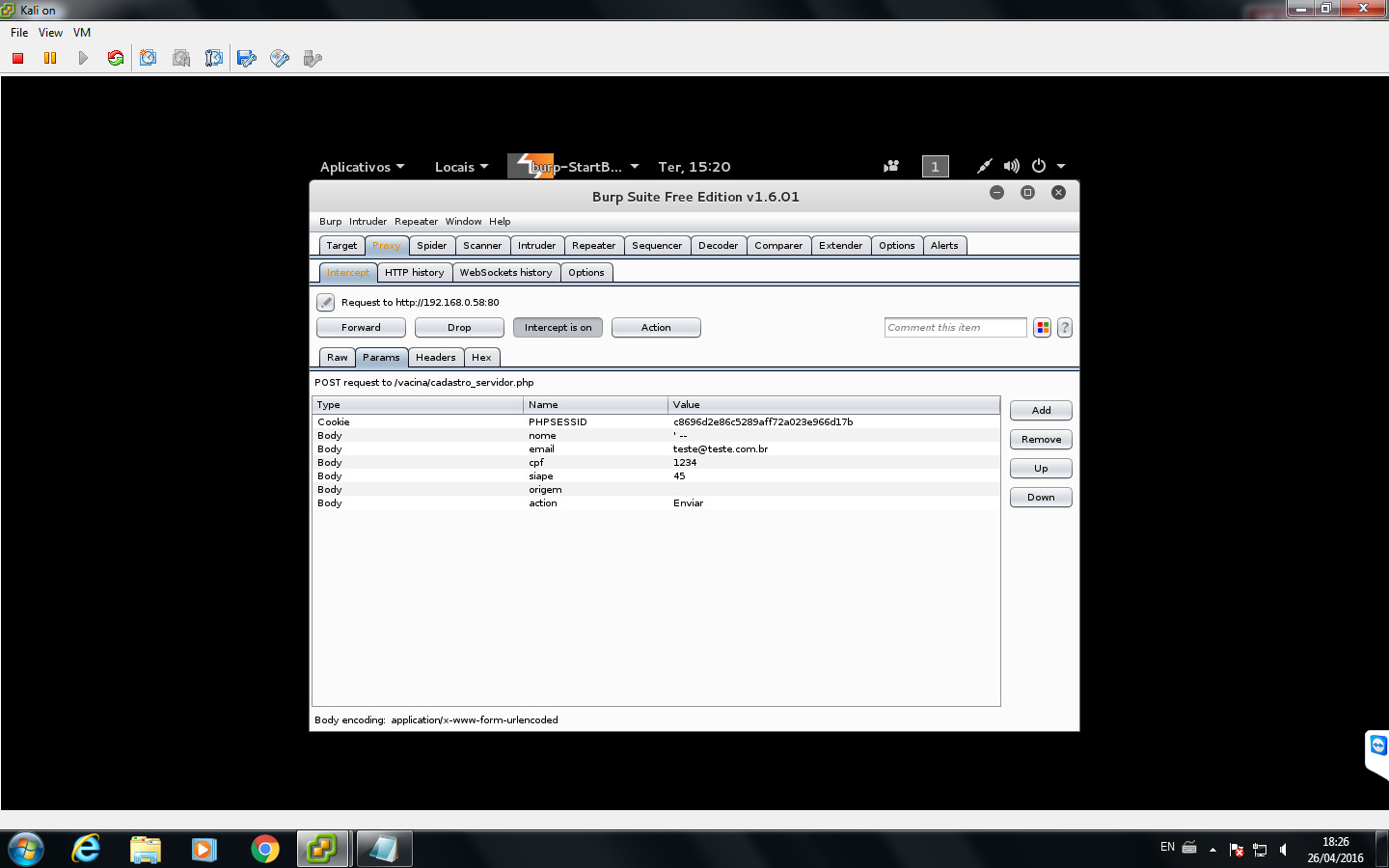


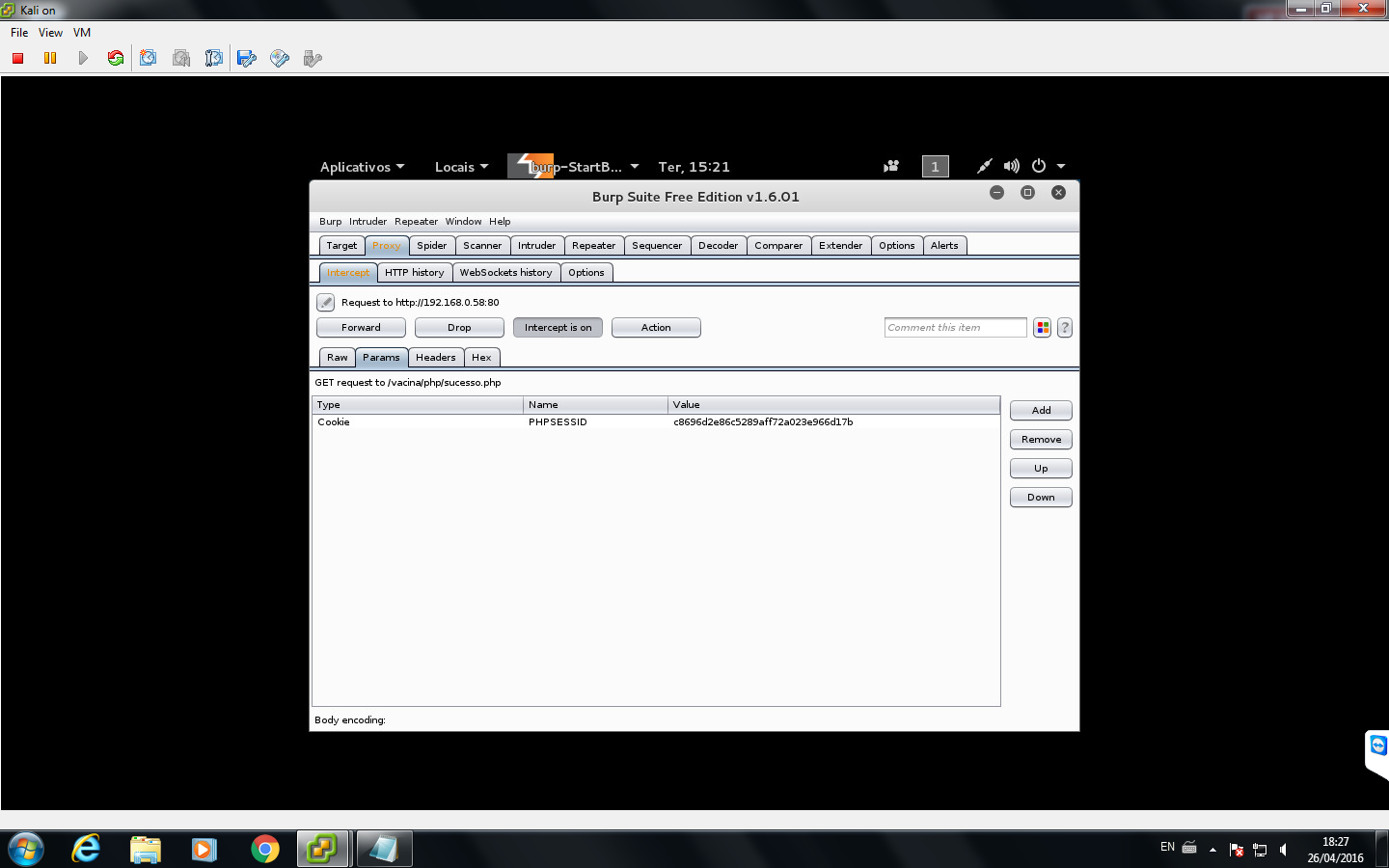
Tentativa 5

Usar burp para modificar parametros enviados via POST na tela de Cadastro de Servidor.









Tentativa 6

Usar a ferramenta automatizada SQL Map para realizar a tentativa de injetar SQL na página.

Salvar a requisição POST capturada num arquivo e indicá-lo ao SQL Map para que possa utilizá-lo na requisição.

*comando*: sqlmap -r paramsTelaConsServidor -p nome

sqlmap -r paramsTelaConsServidor -p siape

sqlmap -r paramsTelaConsServidor -p cpf

sqlmap -r paramsTelaConsServidor -p cpf --dbms=msql



