Penetration Testing vs. Brute Force Attack

reflex

Introduction

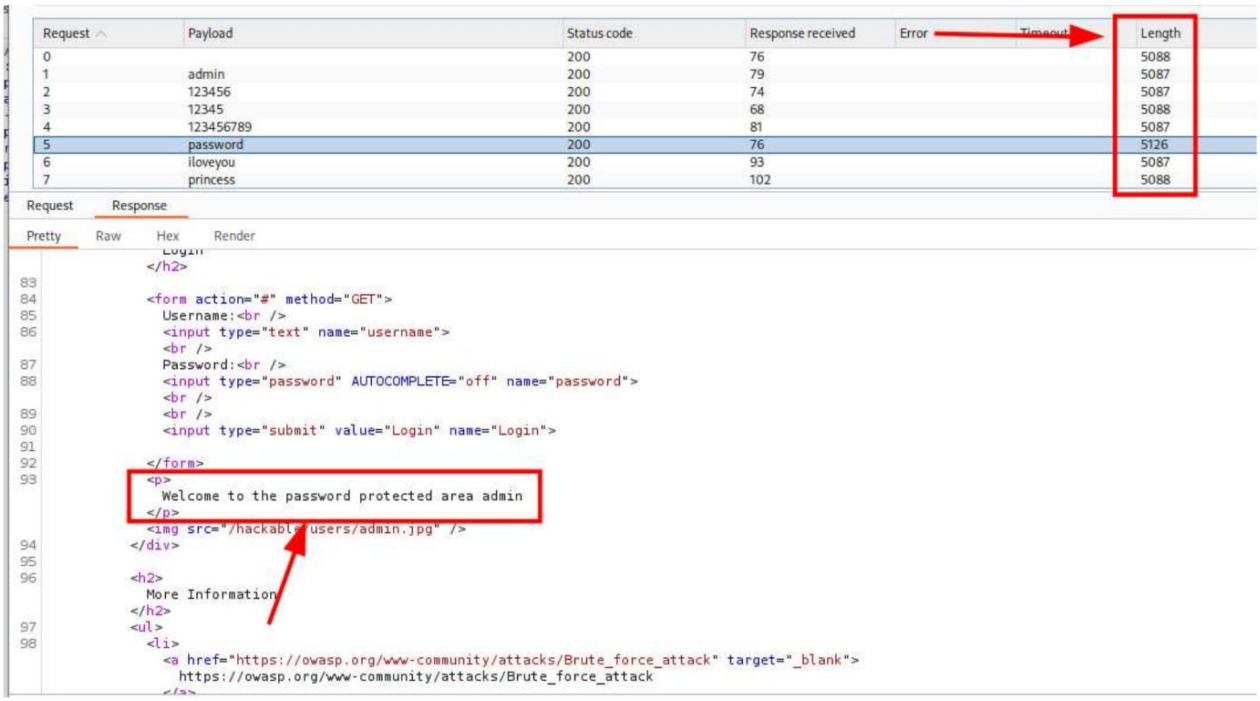
You are part of an authorised penetration testing team assessing a web application. During testing, you identified that the login functionality allows repeated authentication attempts without effective protection. This could enable a brute force attack and lead to account takeover.

Evidence from the penetration test

Below is the login page of the website where the penetration testers attempted to sign in.

The penetration testers then intercepted the login request using an automated testing tool (Burp Suite) to assess whether the application could be brute forced.

The team then tested multiple password attempts against the username “admin” using a password list. As shown below, the responses differed in length. The team identified the successful attempt by looking for the response that contained additional content indicating a successful sign-in. In this example, the response included the message: “Welcome to the password protected area, admin.”



Key Tasks

Record a ~3-minute video as penetration testers. In your video, explain:

1. what a brute force attack is,
2. the risk/impact, and
3. three to four remediation steps that can mitigate the risk.

Use the screenshots provided as evidence of your finding.

Suggested talk track (3 minutes):

1. 0:00–0:20 – Intro / context: Introduce your team, confirm this was an authorised penetration test, and briefly state what you found.
2. 0:20–1:05 – What it is: Explain in your own words what a brute force attack is (no need to demonstrate step-by-step – focus on the concept).
3. 1:05–1:45 – Risk/impact: Describe the business and security risks if an attacker successfully brute forces a login on this application.
4. 1:45–2:50 – Remediation (3–4 steps): Explain three to four remediation steps the business should take to reduce this risk.
5. 2:50–3:00 – Close: Summarise the risk and explain how the recommended controls reduce the likelihood of compromise

Final Requirement

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

Established in 2000 in South Africa, Reflex has evolved from modest origins to become a distinguished provider of Information and Communication Technology (ICT) solutions. Reflex specialises in delivering innovative ICT solutions across various industries, earning a sterling reputation for our excellence in the retail sector and beyond. With a robust network of partnerships, they pride themselves on their ability to swiftly address the technological needs of their clients. Their portfolio of ICT solutions spans various industries. Reflex Carrier understands what it needed to build, manage, and operate complex backbone networks simply. On the other hand, their Enterprise Solutions take complexity out of technology, allowing you to focus on what you can do best. They provide seamless, high-performance solutions for connectivity, communications, workplace management, cloud, and cybersecurity services. Challenge by Karabo Morena.