**Task 6 : Create a Strong Password and Evaluate Its Strength.**

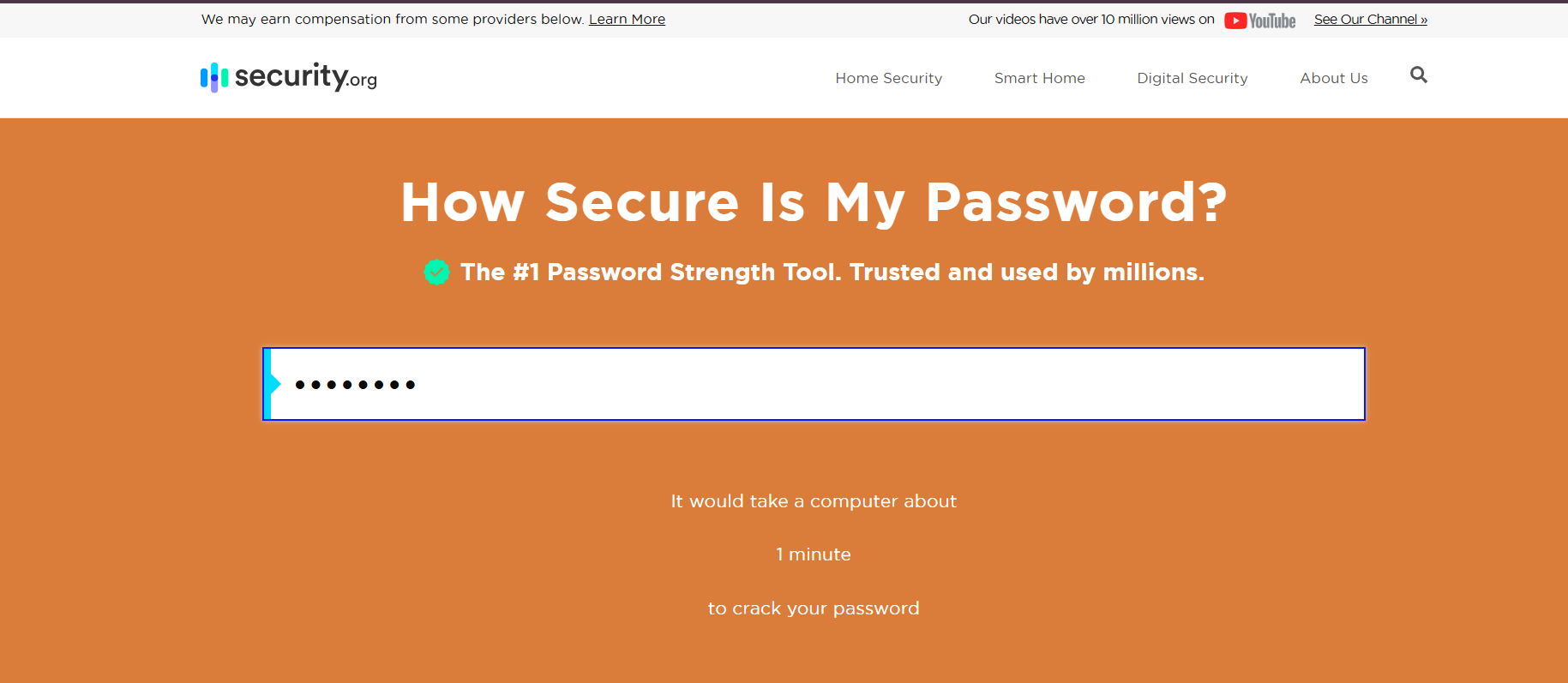
**Objective**: Understand what makes a password strong and test it against password strength tools. **Tools**: Online free password strength checkers (e.g., passwordmeter.com).

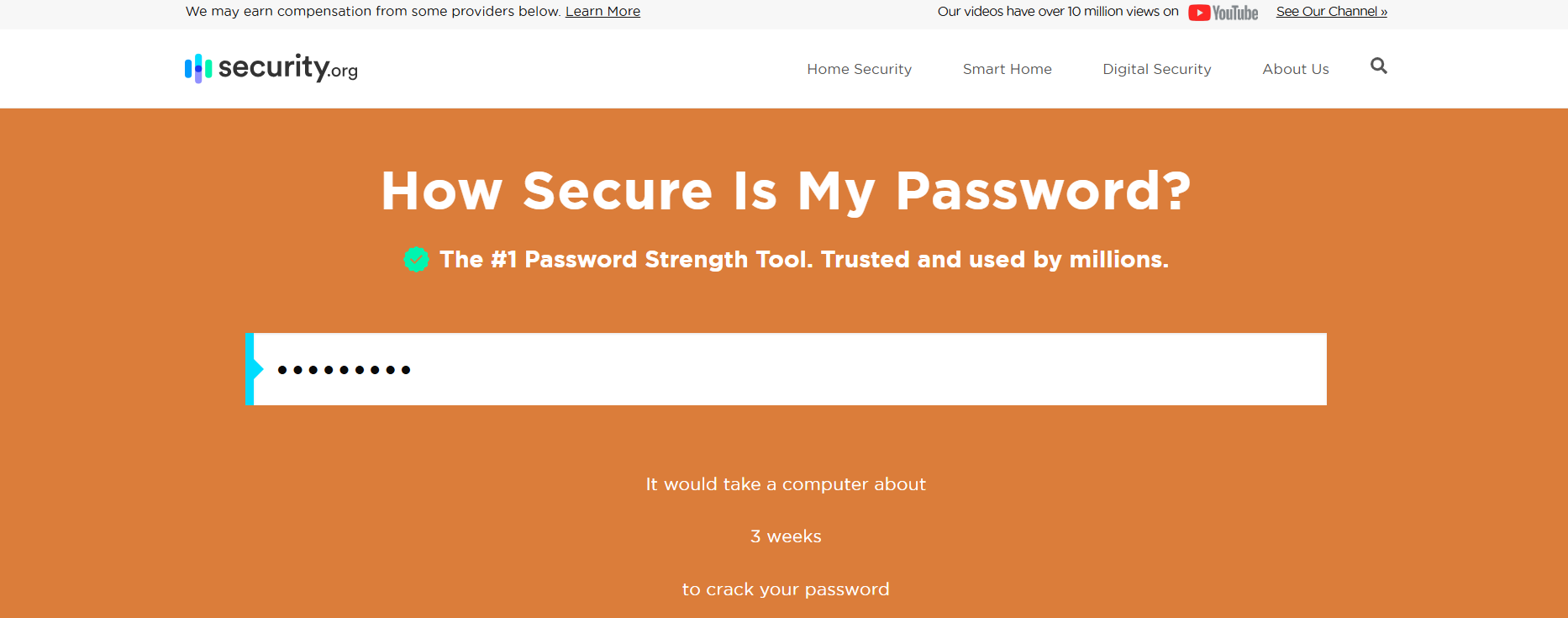
**Deliverables**: Report showing password strength results and explanation.

**Step-1:Password Creation**

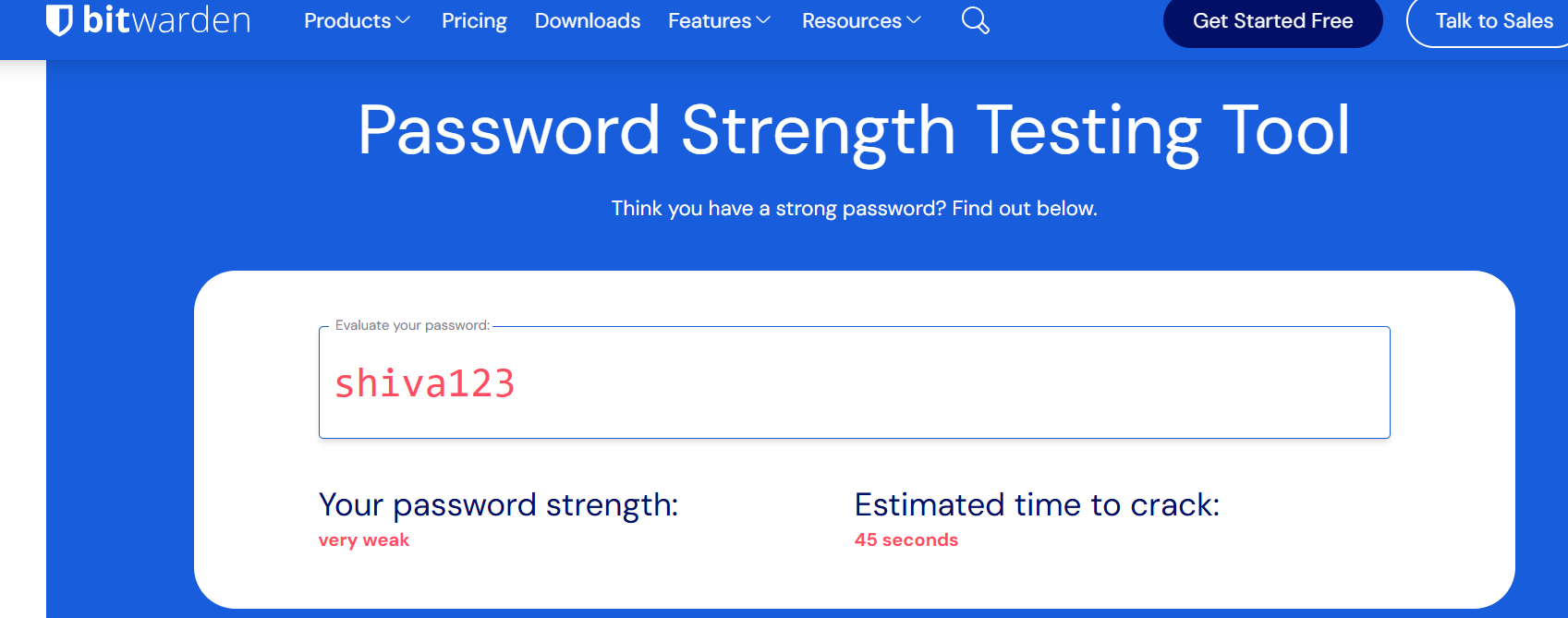
I created the following passwords with increasing levels of complexity:

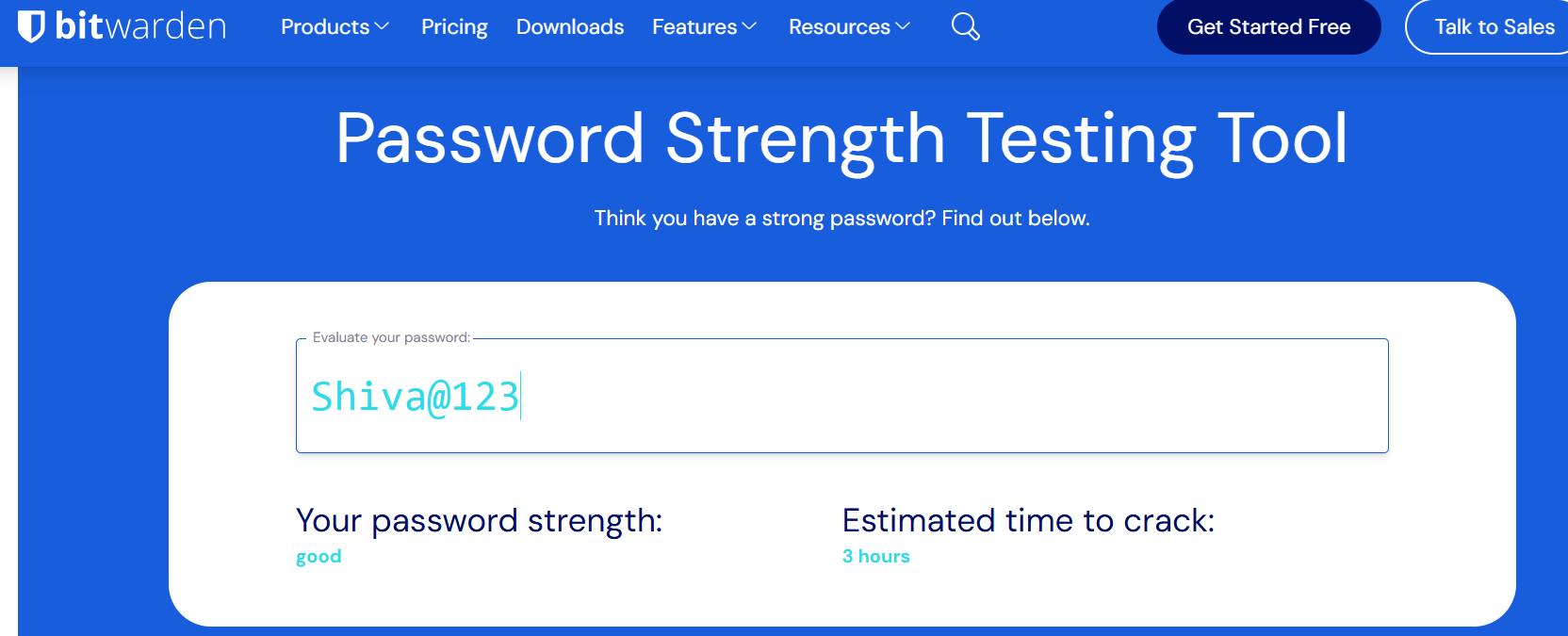
| **Password** | **Complexity Used** |
| --- | --- |
| shiva123 | Lowercase + Numbers |
| Shiva@123 | Uppercase + Lowercase + Symbols |
| Sh!v@\_20#25 | Strong (Mixed characters, long) |
| Step-2:Password Strength Evaluation I tested the above passwords on Security.org Password Strength Test AND Bitwarden |  |

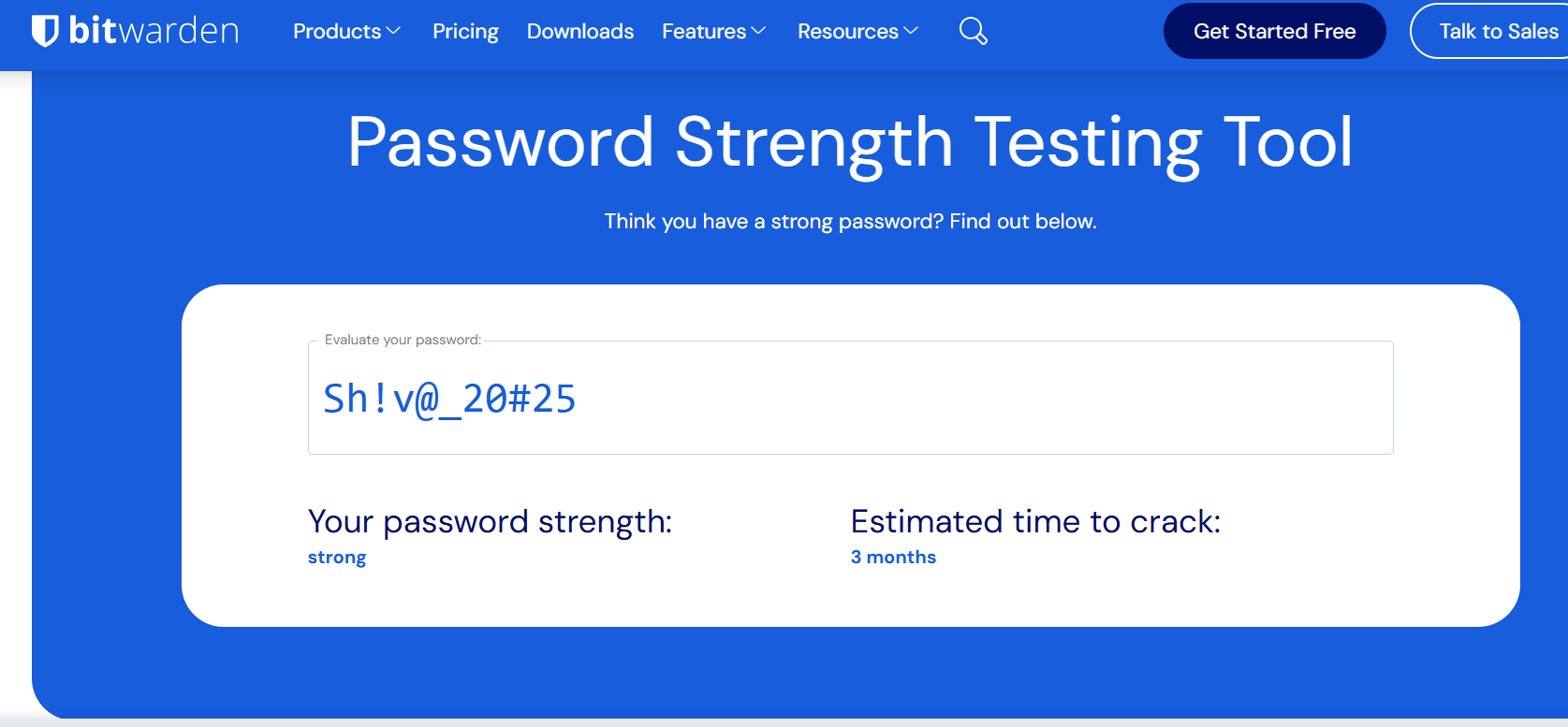












## Step-3:Tips Learned for Creating Strong Passwords

✅ Use a mix of uppercase, lowercase, numbers, and symbols  
✅ Make it at least **12 characters** long  
✅ Avoid dictionary words and predictable patterns  
✅ Use **passphrases** that are random but memorable  
✅ Change passwords regularly  
✅ Don’t reuse the same password across multiple sites

## Step-4:Common Password Attacks

* **Brute Force Attack**: Tries all possible combinations
* **Dictionary Attack**: Uses common words from dictionaries
* **Credential Stuffing**: Tries previously leaked credentials

## Step-5️ Summary: Why Password Complexity Matters

The more complex and longer the password, the harder it is to guess or crack. Simple passwords like "shiva123" can be cracked in seconds, while complex ones like Sh!v@\_20#25\_SeCuRe are nearly impossible with current technology.

### **Brute Force Attack**

A brute force attack is a hacking method where attackers try **all possible combinations** of characters to guess a password. The shorter and simpler the password, the faster it can be cracked.

### **Dictionary Attack**

In a dictionary attack, attackers use a **list of common words and phrases** (like a dictionary) to guess passwords. It's faster than brute force and effective against weak or common passwords like "admin" or "qwerty".

### **Authentication**

Authentication is the process of verifying a user's identity. The most common method is **username + password**, but stronger methods include **multi-factor authentication (MFA)** using OTPs, biometrics, or security keys.

### **Best Practices for Password Security**

* Use **12+ characters**
* Include **uppercase, lowercase, numbers, and symbols**
* Avoid common words, names, and personal info
* Never reuse passwords across sites
* Use a **password manager** to generate and store strong passwords
* Enable **MFA** wherever possible