



Laboratório Avançado de Produção Pesquisa e Inovação em Software

Relatório #03 de atividade da equipe de segurança

Rodolfo Cabral Neves

Brasília, aos 16 de Agosto de 2024

Introdução

O presente documento consiste na apresentação dos resultados dos testes de penetração que foram executados pelo time responsável pela segurança do projeto Brasil Participativo – BP em ambiente local, utilizando a branch *main*. Os testes foram realizados do dia 6 ao dia 16 de agosto de 2024 e a metodologia foi *black-box*. Para mais informações [consulte o documento de escopo](#). O documento também apresenta medidas de mitigação das vulnerabilidades supracitadas.

Sumário

Foram encontradas duas vulnerabilidades, uma do tipo *Information Disclosure* de severidade baixa e outra do tipo *Cross Site Scripting - XSS* de severidade média.

Ferramentas

Durante os testes, foram utilizadas as seguintes ferramentas:

- Sistema Operacional Kali Linux:
 - o Distribuição Linux de código aberto baseada em Debian que permite aos usuários realizar testes avançados de penetração e auditoria de segurança.
- Burp Suite – Community Edition:
 - o Ferramenta usada para testes em aplicações Web e API's.
- Zed Attack Proxy - ZAP:
 - o Ferramenta open-source usada para testes de penetração em Web e API's.
- SecLists e PayloadAllThings:
 - o Uma coleção de vários tipos de listas usadas durante avaliações de segurança. Os tipos de lista incluem nomes de usuários, senhas, URLs, strings grep de dados sensíveis, payloads de fuzzing e muito mais.
- Curl:
 - o Ferramenta para transferir dados de ou para um servidor usando URLs.

Vulnerabilidades encontradas

ID	Título	Classe	Severidade	Estado
VULN01	Information Disclosure via HTTP header	Information Disclosure	Informativo	Não resolvido
VULN02	Cross Site Scripting na página de conversas	Cross Site Scripting	Médio	Não resolvido

VULN01 - Information Disclosure via HTTP header

Descrição

A **exposição de informações sensíveis** via cabeçalho HTTP permite que detalhes sobre a aplicação do servidor e sua versão sejam usados por atacantes para identificar e explorar vulnerabilidades conhecidas específicas dessa versão.

Impacto

Potencialmente alto. Os atacantes podem personalizar ataques direcionados, como exploits de dia zero, que são altamente eficazes contra versões específicas de software. Além disso, essas informações podem ser usadas para mapear a rede, identificando os tipos de servidores e aplicações em uso, facilitando a criação de um plano de ataque mais eficaz. Isso resulta em um aumento do risco de exploração, já que vulnerabilidades específicas das versões do servidor podem ser exploradas, aumentando a probabilidade de comprometer o sistema.

Proof of Concept – PoC

Abra o terminal e digite:

```
$ curl -X OPTIONS -IL https://brasilparticipativo.presidencia.gov.br/?locale=pt-BR
```



```
File Actions Edit View Help
(noob@hostname)-[~]
$ curl -X OPTIONS -IL https://brasilparticipativo.presidencia.gov.br/?locale=pt-BR
HTTP/1.1 404 Not Found
Server: nginx/1.14.1
Date: Thu, 15 Aug 2024 14:53:16 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: strict-origin-when-cross-origin
Vary: Accept
X-Request-Id: 0eb6376e-ea96-4180-9383-ce3670ad19d7
```

Imagem 1 - Cabeçalho da plataforma Brasil Participativo – BP.

Fonte – Do autor.

Mitigação

Para mitigar esta vulnerabilidade é necessário configurar o servidor para ocultar detalhes como o nome e a versão da aplicação para que não sejam expostas nos cabeçalhos HTTP, manter o software e os servidores atualizados e implementar práticas de monitoramento contínuo e auditoria.

VULN02 - Cross Site Scripting na página de conversas

Descrição

Esta falha é do tipo DOM-based , é temporária (não afeta outros usuários do sistema) e permite a execução de código arbitrário JavaScript na página do usuário, quando o servidor envia o código HTML a ser renderizado com a mensagem, quando o usuário envia uma mensagem a outro.

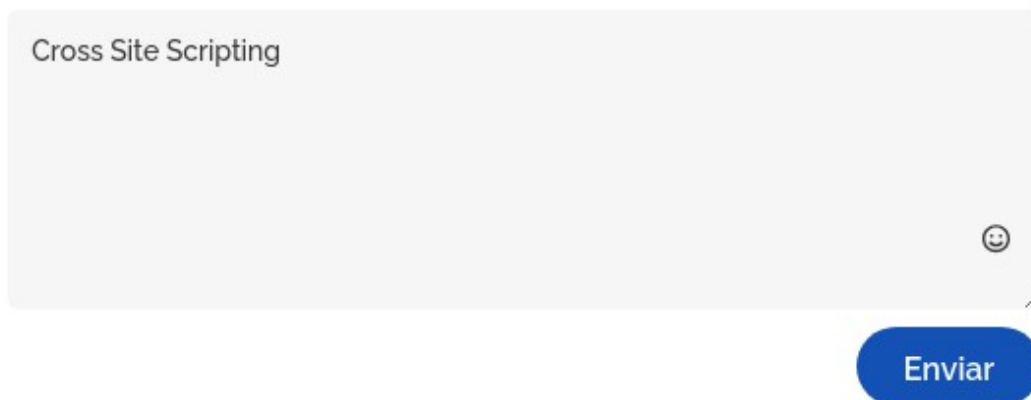
Impacto

Alto. O atacante pode executar código JavaScript arbitrário, incluindo o roubo de cookies e sessões ou redirecionamento para sites maliciosos. Esses ataques podem também ser um vetor para outros tipos de ataques, como Cross-Site Request Forgery (CSRF), ampliando ainda mais os danos potenciais.

Proof of Concept – PoC

1. Na página das conversas do usuário, crie uma conversa com um usuário aleatório
2. Abra o Burp Suite e habilite a opção de *Intercept* e volta para a página das conversas
3. Clique no botão de Enviar e volte para o Burp Suite
4. Clique em *Action -> Do Intercept -> Response to this request*
5. Crie uma tag de script e insira qualquer código JavaScript e clique em *Forward* e volte para a página ver o resultado.

Responder



Cross Site Scripting

😊

Enviar

Imagem 2 – Envio de mensagem para outro usuário.

Fonte – Do autor.

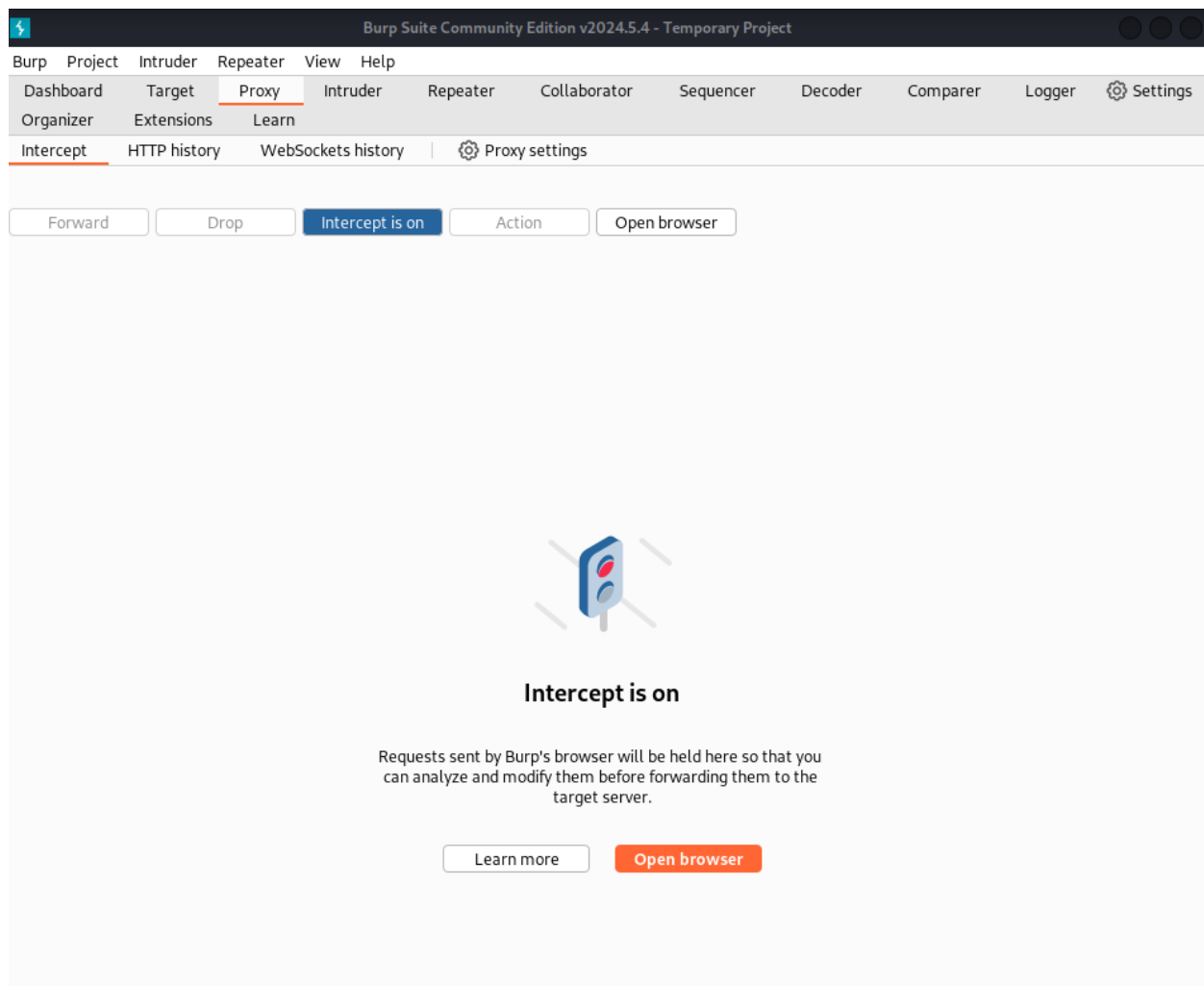


Imagem 3 – Burp Suite com o *Intercept* ativado.

Fonte – Do autor.

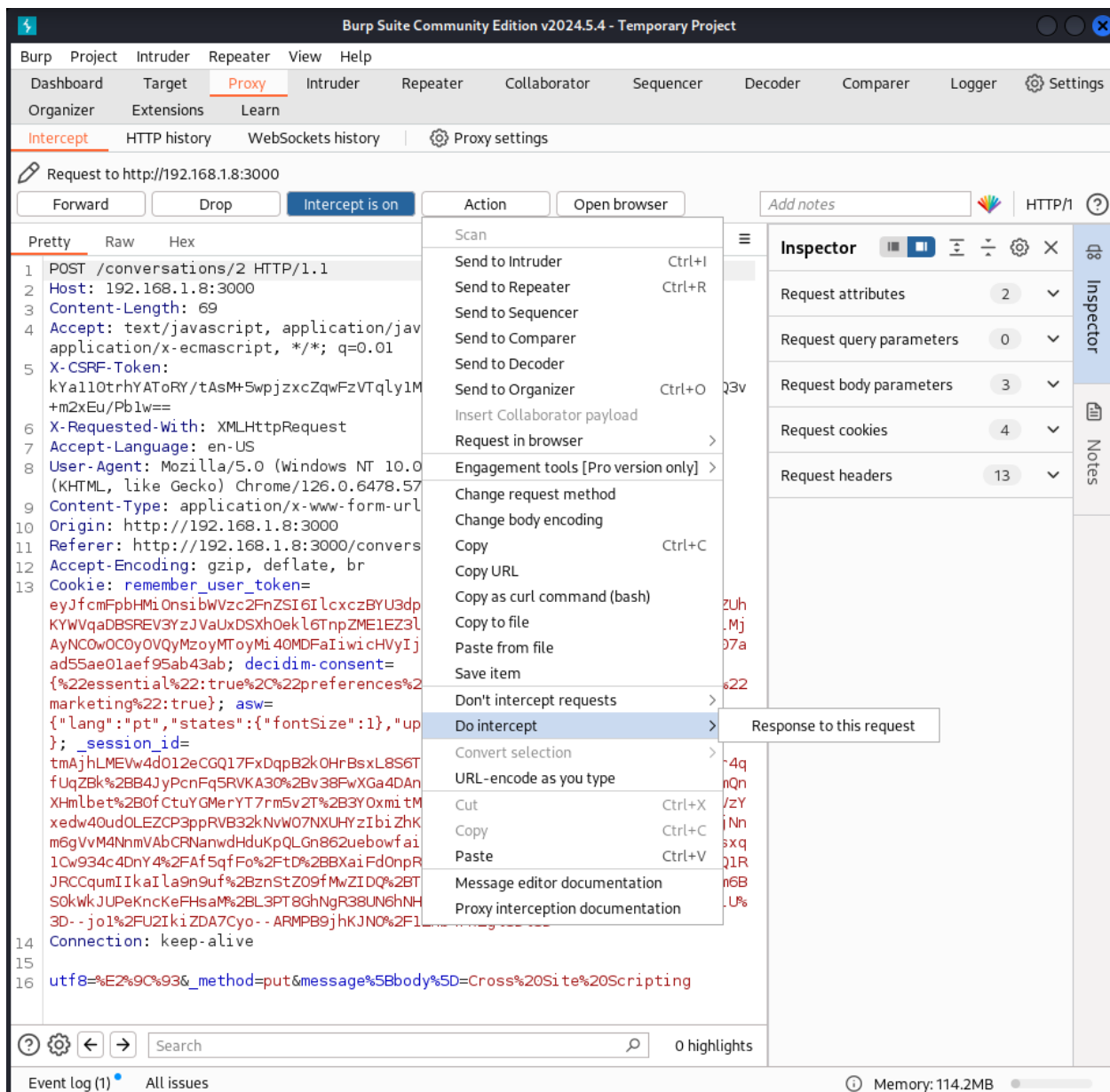


Imagem 4 – Requisição POST para a rota `/conversations/2` .

Fonte – Do autor.

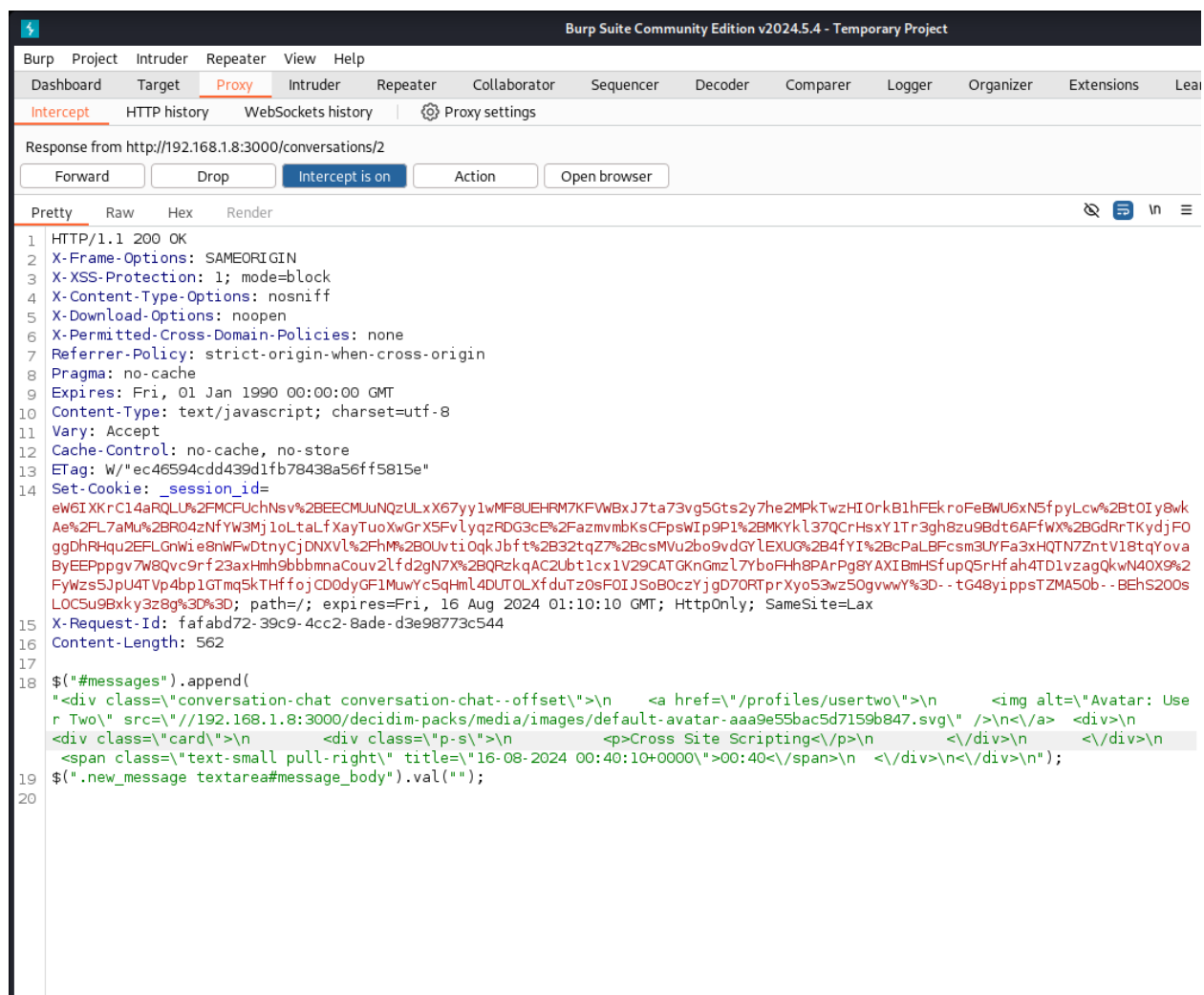


Imagem 5 – Resposta da requisição POST da rota `/conversations/2`.

Fonte – Do autor.

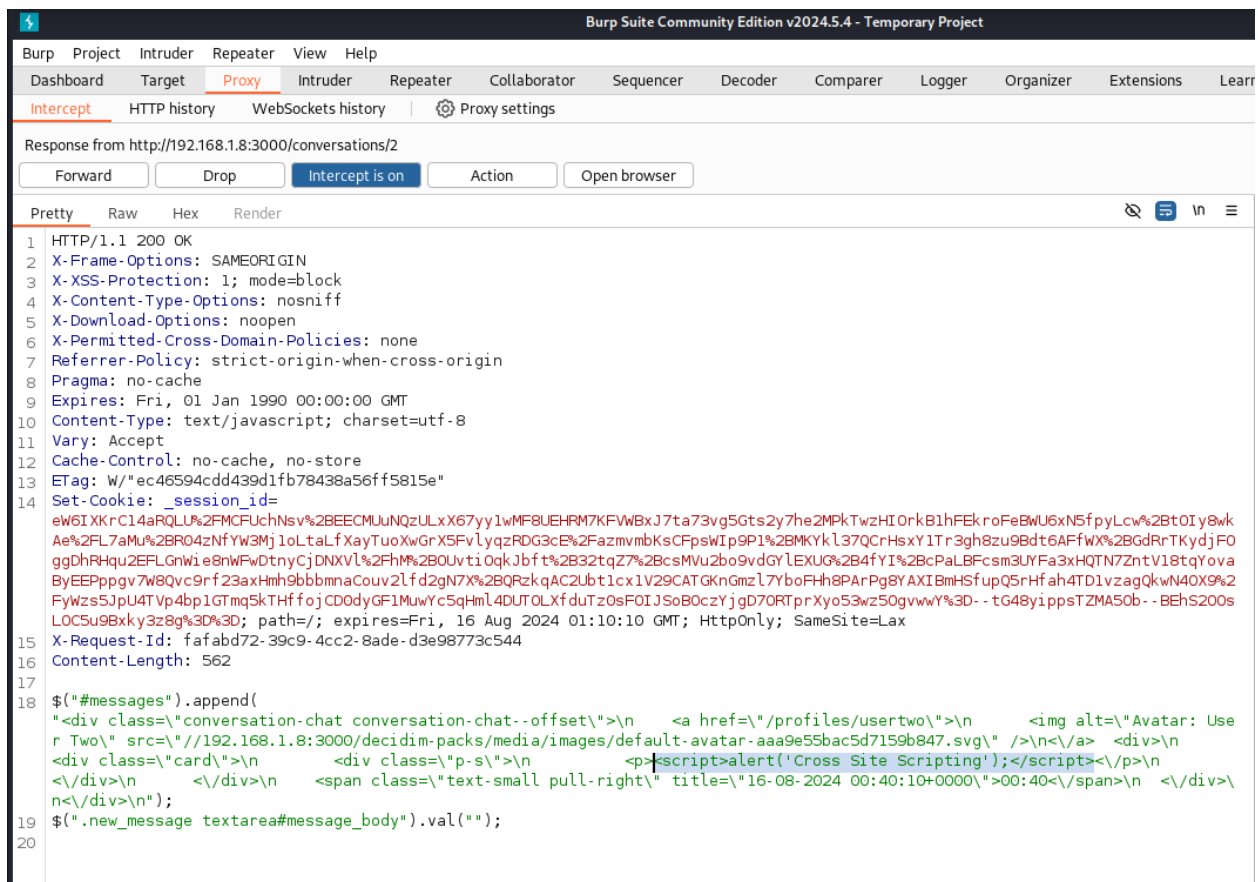


Imagem 6 – Resposta da requisição POST da rota `/conversations/2` e a injeção da tag de script.

Fonte – Do autor.

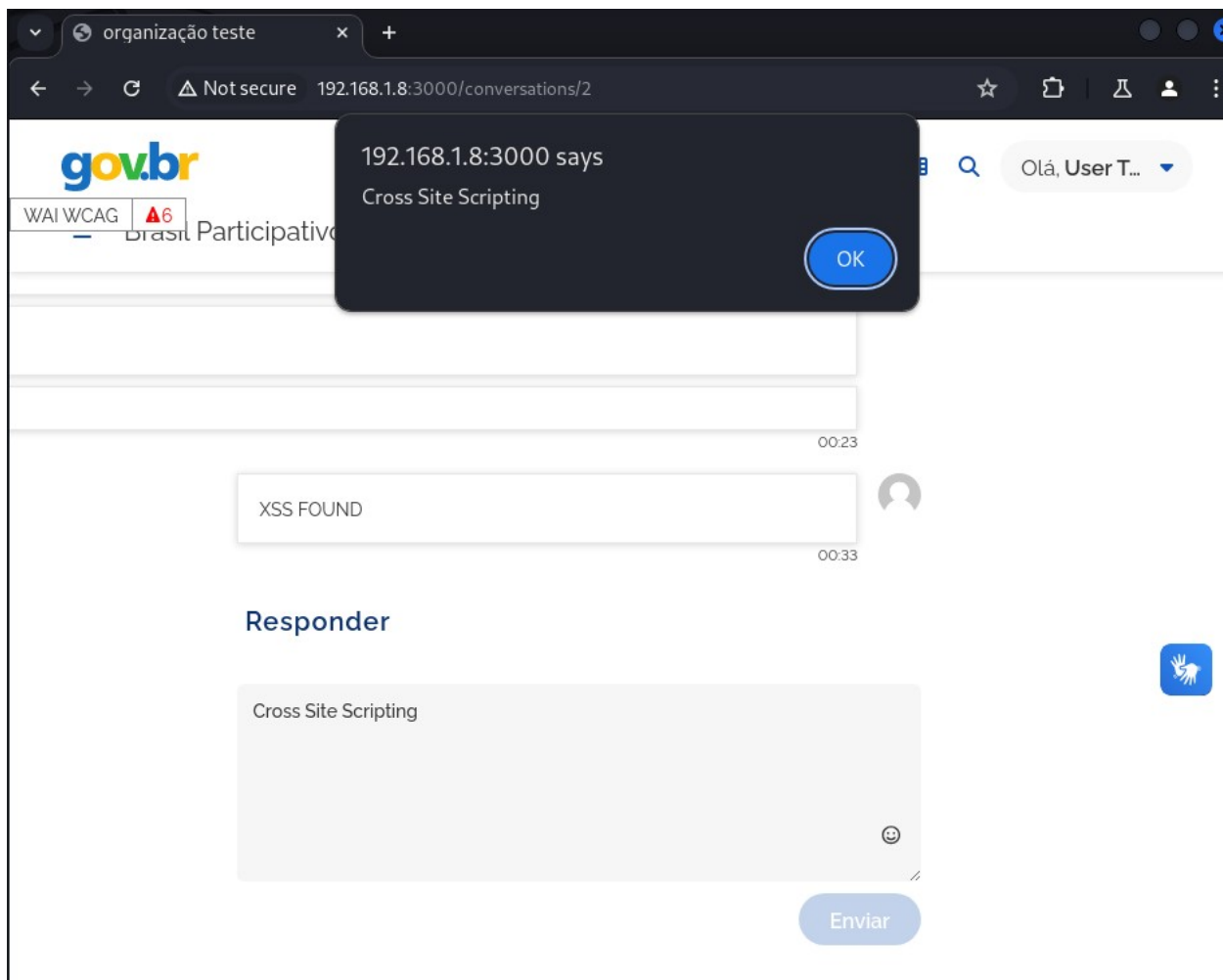


Imagem 7 – Página comprometida.

Fonte – Do autor.

Mitigação

Para mitigar esta vulnerabilidade é necessário que a transferência dos dados seja feita de forma segura. Em vez de enviar um código HTML com os dados, enviar os dados utilizando o Representational State Transfer – REST que utiliza o JSON, ou algum outro método que garanta a segurança dos dados.

Referências Bibliográficas

CURL. curl. Disponível em: <https://curl.se/docs/manpage.html>. Acesso em: 15 ago. 2024.

KALI Linux. What is Kali Linux? Disponível em: <https://www.kali.org/docs/introduction/what-is-kali-linux/>. Acesso em: 15 ago. 2024.

KALI Linux. Seclists. Disponível em: <https://www.kali.org/tools/seclists/>. Acesso em: 15 ago. 2024.

ZAPROXY. Introducing ZAP. Disponível em: <https://www.zaproxy.org/getting-started/>. Acesso em: 15 ago. 2024.