# *IT Security (420-F30-HR)*

# *Lab 05 –Passwords*

Date assigned: Tuesday, Feb 18

Date Due: Tuesday, Feb 18, 16h00

**Objectives:**

Learn:

1. Understand how brute force dictionary password cracking works.
2. Hands-on with BurpSuite on Kali Linux
3. Password best practices

**References:** S0501\_Encryption, S0502\_Password

# NIST CSF

Following the NIST CSF 5 function framework. Similar to the class exercise, identify an asset, vulnerability and risks (that requires mitigation and protection) and walk through the NIST CSF describing what you’d do at each function. Must be reasonable and business relevant (no ninjas!)

## Asset: Jordan 1s

## Identify

They are expensive shoes.

They are very light.

The fabric on them can be stained or ripped.

1. Protect

To protect the shoes, we can wrap them in vacuum sealed plastic.

We can also put them in a very heavy safe, that only I know the code to.

1. Detect

We can set up cameras around the safe to monitor it. Modern security cameras have motion sensors that can deliver notifications to your phone.

1. Respond

Through the camera, it is possible to speak to an intruder and warn them. If they choose to ignore, we can blow up the building.

1. Recover

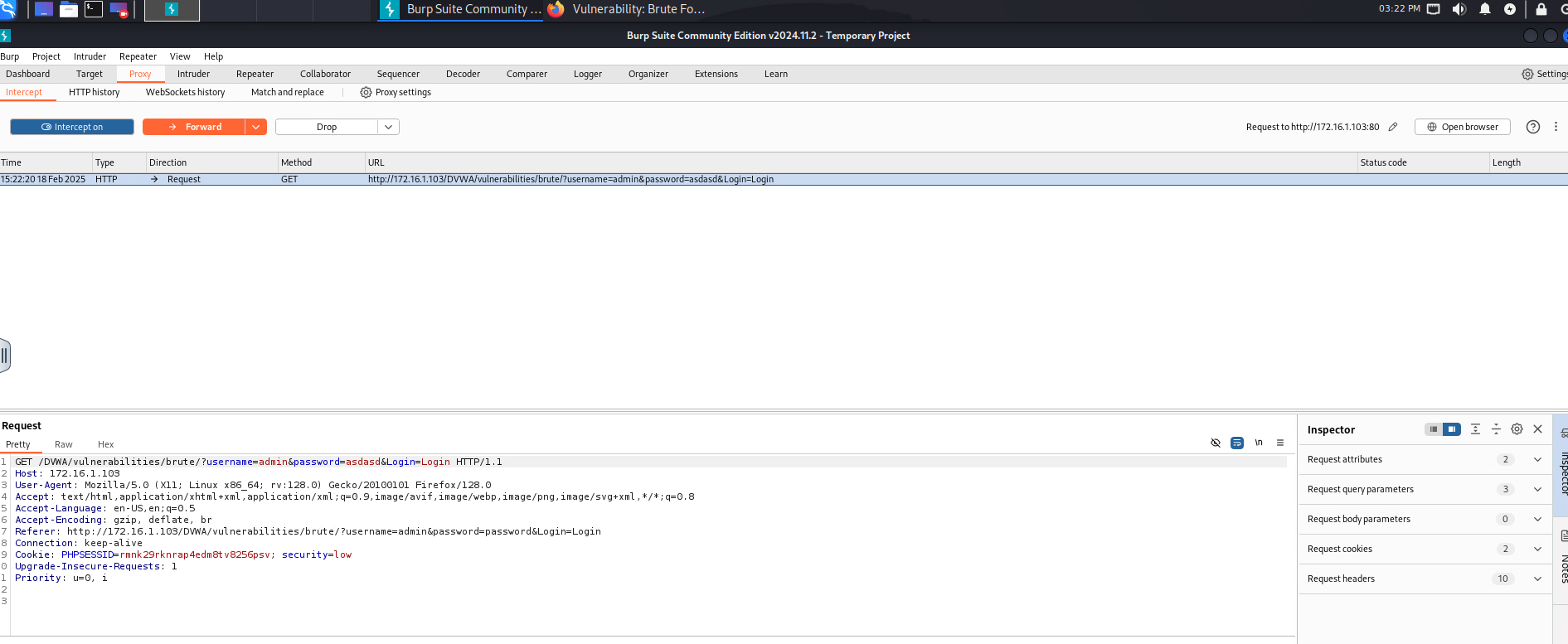
Since the shoes were in a safe, we can safely recover the safe from the rubble, and find the shoes in still mint condition.

# Bruteforce dictionary password crack

Based on <https://himalfrom2061.medium.com/brute-force-in-dvwa-low-security-9e171b89d91e>

## Boot up KaliBox and LinuxBox1.

1. Ensure DVWA is running. Set security to low.
2. Start BurpSuite (temporary project, default everything)
3. Set the proxy on KaliLinux Firefox to 127.0.0.1:8080 (preferences/general/network settings)
4. It should be in intercept mode where it’ll show all the packets. Click on “forward” to pass packets from the BurpSuite Proxy to the endpoints.
5. Show me a screenshot of the intercept working on BurpSuite



1. Explain in your own words, what does BurpSuite allow you to do in intercept mode.

It allows you to capture and modify HTTP(S) requests and responses between the client and the server before they are sent or received.

1. Go to the intruder tab, follow the [tutorial instructions](https://himalfrom2061.medium.com/brute-force-in-dvwa-low-security-9e171b89d91e).
2. Normally we’d use a table of 1000’s common usernames and passwords.

Select these common usernames: (source <https://nordpass.com/blog/all-time-most-popular-usernames/> )

|  |
| --- |
| **Username** |
| David |
| Alex |
| Maria |
| Anna |
| user |
| admin |
| root |
| daemon |

Select the top 10 passwords from <https://md5hashonline.com/most-common-passwords/>

1. Run your attack, what is the username and password?

admin and password

1. Show me a screenshot on DVWA of getting the right username/password.



1. Explain in your own words, what does the intruder feature of BurpSuite allow you to do?

You can run brute force attacks, test for injection attacks, and automated attacks.

1. Explain in your own words, what is the value add of BurpSuite Enterprise (over the community version that we’re using)? How would you use this in a project on a frequent basis?

A feature I noticed was the importing feature which would probably allow you to use large lists to speed up the process of manually adding usernames or passwords. I am sure Enterprise gives access to more automation features.

1. How can you mitigate against a brute force password attack?

You can use phrases or never use the same password twice, you can also add mutations. MFA, captcha, failed attempts.

When you are done, don’t forget to remove the proxy from firefox and shutdown BurpSuite.

# Password best practices

## Explain, what is a “hash function”?

## <answer>

## What is it called if two different inputs generate the same hash value output?

How does this affect hashed passwords

## Hash collision.

## What’s the advantage of using a passphrase over using a password?

## Easy to remember, much longer than a typical password.

## Fill in the table below

|  |  |
| --- | --- |
| **MFA – Factor type** | **Example** |
| What you are | Face |
| What you have | USB key |
| What you know | Password |

## What would take longer to brute force (worst case)?

12 character [a-z,A-Z] or 11 character [0-9,a-z,A-Z,!@#$%^&\*<>,.+\_-=()]

## <answer>

**Marking Scheme**

|  |  |  |
| --- | --- | --- |
|  | **Mark** | **Out of** |
|  |  |  |
| **Part A: NIST CSF** |  |  |
| Identify |  | 2 |
| Protect |  | 2 |
| Detect |  | 2 |
| Respond |  | 2 |
| Recover |  | 2 |
|  |  |  |
| **Part B: BruteForce crack** |  |  |
| Firefox with proxy configured |  | 4 |
| BurpSuite as proxy/intercept & forward |  | 8 |
| Execute Attack and Crack |  | 8 |
| Intruder feature explanation |  | 4 |
| Enterprise value add |  | 4 |
| Mitigations |  | 4 |
|  |  |  |
| **Part C: Best Practices** |  |  |
| Hash function |  | 2 |
| Hash match |  | 2 |
| passphrase |  | 2 |
| MFA |  | 6 |
| Brute force calculation |  | 2 |
|  |  |  |
| **Part D: best practices (MS)** |  |  |
| Minimum Password length |  | 4 |
| 2 weakness with longer |  | 4 |
| Multiple character sets |  | 2 |
| Recommendations for multiple character sets |  | 2 |
| 1 weakness with multiple char sets |  | 2 |
| Case: > 16,000 hashed passwords, how long? |  | 2 |
| qeadzcwrsfxv1331 |  | 1 |
| Case: > 16,000 , source knowledge |  | 2 |
| Password expiry. Weaknesses |  | 2 |
| Password expiry. Case study. Weaknesses |  | 2 |
| Vs passphrase |  | 2 |
|  |  |  |
| **Part E: Password manager** |  |  |
| definition |  | 4 |
| Vs spreadsheet |  | 2 |
| Paid vs free |  | 3 |
| Autofill |  | 2 |
| Table (product 1) |  | 3 |
| Table (product 2) |  | 3 |
| Table (product 3) |  | 3 |
| Personal choice and rationale |  | 2 |
| Business choice and rationale |  | 2 |
|  |  |  |
| Crossword |  | 10 |
|  |  |  |
| Handed in properly |  | 4 |