DVWA

Security Assessment Findings Report

Business Confidential

Date: *Nov 23, 2022*

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and the tester. 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 tester.

The Tester 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.

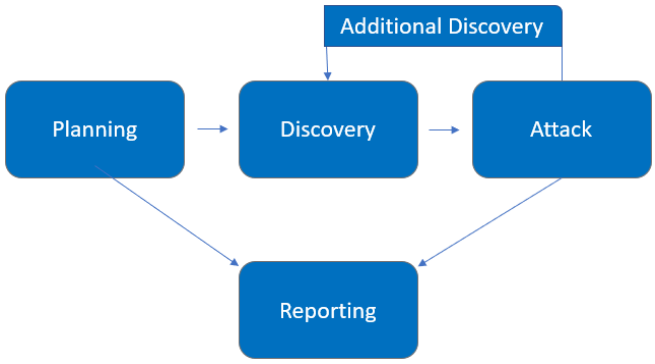
Time-limited engagements do not allow for a full evaluation of all security controls. The tester prioritized the assessment to identify the weakest security controls an attacker would exploit. The tester recommends conducting similar assessments on an annual basis by internal or third-party assessors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

Assessment Overview

From November 10,2022 to November 22, 2022, The tester evaluated the security posture of DVWA compared to current industry best practices that included an web Application Security test. All testing performed is based on the *OWASP Testing Guide (v4).*

Phases of web application testing activities include the following:

- Planning – Understanding the underlying vulnerabilities.
- Discovery – Perform manual testing of the application endpoints and vulnerabilities.
- Attack – Confirm potential vulnerabilities through exploitation.
- Reporting – Document all found vulnerabilities and exploits.



Assessment Components

Web Application Security Test

A web application security test emulates the role of an attacker attempting to gain access to a web application without internal resources or inside knowledge. The engineer performs scanning and enumeration to identify potential underlying technologies and vulnerabilities in hopes of exploitation. Which is then followed by manual testing with tools to confirm and exploit vulnerabilities. The necessary evidence is then gathered in forms of screenshots, reports and charts to convey them.

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	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	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	4.0-6.9	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	0.1-3.9	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
Web Application - DVWA	local IP.

Scope Exclusions

Contained within the present site.

Client Allowances

No allowances were given.

Executive Summary

The tester evaluated DVWA's security posture through a web application security test from November 10, 2022 to November 22, 2022. By leveraging a series of attacks, The tester found critical level vulnerabilities that allowed full access to the DVWA application. It is highly recommended that DVWA address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

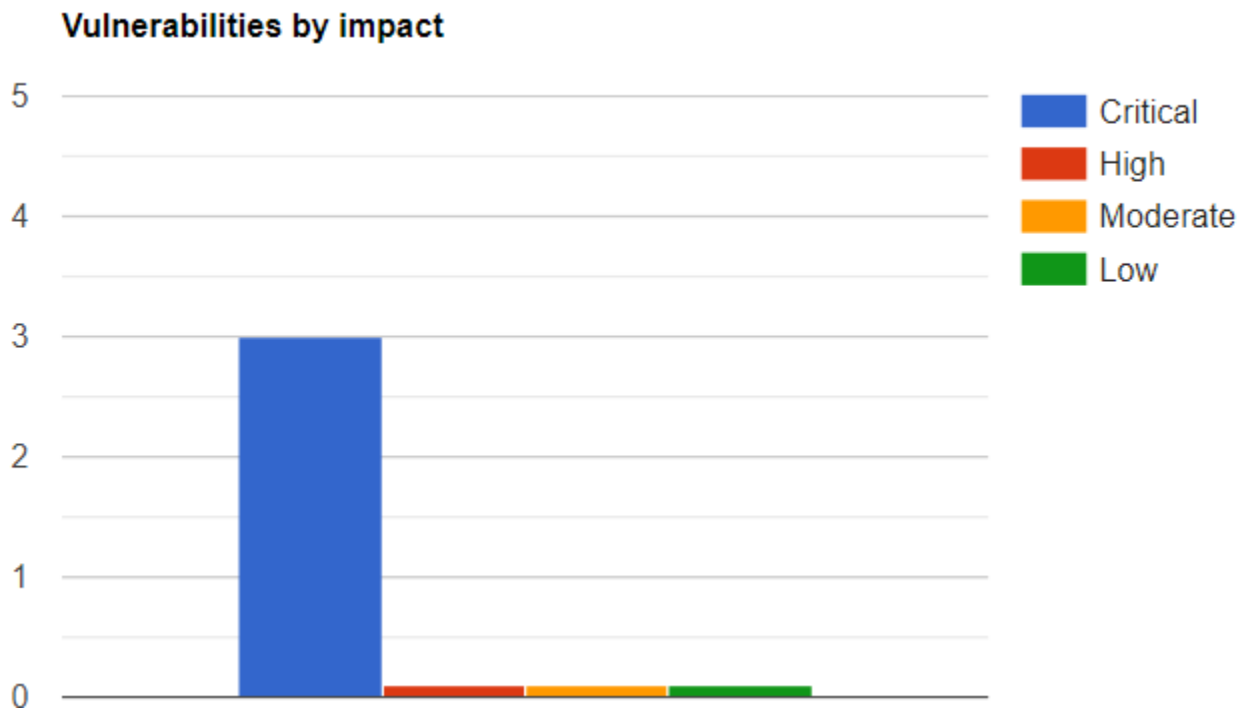
The following table describes how TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	JavaScript Bypass : Understand what the underlying javascript is doing and reverse engineer the token. Pass the token and desired phrase to pass the challenge.	Use secure algorithms to implement tokens which are computationally infeasible and client side firewall configurations.

2	CSP Bypass : Understand how the CSP of the particular site works and bypass using malicious payloads.	Only allow trusted sources to make requests and implement client and server side protections.
3	Weak session ID : Generate the cookie and check for patterns or logic of the cookie.	Use Secure algorithms to generate cookies which are computationally infeasible.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

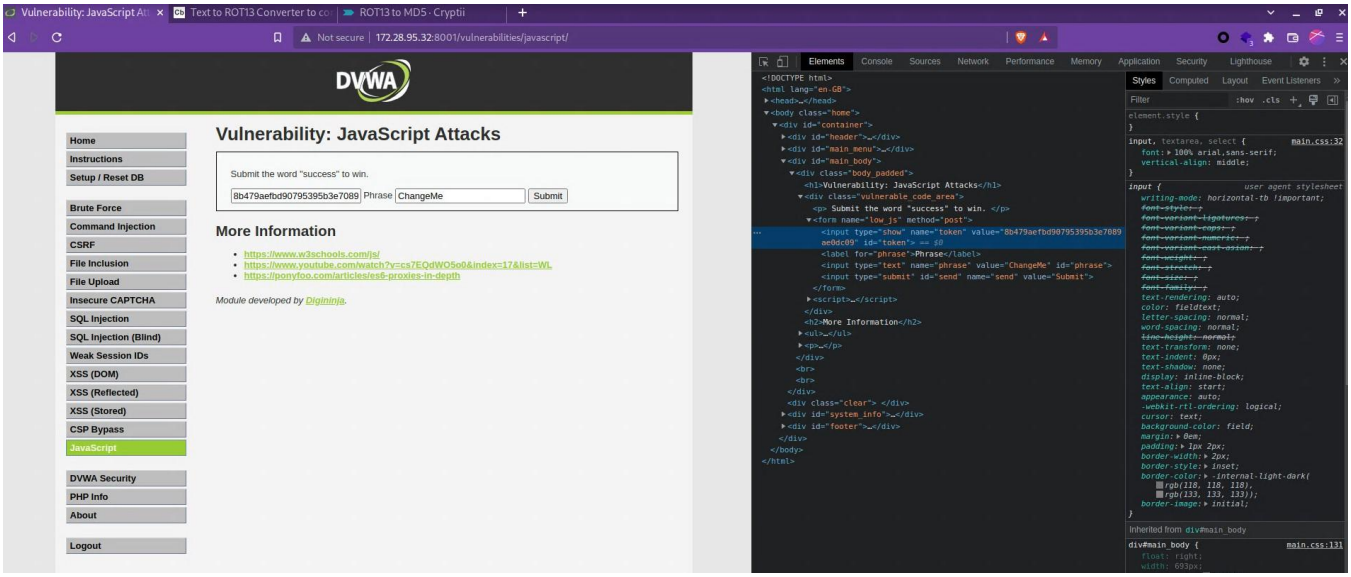


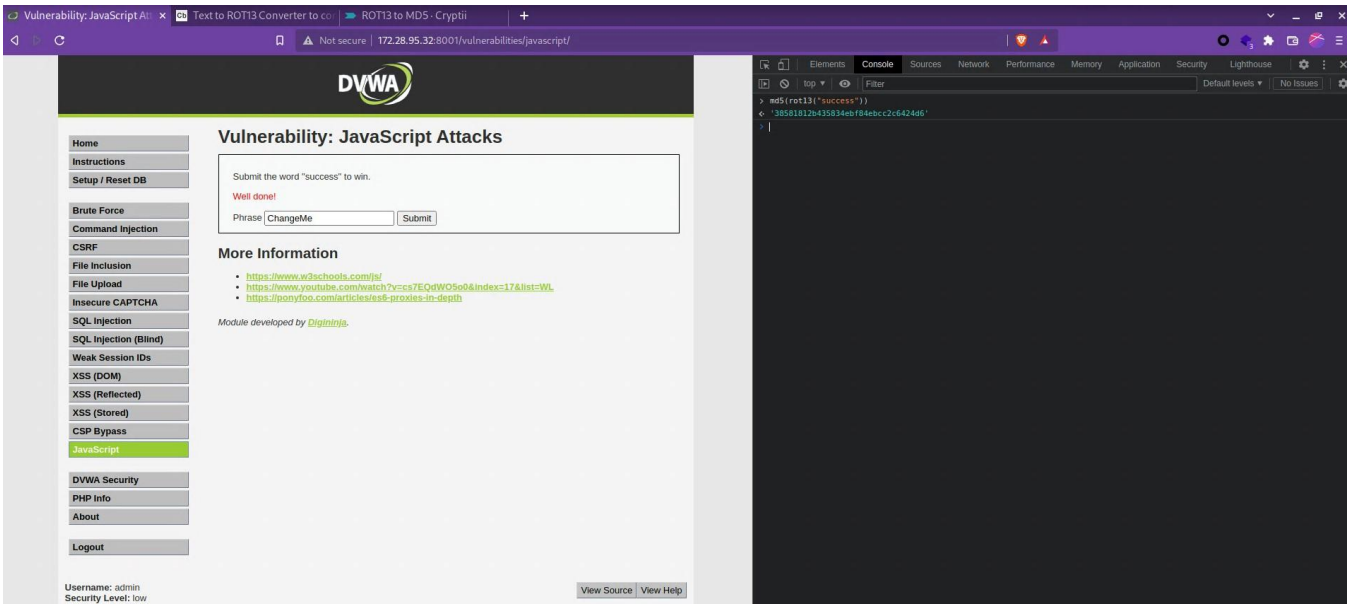
Web Application Test Findings

JavaScript Bypass (Critical)

Description:	DVWA allowed insufficient control of JavaScript access to client-side assets (data and code) This configuration allowed the tester to bypass the inner firewall and gain access to the internal system.
Impact:	Critical
System:	local IP address
References:	OWASP Top 10: A01-2021 - Broken Access Control,

Exploitation Screenshots

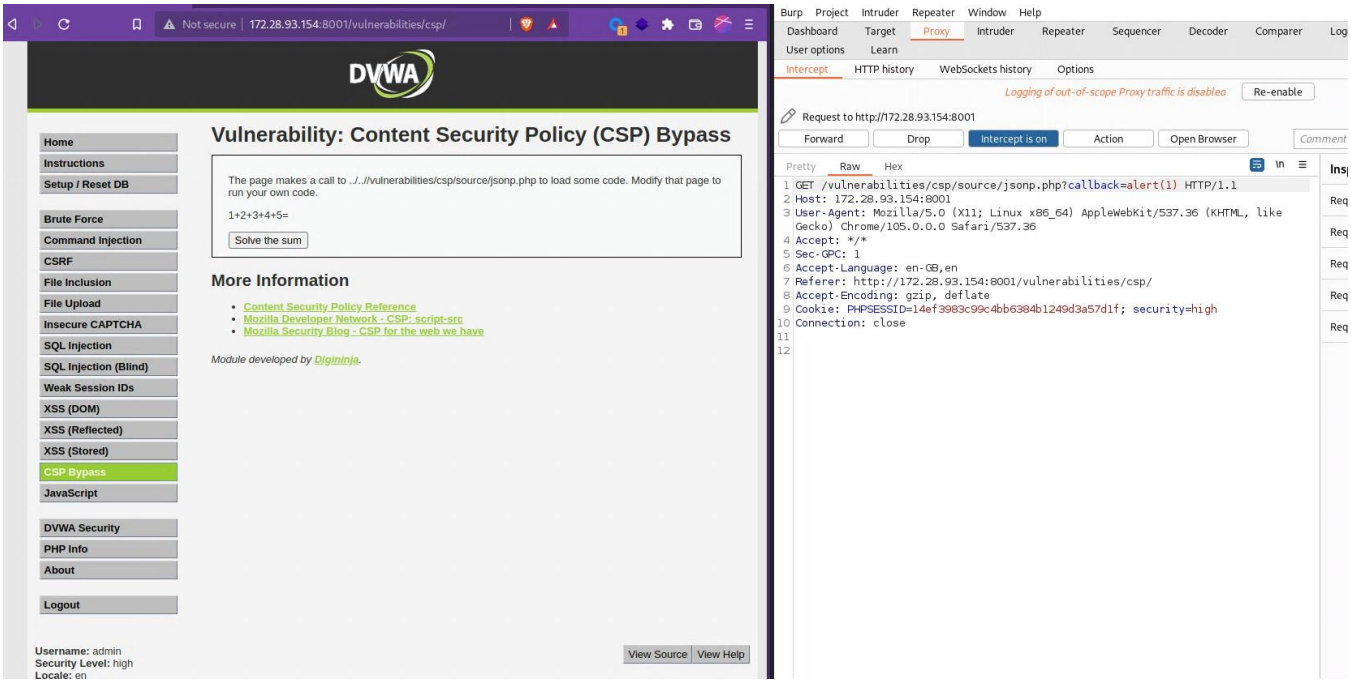


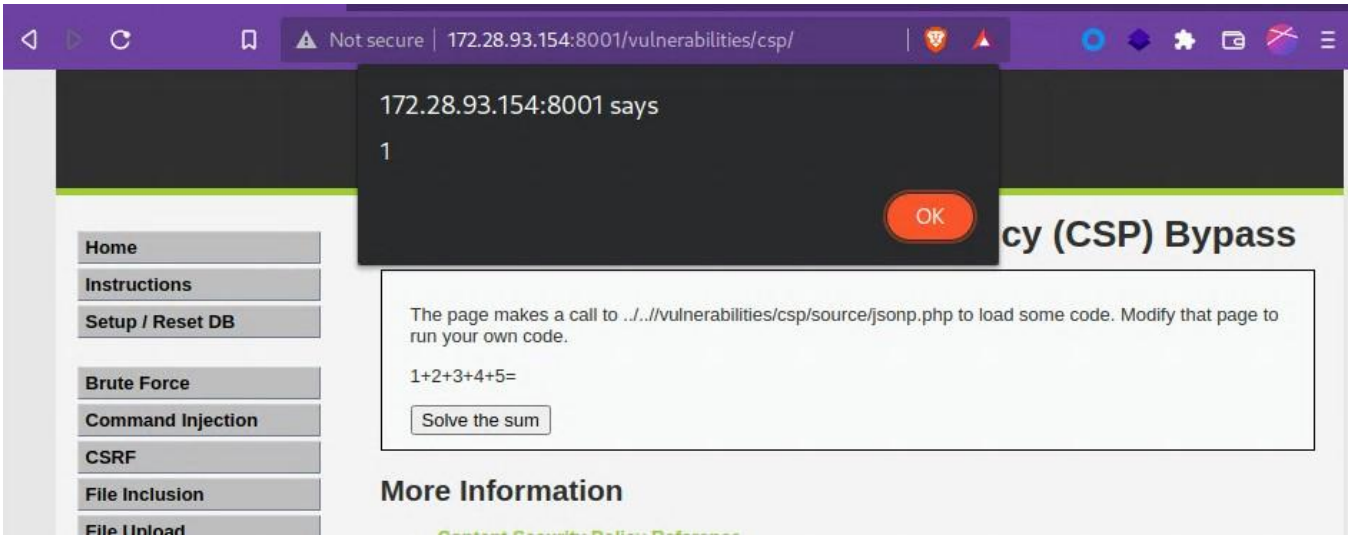


CSP Bypass (Critical)

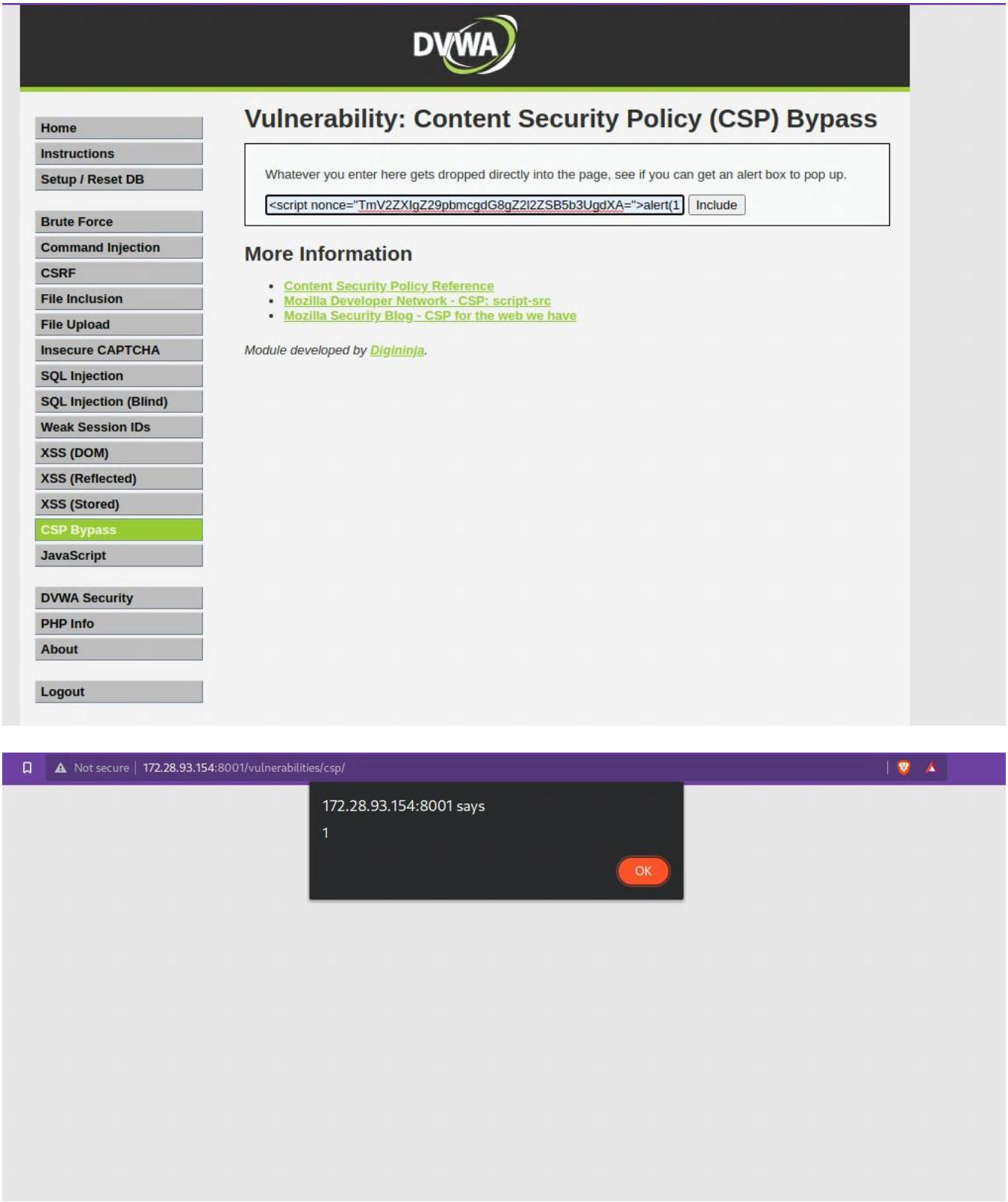
Description:	DVWA was not using common standards-based security controls built into browsers such as CSP headers and source.This configuration allowed the tester to bypass the inner firewall and gain access to the internal system.
Impact:	Critical
System:	local IP address
References:	A06:2021-Vulnerable and Outdated Components A05:2021-Security Misconfiguration

Exploitation Screenshots





Inline CSP Bypass

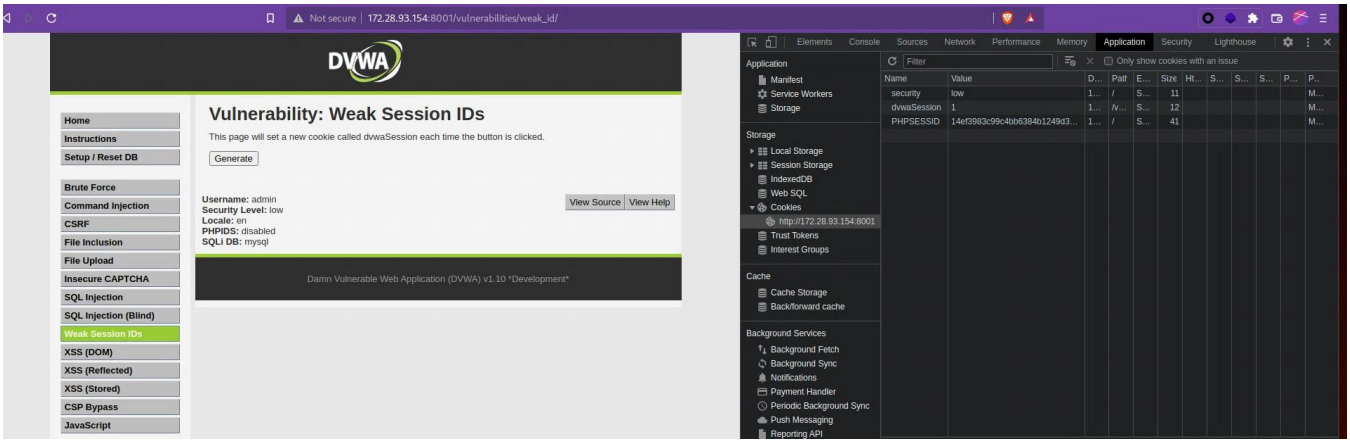


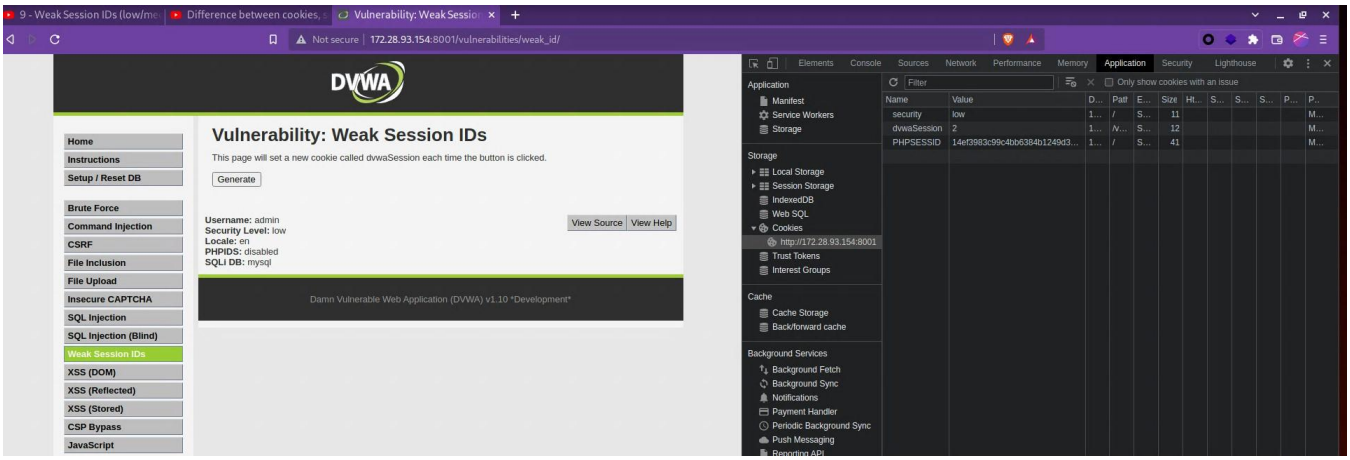
CSP bypass with nonce set.

Weak session ID (Critical)

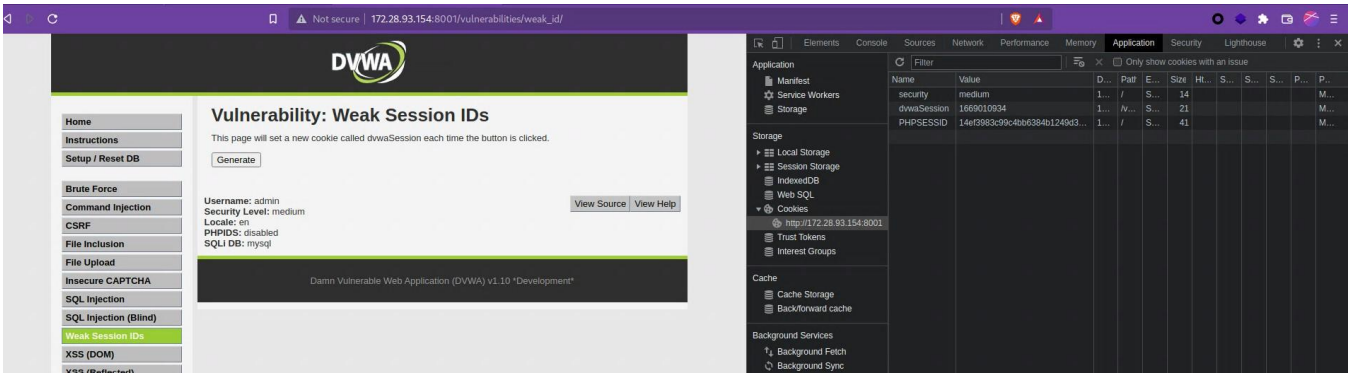
Description:	DVWA allows easily guessable session IDs that can be used to cause session fixations and cause access into other user pages if used maliciously.
Impact:	Critical
System:	local IP address
References:	A02:2021-Cryptographic Failures, A03:2021-Injection

Exploitation Screenshots





Normal Increment



Increment Based on Current Time

Additional Reports and Scans (Informational)

The tester has provided all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet.

DVWA-Test

Last Page