# Analyzing Vulnerabilities - Workshop

## SQL Injection

Lab:[*https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data*](https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data)

### Solution:

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Modify the category parameter, giving it the value '+OR+1=1--
3. Submit the request, and verify that the response now contains additional items.

## XSS

Lab: [*https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded*](https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded)

### Solution:

1. Copy and paste the following into the search box:

<script>alert(1)</script>

1. Click "Search".

## OS Command Injection

Lab: [*https://portswigger.net/web-security/os-command-injection/lab-simple*](https://portswigger.net/web-security/os-command-injection/lab-simple)

### Solution:

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

## Directory Traversal

Lab: [*https://portswigger.net/web-security/file-path-traversal/lab-simple*](https://portswigger.net/web-security/file-path-traversal/lab-simple)

#### Solution:

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

../../../etc/passwd

1. Observe that the response contains the contents of the /etc/passwd file.

## Access Control

Lab:[*https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality*](https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality)

#### Solution:

1. Go to the lab and view robots.txt by appending /robots.txt to the lab URL. Notice that the Disallow line discloses the path to the admin panel.
2. In the URL bar, replace /robots.txt with /administrator-panel to load the admin panel.
3. Delete carlos.

## File Upload

Lab:[*https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload*](https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload)

### Solution:

1. While proxying traffic through Burp, log in to your account and notice the option for uploading an avatar image.
2. Upload an arbitrary image, then return to your account page. Notice that a preview of your avatar is now displayed on the page.
3. In Burp, go to **Proxy > HTTP history**. Click the filter bar to open the **Filter settings** dialog. Under **Filter by MIME type**, enable the **Images** checkbox, then apply your changes.
4. In the proxy history, notice that your image was fetched using a GET request to /files/avatars/<YOUR-IMAGE>. Send this request to Burp Repeater.
5. On your system, create a file called exploit.php, containing a script for fetching the contents of Carlos's secret file. For example:

<?php echo file\_get\_contents('/home/carlos/secret'); ?>

1. Use the avatar upload function to upload your malicious PHP file. The message in the response confirms that this was uploaded successfully.
2. In Burp Repeater, change the path of the request to point to your PHP file:

GET /files/avatars/exploit.php HTTP/1.1

1. Send the request. Notice that the server has executed your script and returned its output (Carlos's secret) in the response.
2. Submit the secret to solve the lab.