REPORT ON THE OWASPBWA

Student Name

Oluwatimilehin Oluwagbemi

Reg. No

2025/GRC/10712

24th September, 2025

Course Title

GRC 103 – Risk Assessment and Management Techniques

To: CISO & Application Development Management

From: GRC Audit Team

Date: 23rd September, 2025

Subject: Critical OWASP Top 10 Findings in Legacy Web Applications.

Executive Summary:

The OWASP Broken Web Applications (BWA) virtual lab was tested in the context of governance, risk, and compliance (GRC). This assessment is a summary of the results. The goal was to check the security of the vulnerable web apps that were already in use, find the most important or important issues, connect the found flaws to common control frameworks like OWASP Top 10, PCI DSS, NIST CSF and relevant regulatory requirements, and then make suggestions for how to fix the problems.

An assessment of the OWASPBWA server revealed multiple severe web application vulnerabilities that align with the OWASP Top 10 such as SQL Injection, Broken Access Control, Cryptographic Failures and Identification Failures. These findings indicate a systemic failure in our Secure Development Lifecycle (SDLC) and pose a direct threat to customer and company data.

Key Findings & Risks:

- Critical Risk – Data Breach Vector: Several applications were found to be vulnerable to SQL Injection (A03:2021). This could allow an attacker to steal, modify or delete the entire application database.
- Critical Risk – Broken Access Controls (A01:2021): Administrative interfaces were accessible without proper authentication, allowing any user to gain privileged access to application functions and data.
- High Risk – Lack of Encryption (A02:2021): User credentials were observed being transmitted without encryption, making them susceptible to interception.

Recommended Actions:

1. Immediate Mitigation: isolate the affected systems from any network reachable by untrusted users.
2. Remediation: The development team must prioritize fixing these vulnerabilities using OWASP proactive controls and cheat sheets.
3. Process Improvement: Mandate formal security training for developers focused on the OWASP Top 10. Integrate SAST/DAST tools (like Burp Suite) into the CI/CD pipeline.
4. Penetration Testing: Commission a full third-party penetration test before any similar applications is delayed in production.

Phase 1 – Discovery and Reconnaissance

Step 1: Target Discovery

The owaspbwa which serves as the target was powered on, I ran the 'ifconfig' command to get the IP address that will be pinged on Kali Linux which is the attack machine. The command returns the IP address '192.18.1.4' which was pinged on kali using the command 'ping -c 4 192.168.1.4' and it returned a response which showed that the target is alive.

Step 2: Service Enumeration

This step involves the identification of the type of services running on the server, and the open ports on the server. The task was carried out using the command ' nmap -sV -sC -O -p- -oA initial_scan 192.168.1.4'

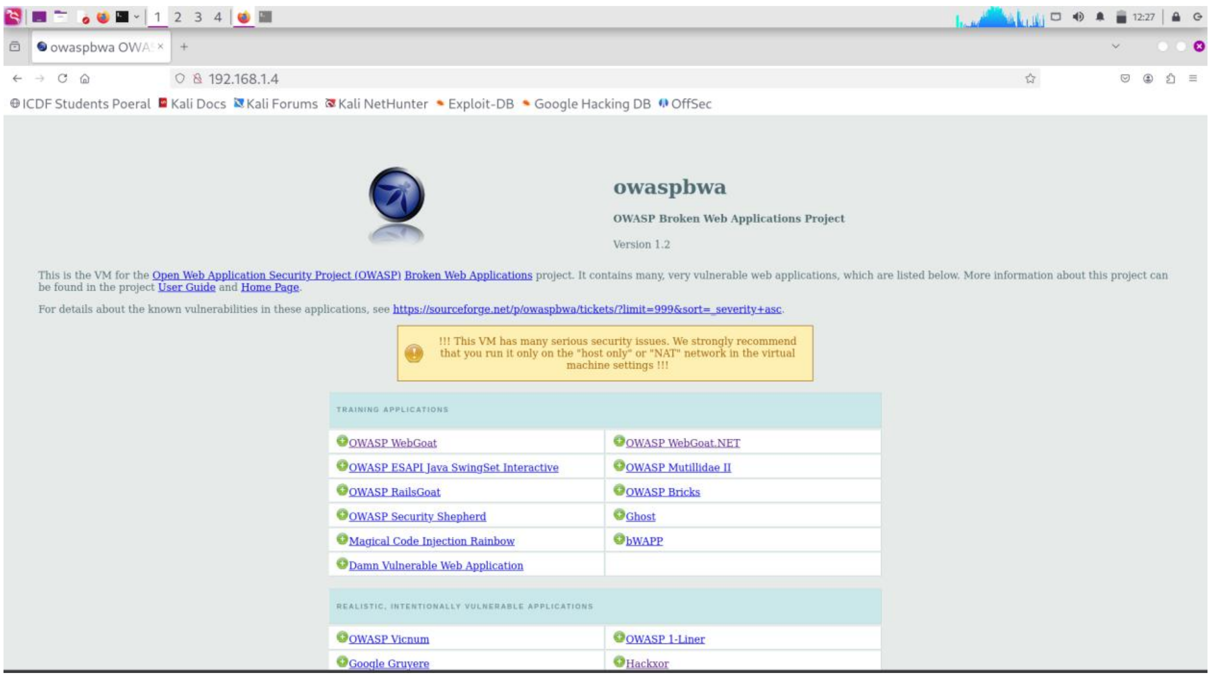
The command generated a report of the open ports on the server. The ports opened are:

- 22 – SSH running tcp, the version is 5.31p1 Debian 3ubuntu4, this poses a risk of backdoor, the ssh-hostkey is also exposed with the type of service such as DSA and RSA, this poses a compliance violation.
- 80, 8080 – HTTP running tcp is open with potentially risky methods such as TRACE, the server is running an outdated version of Apache 2.2.14, this can be exploited to compromise the server.
- 139 & 445 – NETBIOS-SSN running tcp is open, the server is running Samba smbd 3.X – 4.X which is an outdated version, this poses a compliance violation.
- 143 – IMAP
- 443, 8081– HTTPS running tcp is open with potentially risky methods such as TRACE, the server is running an outdated version of Apache 2.2.14, this can be exploited to compromise the server.

Nmap full scan report: https://drive.google.com/file/d/194UmG-N6rsNlUvi3Yda5s-uZ0iz_sSCN/view?usp=sharing

Step 3: Application Discovery

The target was further explored to find vulnerable applications running on the server, to achieve this, I opened the target IP address on Firefox browser; http://192.168.1.4, and I saw a directory listing available applications such as WordPress, WebGoat, Hackxnor, DVWA, BodgeIt Store and many more. Find the screenshot of the directory listing below:



owaspbwa

OWASP Broken Web Applications Project

Version 1.2

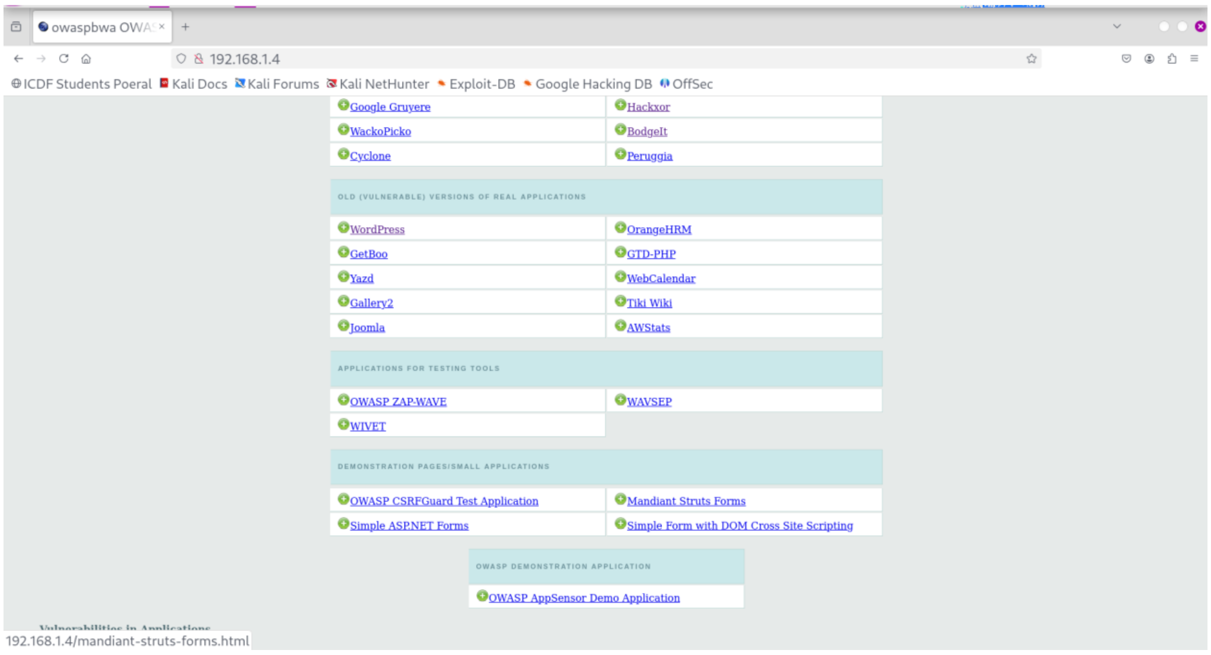
This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS	
OWASP Vicnum	OWASP 1-Liner
Google Gruyere	Hackxor



Google Gruyere	Hackxor
WackoPicko	BodgeIt
Cyclone	Peruggia

OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS	
WordPress	OrangeHRM
GetBoo	GTD-PHP
Yazd	WebCalendar
Gallery2	Tiki Wiki
Joomla	AWStats

APPLICATIONS FOR TESTING TOOLS	
OWASP ZAP-WAVE	WAVSEP
WIVET	

DEMONSTRATION PAGES/SMALL APPLICATIONS	
OWASP CSRFGuard Test Application	Mandiant Struts Forms
Simple ASP.NET Forms	Simple Form with DOM Cross Site Scripting

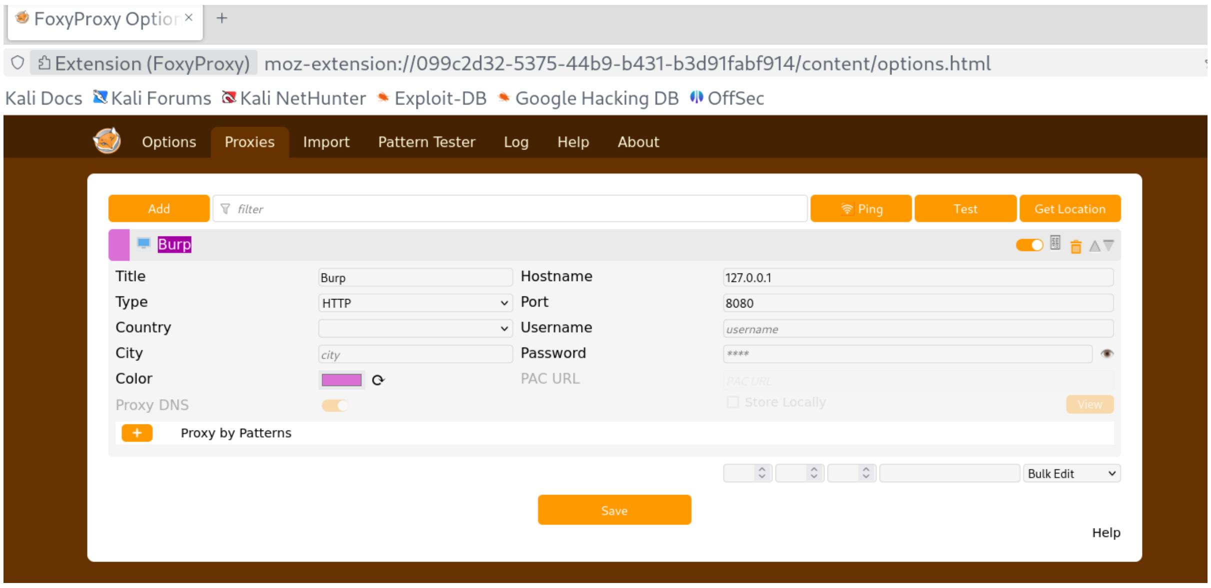
OWASP DEMONSTRATION APPLICATION
OWASP AppSensor Demo Application

192.168.1.4/mandiant-struts-forms.html

Phase 2: Tool Configuration & Automated Scanning

Step 4: Configuring Burp Suite Professional

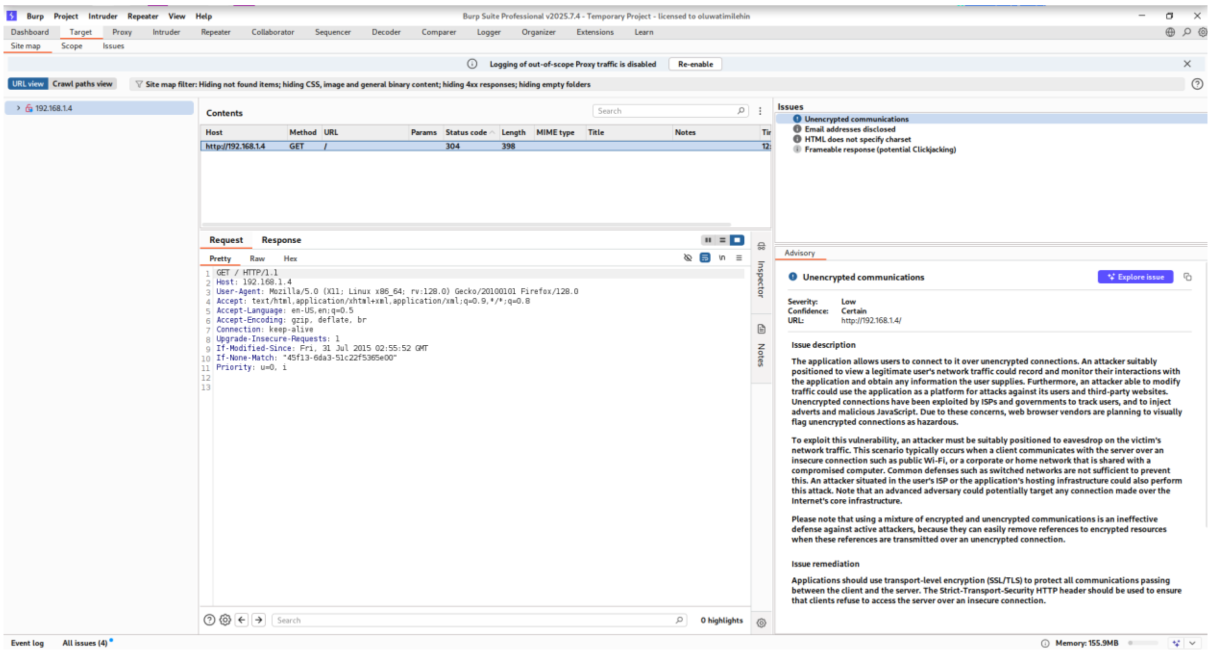
To set up my environment to route traffic through Burp, I launched my Burp Suite Professional, navigate to my Firefox browser, installed foxyproxy an adds-on that enables traffic interception. Then I set up my foxy proxy using the proxy settings in Burp Suite Professional ‘Proxy: 127.0.0.1, Port: 8080’.


moz-extension://099c2d32-5375-44b9-b431-b3d91fabf914/content/options.html

Title	Burp	Hostname	127.0.0.1
Type	HTTP	Port	8080
Country		Username	username
City	city	Password	****
Color		PAC URL	
Proxy DNS			

In order to route traffic from my browser to the Burp Suite, it is essential to turn on intercept which is a feature on the proxy tab.

Then I browsed to http://192.168.1.4, forwarded the request to populate the Site map


Burp Suite Professional v2025.7.4 - Temporary Project - licensed to oluwatimilehin

Logging of out-of-scope Proxy traffic is disabled

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
http://192.168.1.4	GET	/		304	398			

Issues
- Unencrypted communications
- Email addresses disclosed
- HTML does not specify charset
- Frameable response (potential Clickjacking)

```
GET / HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 31 Jul 2015 02:55:52 GMT
If-None-Match: "45f13-6da3-51c22f5365e00"
Priority: u=0, i


```

Unencrypted communications

Severity: Low
Confidence: Certain
URL: http://192.168.1.4/

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

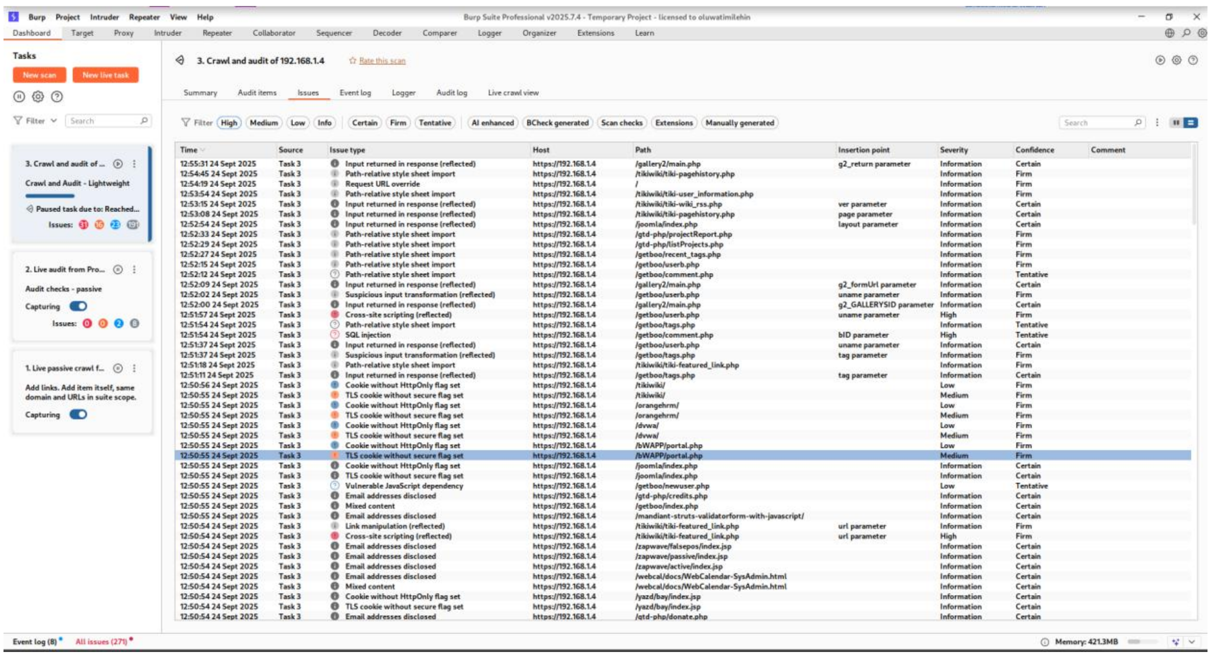
Issue remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

Memory: 155.9MB

Step 5: Automated Passive & Active Scanning

After populating the site map, I right clicked on the folder and selected scan to scan the website for vulnerabilities.


Burp Suite Professional v2025.7.4 - Temporary Project - licensed to oluwatimilehin

3. Crawl and audit of 192.168.1.4

Tasks: 3. Crawl and audit of ... — Crawl and Audit - Lightweight — Paused task due to: Reached...
2. Live audit from Pro... — Audit checks - passive — Capturing
1. Live passive crawl f... — Add links. Add item itself, same domain and URLs in suite scope. — Capturing

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
12:55:31 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/gallery2/main.php	g2_return parameter	Information	Certain	
12:54:45 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/tikiwiki/tiki-pagehistory.php		Information	Firm	
12:54:19 24 Sept 2025	Task 3	Request URL override	https://192.168.1.4	/		Information	Firm	
12:53:54 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/tikiwiki/tiki-user_information.php		Information	Firm	
12:53:15 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/tikiwiki/tiki-wiki_rss.php	ver parameter	Information	Certain	
12:53:08 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/tikiwiki/tiki-pagehistory.php	page parameter	Information	Certain	
12:52:54 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/joomla/index.php	layout parameter	Information	Certain	
12:52:33 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/gtd-php/projectReport.php		Information	Firm	
12:52:29 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/gtd-php/listProjects.php		Information	Firm	
12:52:27 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/getboo/recent_tags.php		Information	Firm	
12:52:15 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/getboo/userb.php		Information	Firm	
12:52:12 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/getboo/comment.php		Information	Tentative	
12:52:09 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/gallery2/main.php	g2_formUrl parameter	Information	Certain	
12:52:02 24 Sept 2025	Task 3	Suspicious input transformation (reflected)	https://192.168.1.4	/getboo/userb.php	uname parameter	Information	Firm	
12:52:00 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/gallery2/main.php	g2_GALLERYSID parameter	Information	Certain	
12:51:57 24 Sept 2025	Task 3	Cross-site scripting (reflected)	https://192.168.1.4	/getboo/userb.php	uname parameter	High	Firm	
12:51:54 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/getboo/tags.php		Information	Tentative	
12:51:54 24 Sept 2025	Task 3	SQL injection	https://192.168.1.4	/getboo/comment.php	bID parameter	High	Tentative	
12:51:37 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/getboo/userb.php	uname parameter	Information	Certain	
12:51:37 24 Sept 2025	Task 3	Suspicious input transformation (reflected)	https://192.168.1.4	/getboo/tags.php	tag parameter	Information	Firm	
12:51:18 24 Sept 2025	Task 3	Path-relative style sheet import	https://192.168.1.4	/tikiwiki/tiki-featured_link.php		Information	Firm	
12:51:11 24 Sept 2025	Task 3	Input returned in response (reflected)	https://192.168.1.4	/getboo/tags.php	tag parameter	Information	Certain	
12:50:56 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/tikiwiki/		Low	Firm	
12:50:55 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/tikiwiki/		Medium	Firm	
12:50:55 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/orangehrm/		Low	Firm	
12:50:55 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/orangehrm/		Medium	Firm	
12:50:55 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/dvwa/		Low	Firm	
12:50:55 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/dvwa/		Medium	Firm	
12:50:55 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/bWAPP/portal.php		Low	Firm	
12:50:55 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/bWAPP/portal.php		Medium	Firm	
12:50:55 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/joomla/index.php		Information	Certain	
12:50:55 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/joomla/index.php		Information	Certain	
12:50:55 24 Sept 2025	Task 3	Vulnerable JavaScript dependency	https://192.168.1.4	/getboo/newuser.php		Low	Tentative	
12:50:55 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/gtd-php/credits.php		Information	Certain	
12:50:55 24 Sept 2025	Task 3	Mixed content	https://192.168.1.4	/getboo/index.php		Information	Certain	
12:50:55 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/mandiant-struts-validatorform-with-javascript/		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Link manipulation (reflected)	https://192.168.1.4	/tikiwiki/tiki-featured_link.php	url parameter	Information	Firm	
12:50:54 24 Sept 2025	Task 3	Cross-site scripting (reflected)	https://192.168.1.4	/tikiwiki/tiki-featured_link.php	url parameter	High	Firm	
12:50:54 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/zapwave/falsepos/index.jsp		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/zapwave/passive/index.jsp		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/zapwave/active/index.jsp		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/webcal/docs/WebCalendar-SysAdmin.html		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Mixed content	https://192.168.1.4	/webcal/docs/WebCalendar-SysAdmin.html		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Cookie without HttpOnly flag set	https://192.168.1.4	/yazd/bay/index.jsp		Information	Certain	
12:50:54 24 Sept 2025	Task 3	TLS cookie without secure flag set	https://192.168.1.4	/yazd/bay/index.jsp		Information	Certain	
12:50:54 24 Sept 2025	Task 3	Email addresses disclosed	https://192.168.1.4	/gtd-php/donate.php		Information	Certain	

Event log (8) · All issues (271) · Memory: 421.3MB

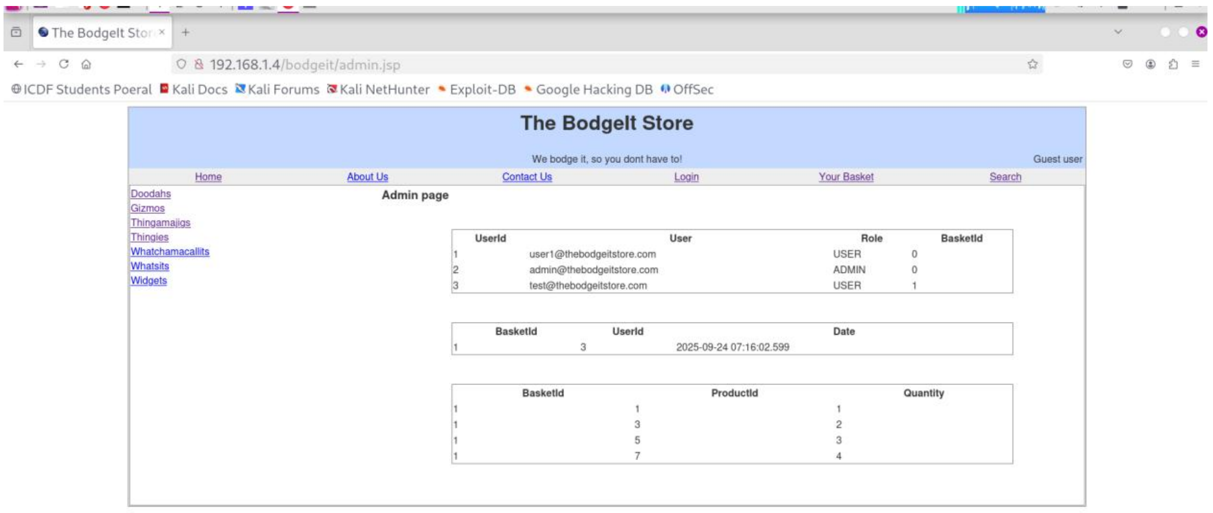
https://drive.google.com/file/d/1pvlaBZtvouqkdqBEond7KtOZmSv2j5Z8/view?usp=sharing

https://drive.google.com/file/d/1o0J45RD2oKQuJzIFu9WJNsBEQt0fEzdk/view?usp=sharing

Step 6: Testing for A01:2021-Broken Access Control (BodgeIt Store)

Using BodgeIt Store to test for broken access control, which is a critical failure in authorization policies, directly violating the principle of least privilege, I tried to access an administrative page directly using the url http://192.168.1.4/bodgeit/admin.jsp and i was able to access the admin page of the web site, this is a critical risk violating PCI DSS 7.2.1, because unauthorized person can have access to credentials of everyone that has logged in to that website.

A01:2021-Broken Access Control doesn't follow PCI DSS 7.2.1, which says that access control systems should use least privilege and need-to-know. The found flaws allow for increased privileges and unauthorized access to data, showing a lack of compliance.



Admin page

UserId	User	Role	BasketId
1	user1@thebodgeitstore.com	USER	0
2	admin@thebodgeitstore.com	ADMIN	0
3	test@thebodgeitstore.com	USER	1

BasketId	UserId	Date
1	3	2025-09-24 07:16:02.599

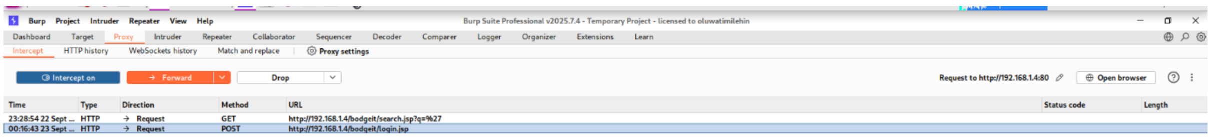
BasketId	ProductId	Quantity
1	1	1
1	3	2
1	5	3
1	7	4

Step 7: Testing for A02:2021-Cryptographic Failures (WebGoat)

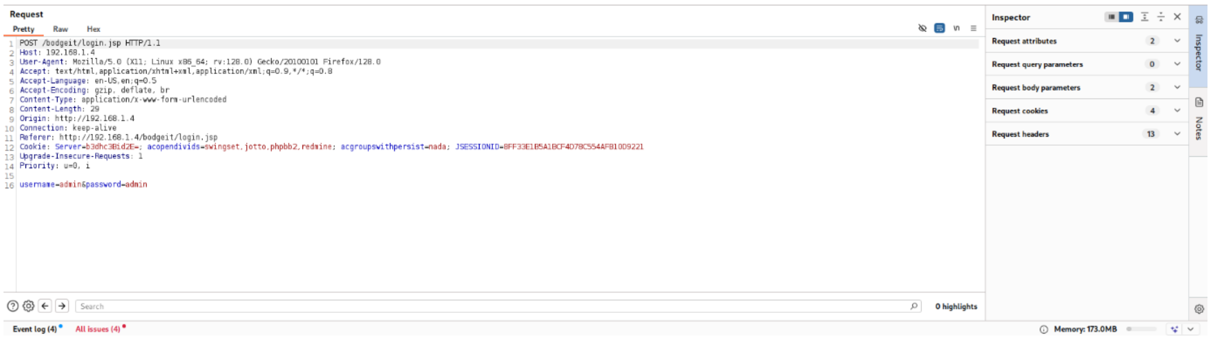
WebGoat application was used to test for cryptographic failure on the server, which means the transmitting of passwords in cleartext, which is a severe violation of every data protection standards including GDPR and PCI DSS, which poses risk of information disclosure.

The application (WebGoat) was used to test for this vulnerability, and the result showed that it is vulnerable, I used Burp Suite to intercept the traffic of the operation carried out on WebGoat which is randomly inputting password and username to check for this vulnerability, turning on the intercept, from the proxy tab, I clicked on the HTTP history tab to get the information captured by Burp Suite, then looked for the POST request that contained a password, from the raw request, the password returned is a plaintext.

PCI DSS Requirement 4.1 says if there is need to send sensitive data over an open network, it must be pass through strong encryption technique. A02:2021-Cryptographic Failures map directly to this need. Cardholder data can be stolen because weak or missing encryption mechanisms are known to be used. This is a breach of compliance.


Burp Project Intruder Repeater View Help
Burp Suite Professional v2025.7.4 - Temporary Project - licensed to oluwatimilehin
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.1.4:80
Open browser

Time	Type	Direction	Method	URL	Status code	Length
23:28:54 22 Sept ...	HTTP	→ Request	GET	http://192.168.1.4/bodgeit/search.jsp?q=%27		
00:16:43 23 Sept ...	HTTP	→ Request	POST	http://192.168.1.4/bodgeit/login.jsp		



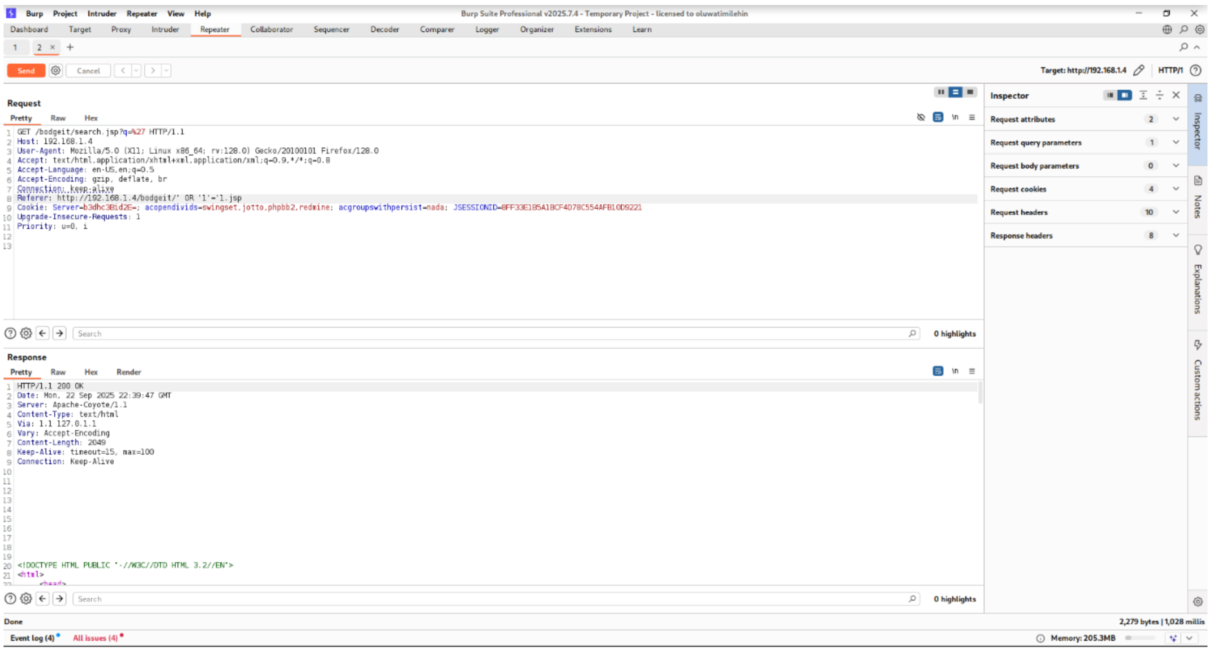
```
POST /bodgeit/login.jsp HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://192.168.1.4
Connection: keep-alive
Referer: http://192.168.1.4/bodgeit/login.jsp
Cookie: Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=8FF33E1B5A1BCF4D78C554AFB10D9221
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=admin
```

Step 8: Testing for A03:2021-Injection (BodgeIt Store Search)

To test for SQL Injection, the BodgeIt Store application was used and the results indicate that the application is vulnerable to SQL Injection which is a classic high-impact vulnerablity, which can lead to full data breach as attackers can inject malicious code, this violates data integrity and confidentiality policies.

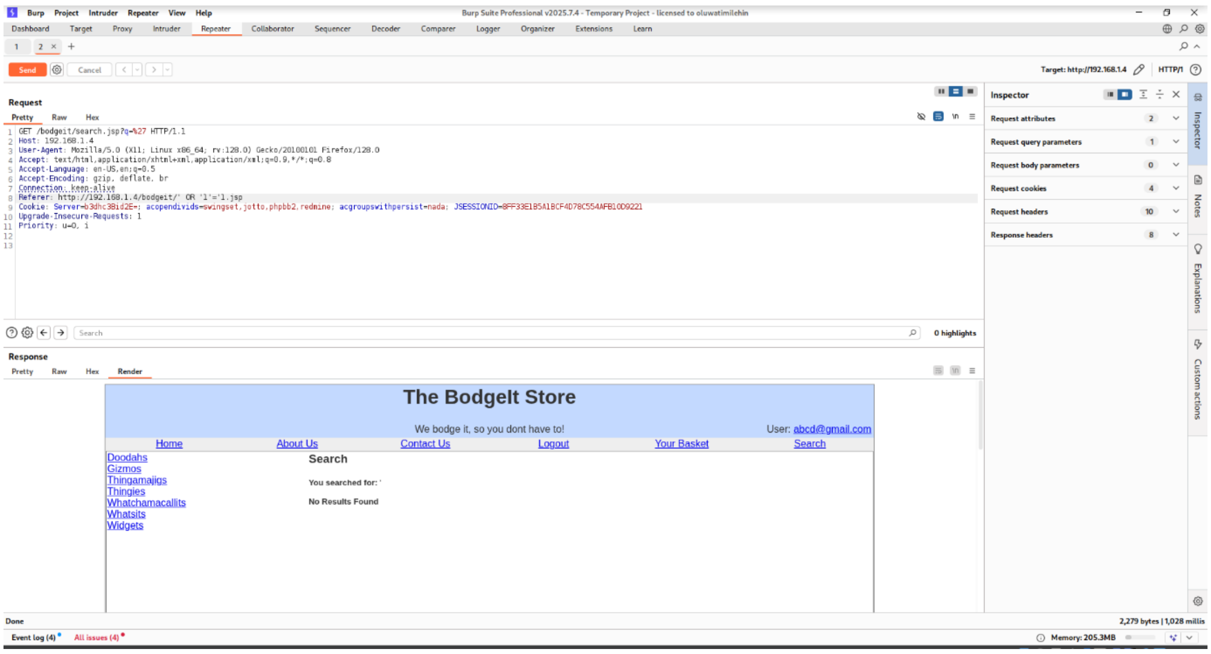
The process started by turning on intercept in Burp, while on the WebGoat Application, I navigated to the search bar and inputted the codes used to test for SQL Injection, the codes used are: ‘, ‘ OR ‘1’=’1 and ‘ UNION SELECT 1,2,3,4,5,6 which returned items using the Repeater in Burp Suite. The HTTP response was OK code 200, no error was returned for each code. This proved that the site is vulnerable to SQL Injection.

A03:2021-Injection and PCI DSS 6.5.1 both addresses injection vulnerabilities. PCI DSS 6.5.1 says that custom applications must find and fix injection flaws like SQL injection. It's against the rules not to fix these issues, and someone could get to your data without proper authorization/permission.


Burp Suite Professional v2025.7.4 - Temporary Project - licensed to oluwatimilehin
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: http://192.168.1.4 HTTP/1
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 4
Request headers 10
Response headers 8
0 highlights
Response
Pretty Raw Hex Render
Done
2,279 bytes | 1,028 millis
Event log (4) All issues (4)
Memory: 205.3MB

```
GET /bodgeit/search.jsp?q=%27 HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.1.4/bodgeit/' OR '1'='1.jsp
Cookie: Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=8FF33E1B5A1BCF4D78C554AFB10D9221
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Mon, 22 Sep 2025 22:39:47 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Content-Length: 2049
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive










<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<html>
    <head>
```


Burp Suite Professional v2025.7.4 - Temporary Project - licensed to oluwatimilehin
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: http://192.168.1.4 HTTP/1
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 4
Request headers 10
Response headers 8
0 highlights
Response
Pretty Raw Hex Render
Done
2,279 bytes | 1,028 millis
Event log (4) All issues (4)
Memory: 205.3MB

```
GET /bodgeit/search.jsp?q=%27 HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.1.4/bodgeit/' OR '1'='1.jsp
Cookie: Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=8FF33E1B5A1BCF4D78C554AFB10D9221
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

The BodgeIt Store

We bodge it, so you dont have to! User: abcd@gmail.com

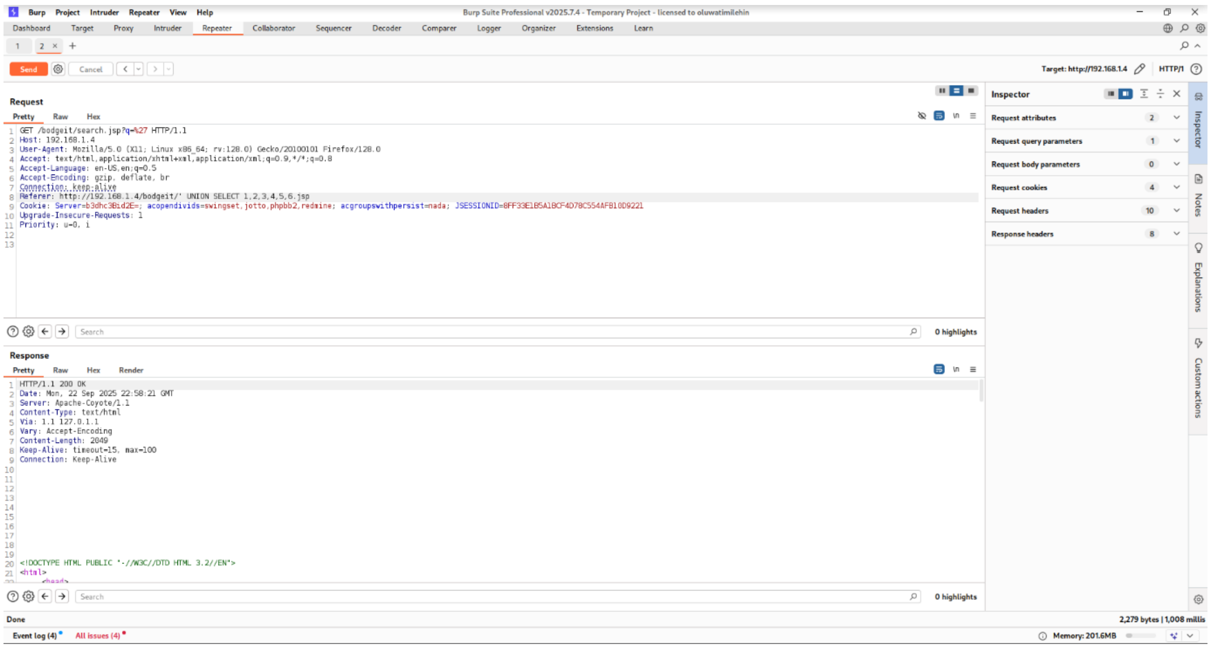
Home | About Us | Contact Us | Logout | Your Basket | Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

Search

You searched for: '

No Results Found



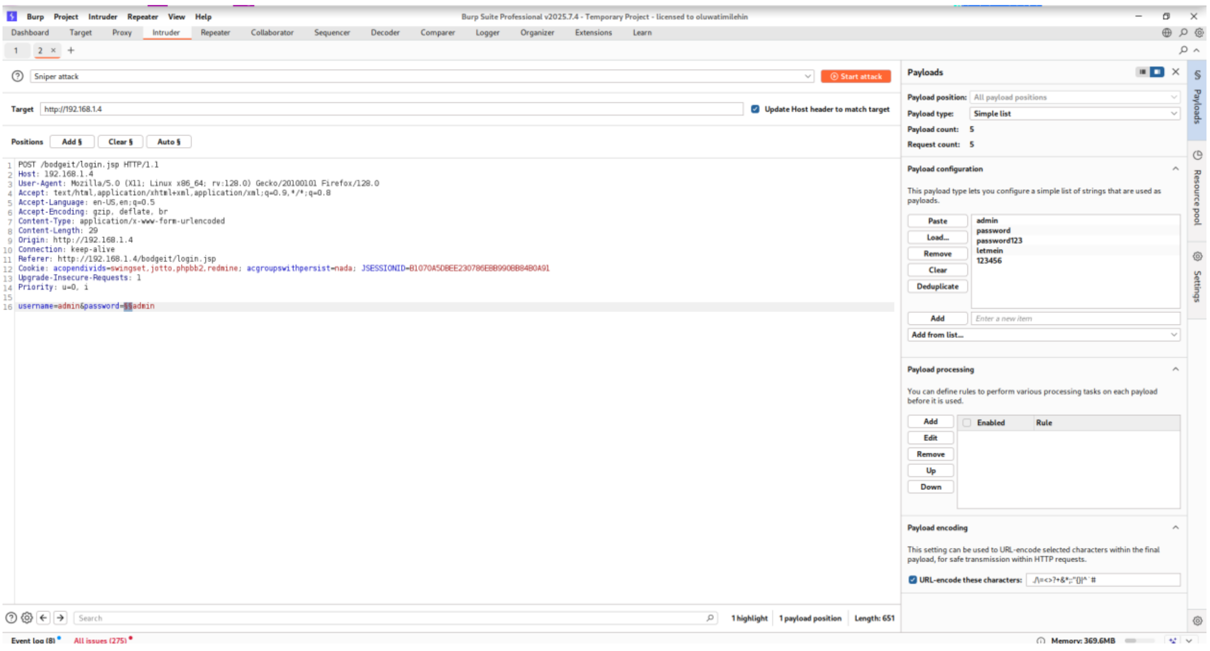
```
GET /bodgeit/search.jsp?q=%27 HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.1.4/bodgeit/' UNION SELECT 1,2,3,4,5,6.jsp
Cookie: Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=8FF33E1B5A1BCF4D78C554AFB10D9221
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Mon, 22 Sep 2025 22:58:21 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html
Via: 1.1 127.0.1.1
Vary: Accept-Encoding
Content-Length: 2049
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive










<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<html>
```

Step 9: Testing for A07:2021-Identification and Authentication Failures (BodgeIt Login)

To test for weak authentication mechanisms using Burp Suite Intruder, I navigated to the login page tried out weak credentials such as admin:admin and test:test, turned on the intercept and clear all payloads and setting a new one for the password parameter. I added list of payloads such as password, admin, 123456, letmein, password123 to check for a response with a different length or status code which might indicate a successful login.

A07:2021-Identification Failures results in problems with identifying and authenticating people. This is non-compliant to NIST CSF PR.AC-1, which says that identities and credentials should be safely issued, checked, and managed. It has been found that using default credentials and weak authentication controls goes against PR.AC-1 and lets people in who aren't supposed to be there.



Sniper attack

Target: http://192.168.1.4

```
POST /bodgeit/login.jsp HTTP/1.1
Host: 192.168.1.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://192.168.1.4
Connection: keep-alive
Referer: http://192.168.1.4/bodgeit/login.jsp
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; JSESSIONID=B1070A5DBEE230786EBB990BB84B0A91
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=§§admin
```

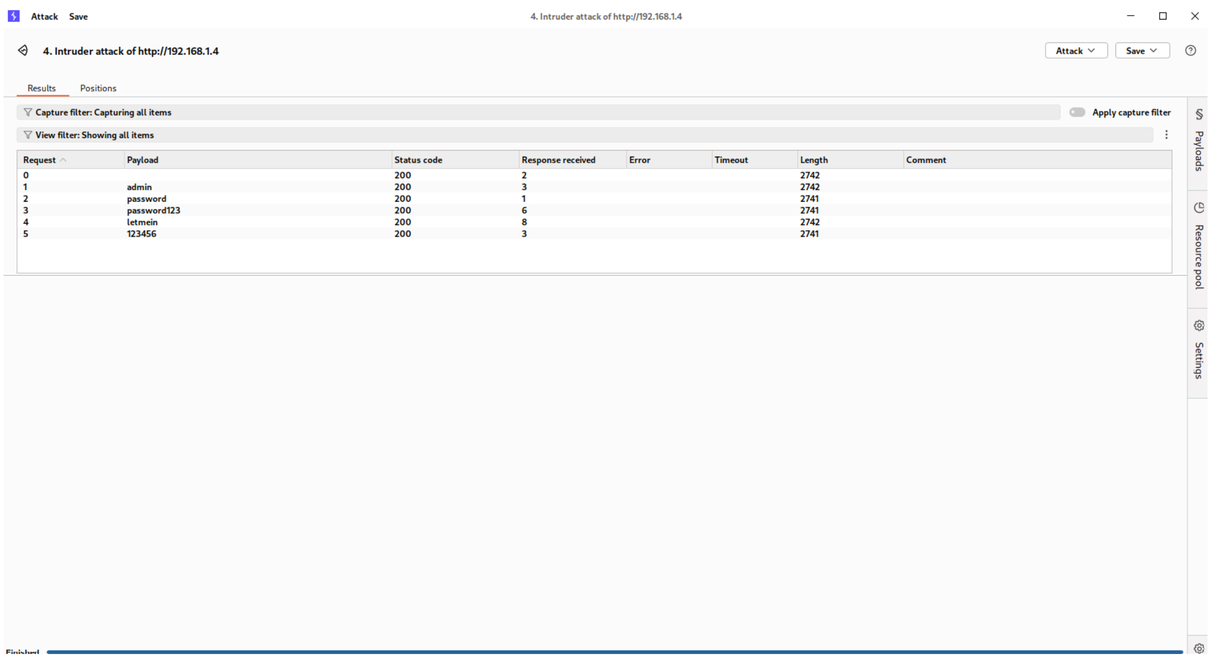
Payloads

Payload position:	All payload positions
Payload type:	Simple list
Payload count:	5
Request count:	5

Payload configuration: admin, password, password123, letmein, 123456

URL-encode these characters: ./\=<>?+&*;:"{}|^`#

1 highlight | 1 payload position | Length: 651



4. Intruder attack of http://192.168.1.4

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	2			2742	
1	admin	200	3			2742	
2	password	200	1			2741	
3	password123	200	6			2741	
4	letmein	200	8			2742	
5	123456	200	3			2741	

Phase 4: Analysis and Reporting

Step 10: Triage and Risk Assessment

OWASP Top 10 Category	Vulnerability Example	Affected Application	Inherent Risk (L,M,H)	Compliance Violation	Business Impact
A01: Broken Access Control	Unprotected Admin Page	BodgeIt Store	H	PCI DSS 7.2.1	Unauthorized data access, privilege escalation
A02: Cryptographic Failures	Cleartext Password Transmission	WebGoat	H	PCI DSS 4.1	Credential theft, account takeover

A03: Injection	SQL Injection in Search	BodgeIt Store	H	PCI DSS 6.5.1	Full Database compromise, data loss
A07: Identification Failures	Weak Password Policy	BodgeIt Store	M/H	NIST CSF PR.AC -1	Unauthorized access, initial breach vector.