Web Application Vulnerability Assessment Report

Target Application: OWASP Juice Shop
Assessment Date: July 2025
Security Analyst: Adegboyega Toluwani
Tools Used: Burp Suite, Nikto, Wget

Executive Summary

This report summarizes a vulnerability assessment of the OWASP Juice Shop web application. The objective was to identify potential security weaknesses and align them with the OWASP Top 10 and relevant CWE identifiers. Findings highlight critical flaws such as SQL injection, use of default credentials, and exposure of sensitive data via backup files.

Summary of Findings

Vulnerability	Severity	Tool Used	OWASP Mapping
SQL Injection (Auth Bypass)	High	Manual/Burp	A01:2021 - Broken Access Control
Broken Authentication (Default)	High	Manual	A07:2021 - Identification & Authentication Failures
Sensitive Data Exposure (Backup)	High	Nikto/Wget	CWE-530 - Backup File Exposure

SQL Injection – Authentication Bypass

Description:
The login form is vulnerable to SQL injection, allowing an attacker to bypass authentication and access protected areas without valid credentials.

Payload Used:

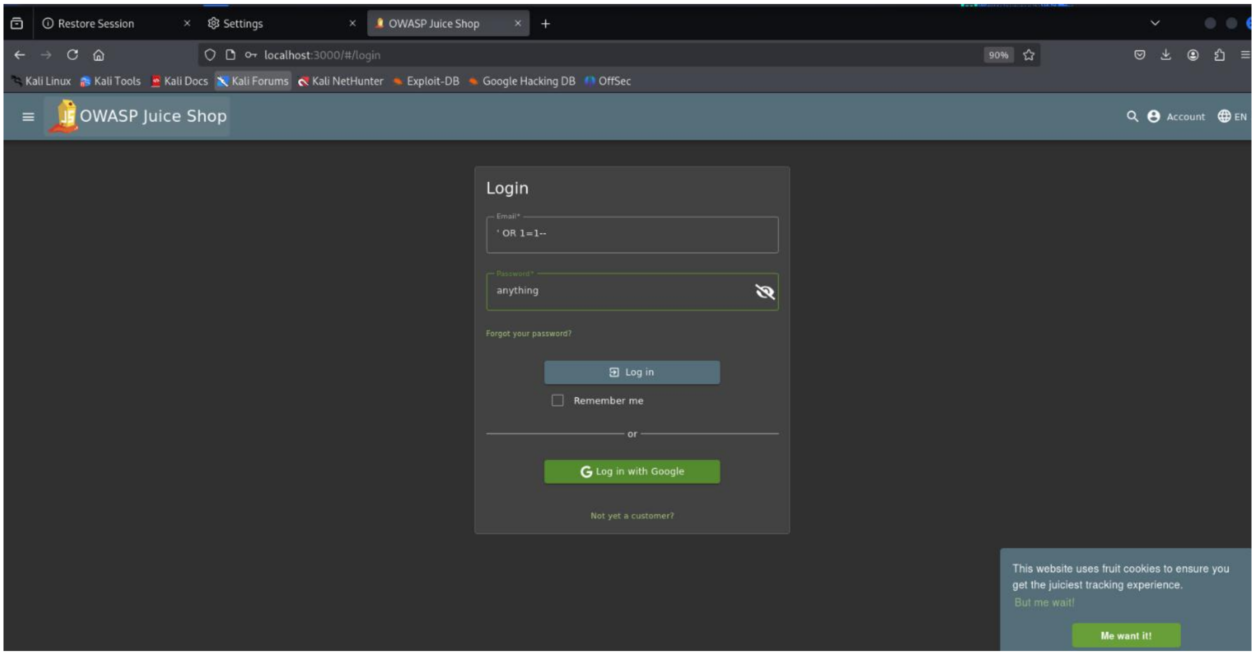
Email: ' OR 1=1--

Password: anything

Impact:

Attackers can login as any user (e.g., admin), which can lead to full compromise of the application.

Screenshot Evidence:

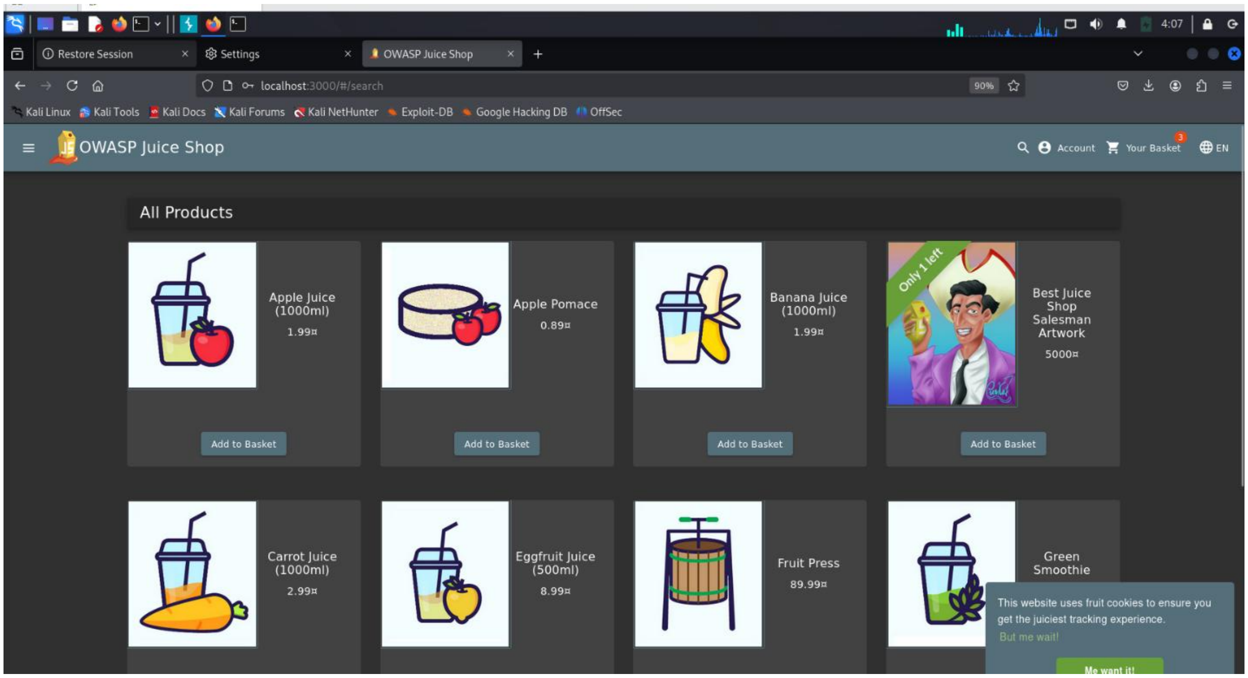


Login

Email*
' OR 1=1--

Password*
anything

This website uses fruit cookies to ensure you get the juiciest tracking experience.



This website uses fruit cookies to ensure you get the juiciest tracking experience.

Screenshot of the login form and successful bypass result here.

Mitigation:

- Use parameterized queries (prepared statements)
- Apply server-side input validation
- Sanitize user inputs

Reference:

- OWASP A01:2021 - Broken Access Control
- CWE-89: SQL Injection

Broken Authentication via Default Credentials

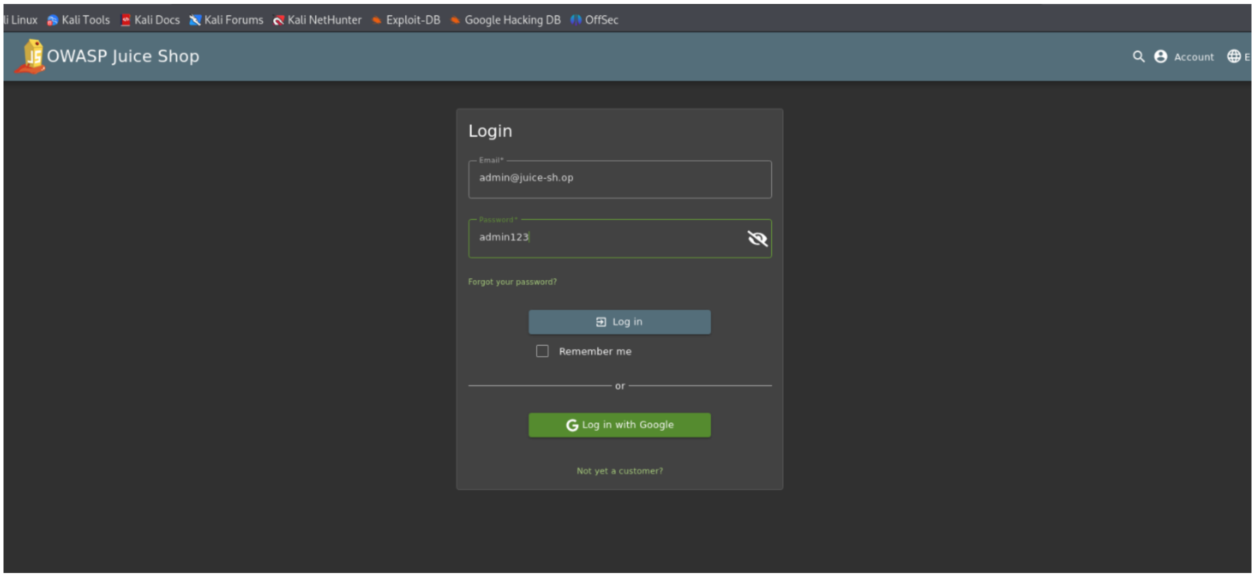
Description:
The application allowed login using publicly known default credentials.

Credentials Used:

Username: admin@juice-sh.op
Password: admin123

Impact:
Full administrative access was gained without brute-force or social engineering.

Screenshot Evidence:

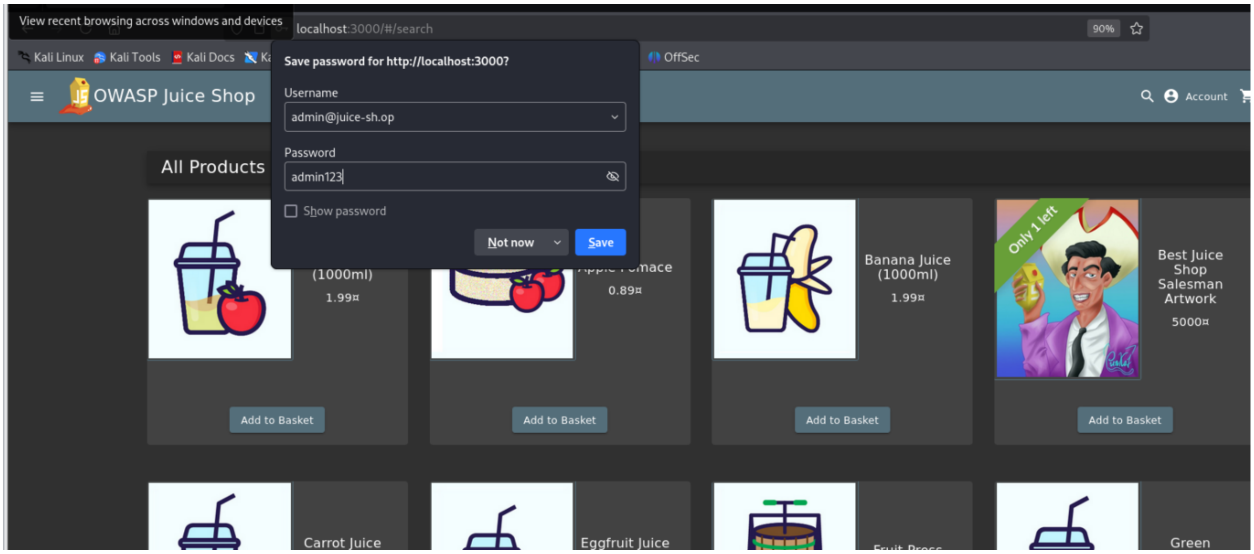


Login

Email*: admin@juice-sh.op

Password*: admin123

□ Remember me



View recent browsing across windows and devices

localhost:3000/#/search

Save password for http://localhost:3000?

Username: admin@juice-sh.op

Password: admin123

□ Show password

Screenshot of the login page and dashboard access after login.

Mitigation:

- Force password Change on first login
- Disable default accounts before deployment
- Implement account lockout after multiple failed login attempts
- Enforce MFA (Multi-Factor Authentication)

Reference:

- OWASP A07:2021 - Identification & Authentication Failures
- CWE-521: Weak Password Requirements

Sensitive Data Exposure via Backup File

Description:
A publicly accessible backup file was discovered during scanning, potentially leaking sensitive data.

Tool Used: Nikto
URL Discovered: https://cwe.mitre.org/data/definitions/530.html

Command Used:

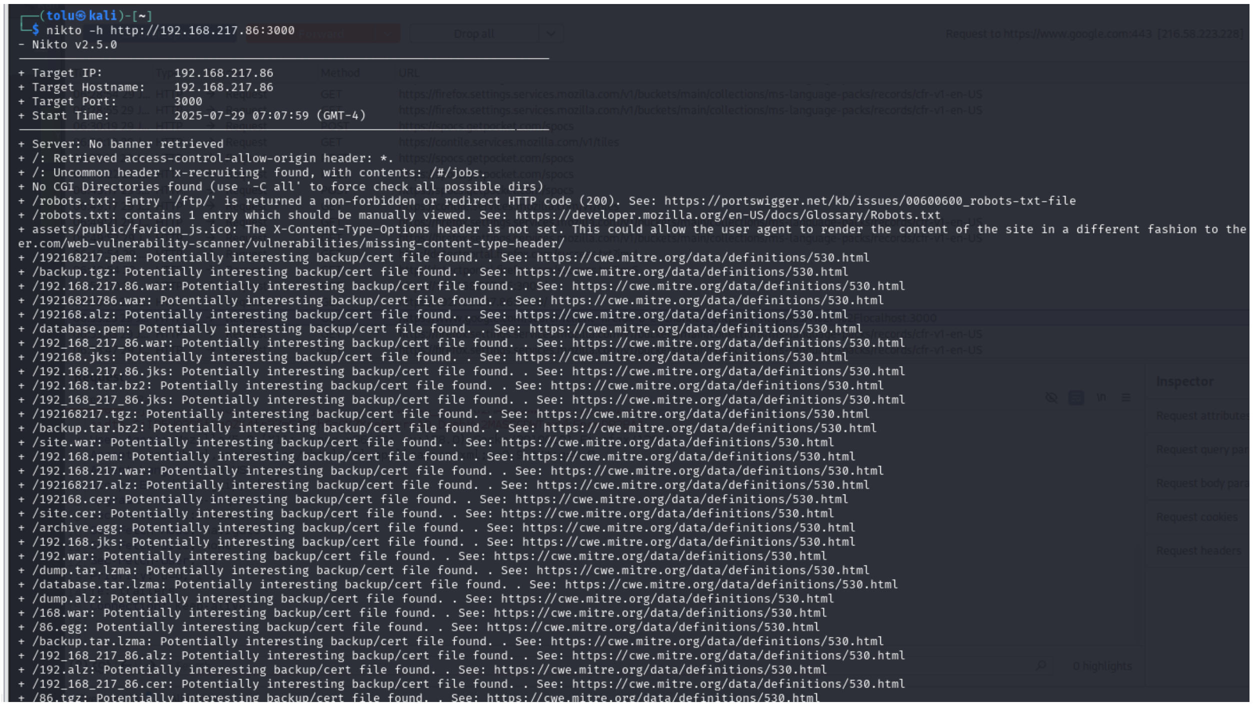
```
wget https://cwe.mitre.org/data/definitions/530.html
```

Impact:

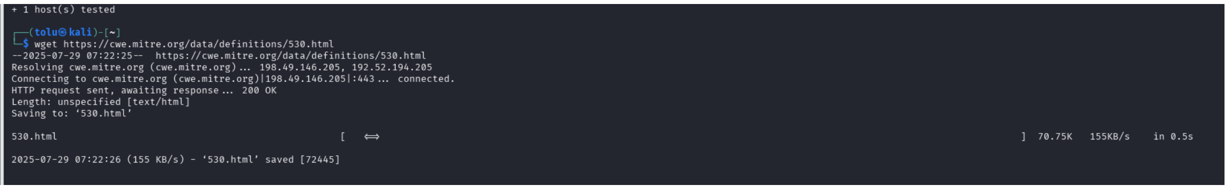
Backup files may include:

- Application source code
- Database credentials
- API keys
- Business logic

Screenshot Evidence:



```
┌──(tolu㉿kali)-[~]
└─$ nikto -h http://192.168.217.86:3000
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.217.86
+ Target Hostname:    192.168.217.86
+ Target Port:        3000
+ Start Time:         2025-07-29 07:07:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ assets/public/favicon_js.ico: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
er.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /192168217.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.217.86.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /19216821786.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_217_86.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.217.86.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_217_86.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168217.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.217.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168217.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /86.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_217_86.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_217_86.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /86.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

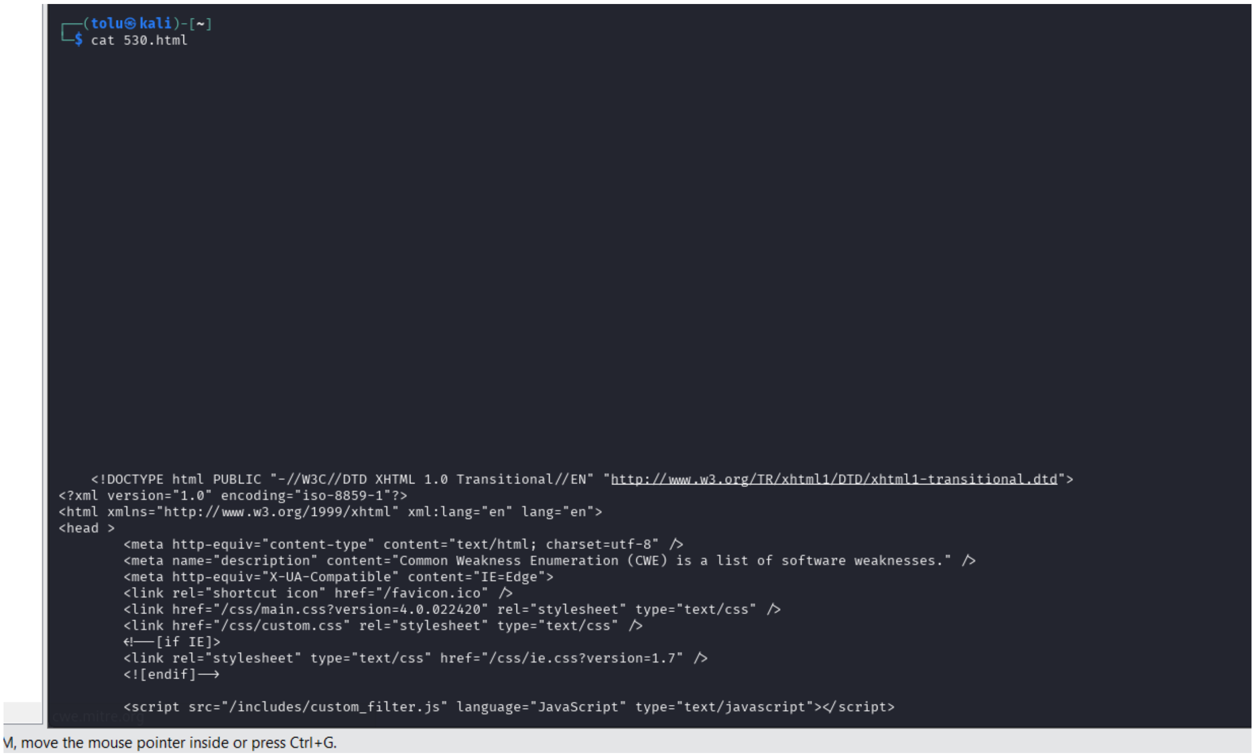


```
+ 1 host(s) tested

┌──(tolu㉿kali)-[~]
└─$ wget https://cwe.mitre.org/data/definitions/530.html
--2025-07-29 07:22:25--  https://cwe.mitre.org/data/definitions/530.html
Resolving cwe.mitre.org (cwe.mitre.org)... 198.49.146.205, 192.52.194.205
Connecting to cwe.mitre.org (cwe.mitre.org)|198.49.146.205|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘530.html’

530.html                              [   <=>                                                                          ]  70.75K   155KB/s    in 0.5s

2025-07-29 07:22:26 (155 KB/s) - ‘530.html’ saved [72445]
```



```
┌──(tolu㉿kali)-[~]
└─$ cat 530.html

    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<?xml version="1.0" encoding="iso-8859-1"?>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head >
        <meta http-equiv="content-type" content="text/html; charset=utf-8" />
        <meta name="description" content="Common Weakness Enumeration (CWE) is a list of software weaknesses." />
        <meta http-equiv="X-UA-Compatible" content="IE=Edge">
        <link rel="shortcut icon" href="/favicon.ico" />
        <link href="/css/main.css?version=4.0.022420" rel="stylesheet" type="text/css" />
        <link href="/css/custom.css" rel="stylesheet" type="text/css" />
        <!--[if IE]>
        <link rel="stylesheet" type="text/css" href="/css/ie.css?version=1.7" />
        <![endif]-->

        <script src="/includes/custom_filter.js" language="JavaScript" type="text/javascript"></script>
```

M, move the mouse pointer inside or press Ctrl+G.

Screenshot showing Nikto output or the downloaded backup file.

Mitigation:

- Avoid storing backups in web-accessible locations
- Restrict file access with proper permissions
- Regularly audit deployment directories
- Automate backup removal via CI/CD

Reference:

- CWE-530: Exposure of Backup File
- OWASP A06:2021 - Vulnerable and Outdated Components

Recommendations Summary

- Implement input validation and output encoding
- Remove or secure default credentials
- Restrict public access to sensitive files

- Regularly scan applications for known vulnerabilities
- Align with OWASP secure coding best practices

Tools Used:

- **Nikto**: Web server vulnerability scanner
- **Burp Suite**: Manual and automated web app testing
- **Wget**: For downloading exposed files