Homework 3

Computer Security

Sol Andres Martinez

Emilia Saenz

**Deployed application**



**URL**

[**https://dvwa.azurewebsites.net/**](https://dvwa.azurewebsites.net/)

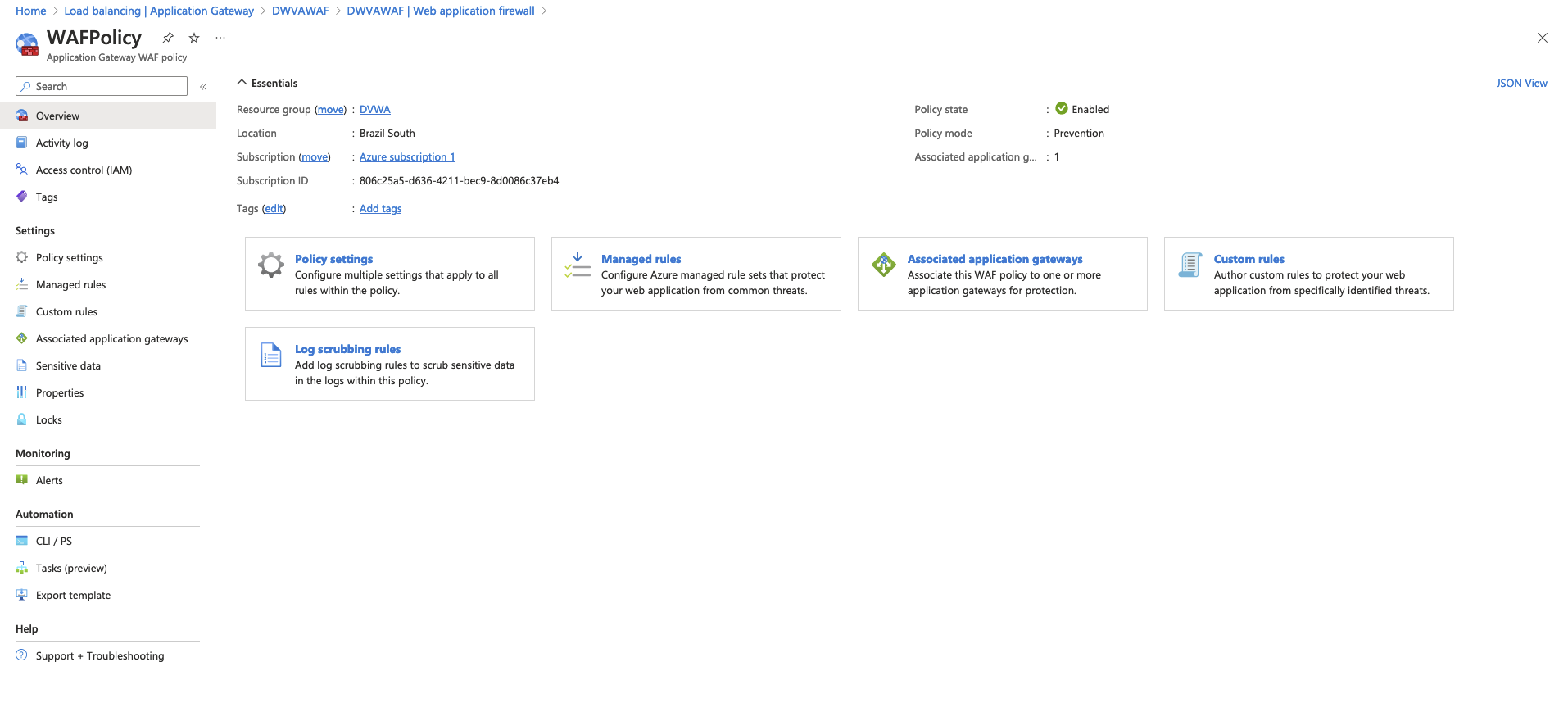
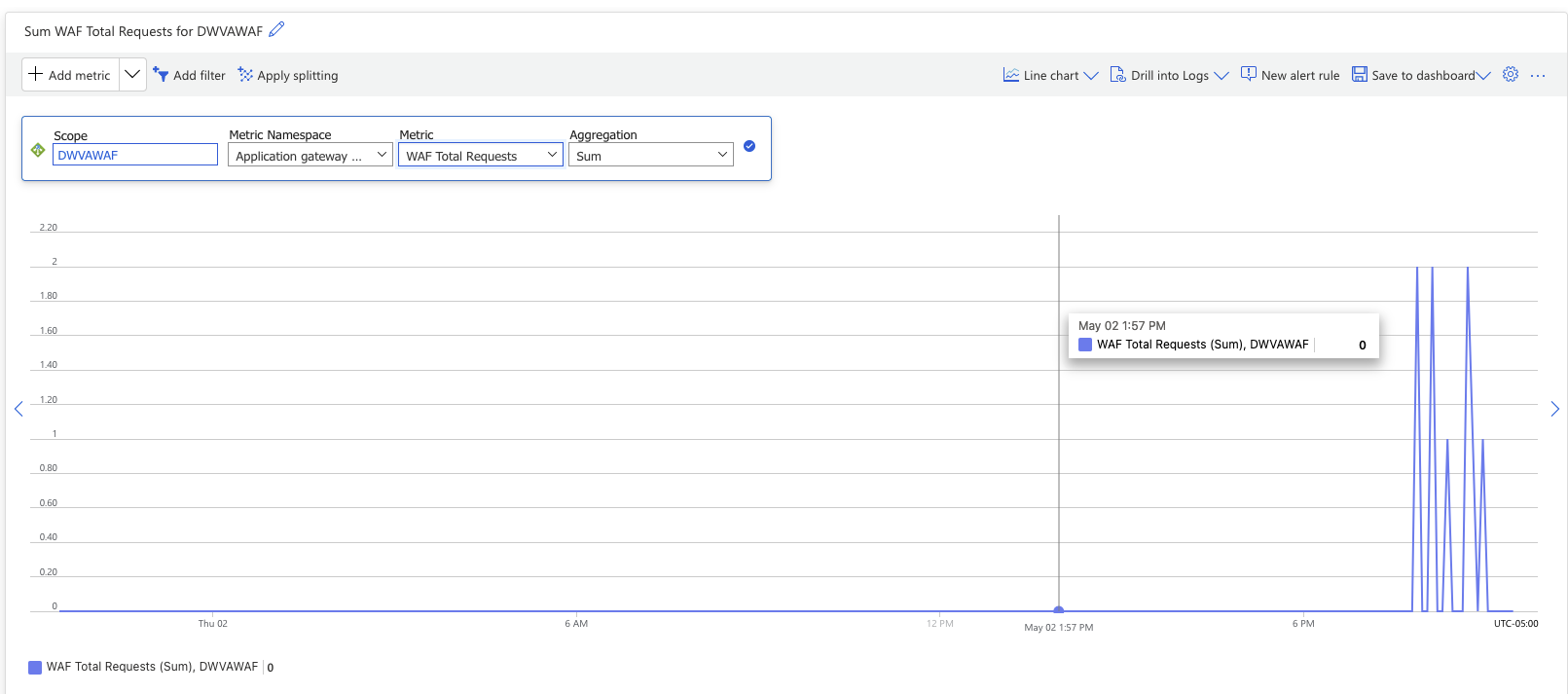
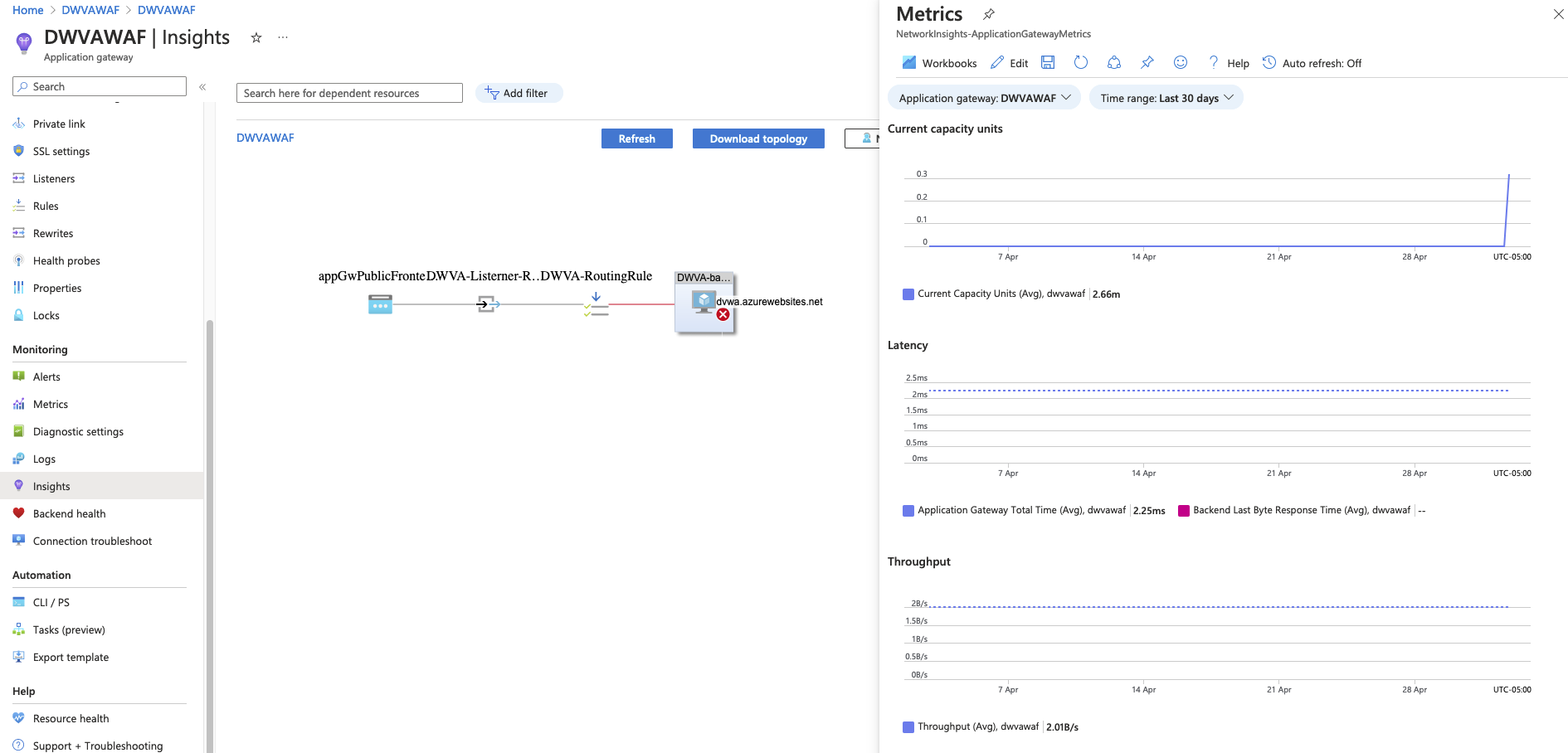
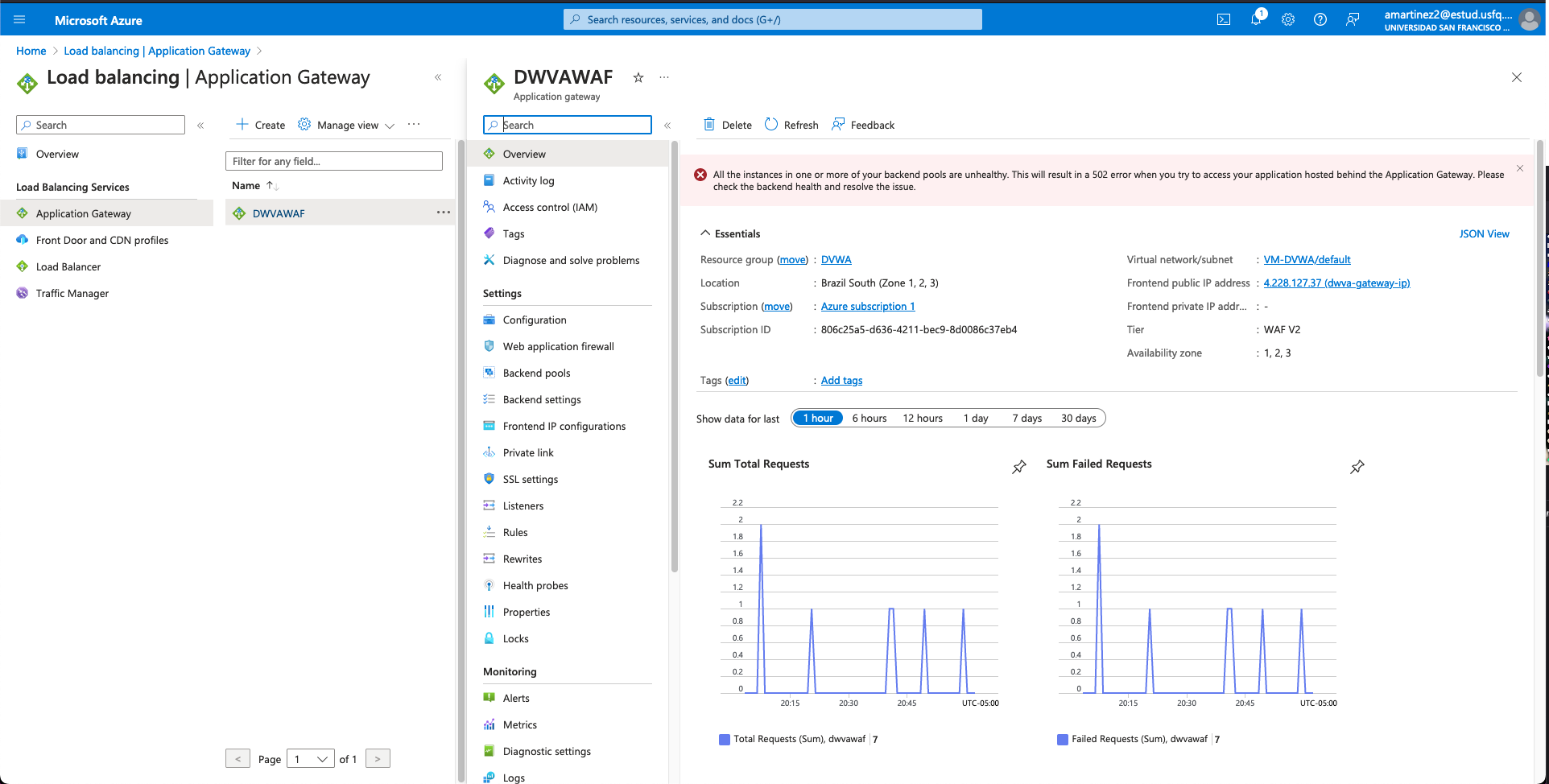
**Azure WAF**

Azure Web Application Firewall is a cloud-based service that safeguards web applications against common hacking methods like SQL injection, vulnerabilities such as cross-site scripting (XSS) and other exploits that are part of the OWASP Top 10 security risks (Azure, s/f).

It operates by filtering and monitoring HTTP traffic before it reaches your application, Azure WAF helps in identifying and blocking malicious requests that could potentially harm the application. Azure WAF also supports custom rules, enabling administrators to tailor the firewall settings to meet specific security needs of their applications. These rules can be configured to block or allow certain traffic patterns, IP addresses, geographic locations, and even specific types of HTTP requests (HackerOne, s/f).

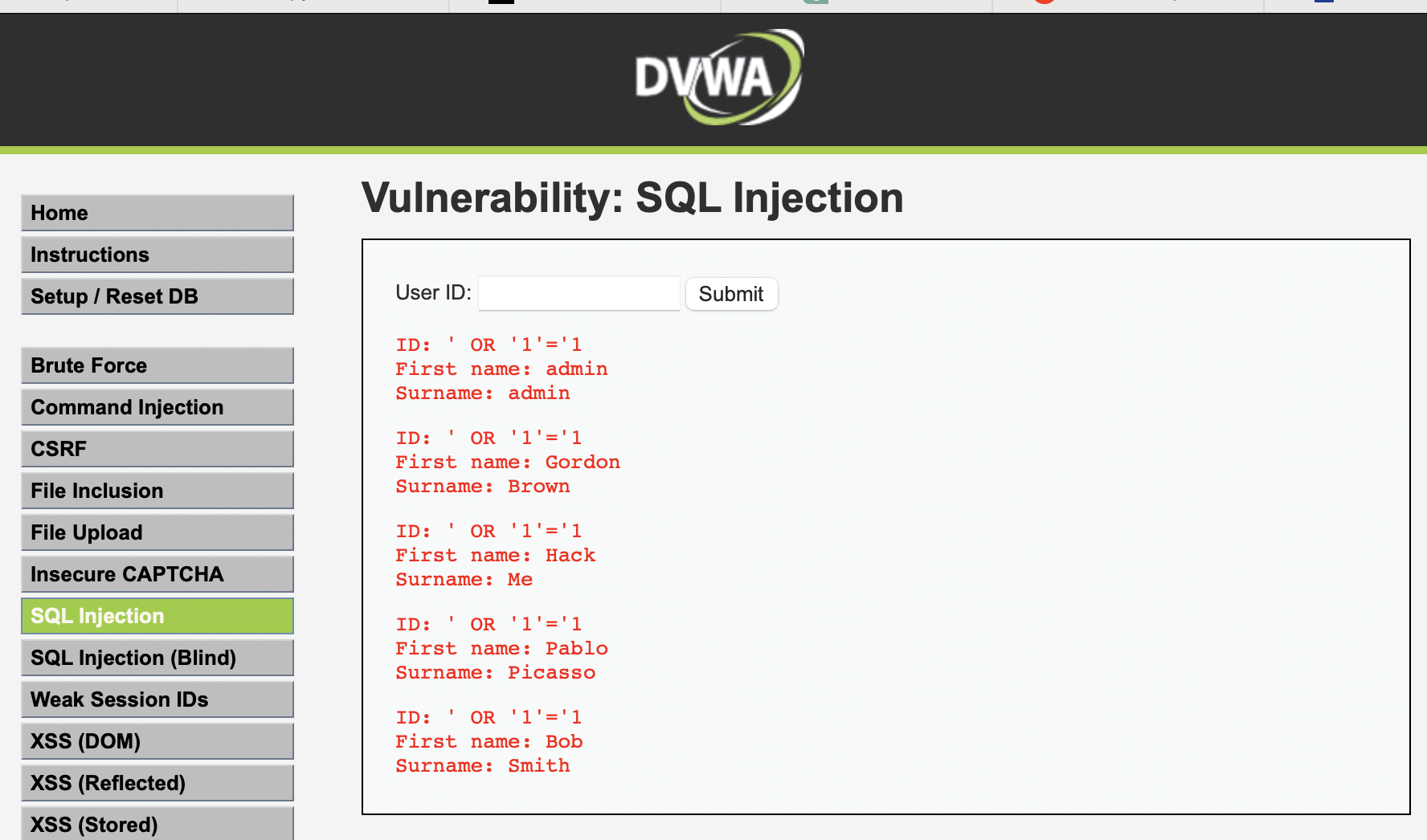
Many security threats exploit the trust applications place in user input; user credentials entered into web forms can be manipulated to perform unauthorized actions. Azure WAF counters these risks by sanitizing user inputs, stripping away harmful elements.

Azure WAF can operate in either detection or prevention modes. Detection mode allows all traffic but logs suspicious activities, useful for monitoring and refining firewall configurations without impacting traffic. Prevention mode, on the other hand, blocks identified threats in addition to logging them, providing robust defense against potential attacks (HackerOne, s/f).

The WAF was applied to the web application via an Application Gateway out of which a WAF Rule policy decides how to interact with the DVWA  


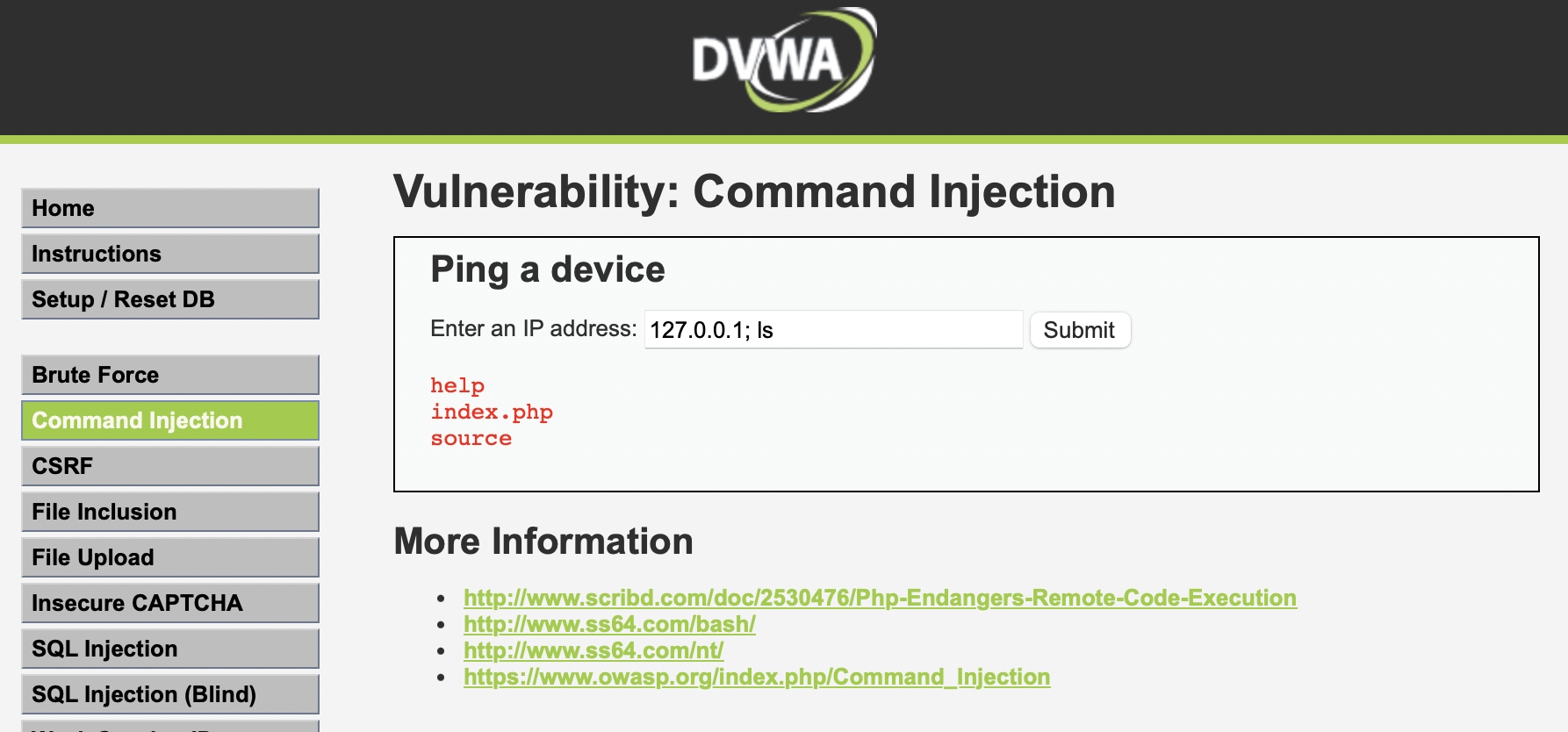
**Attacks without the Firewall**

SQL injection

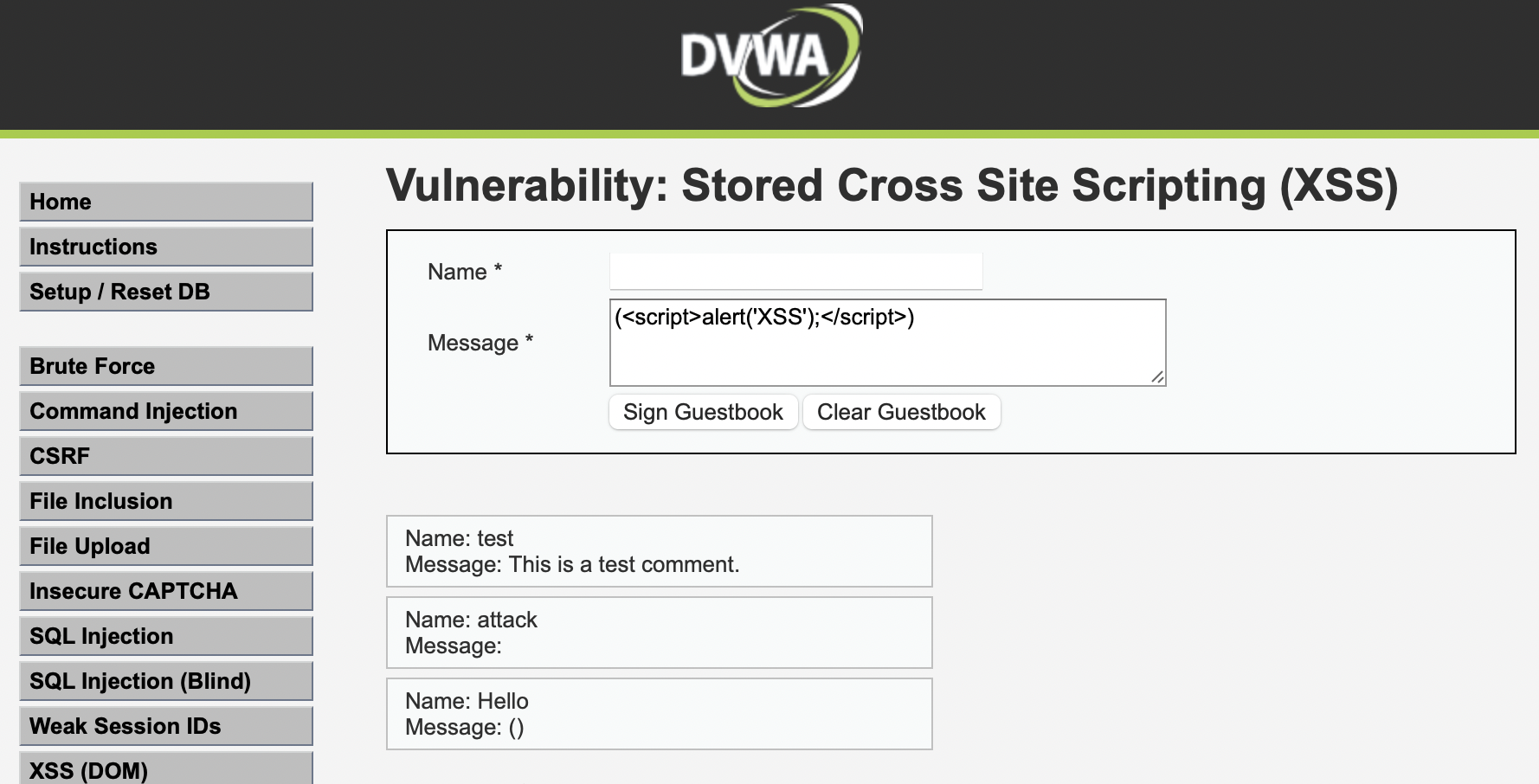
£

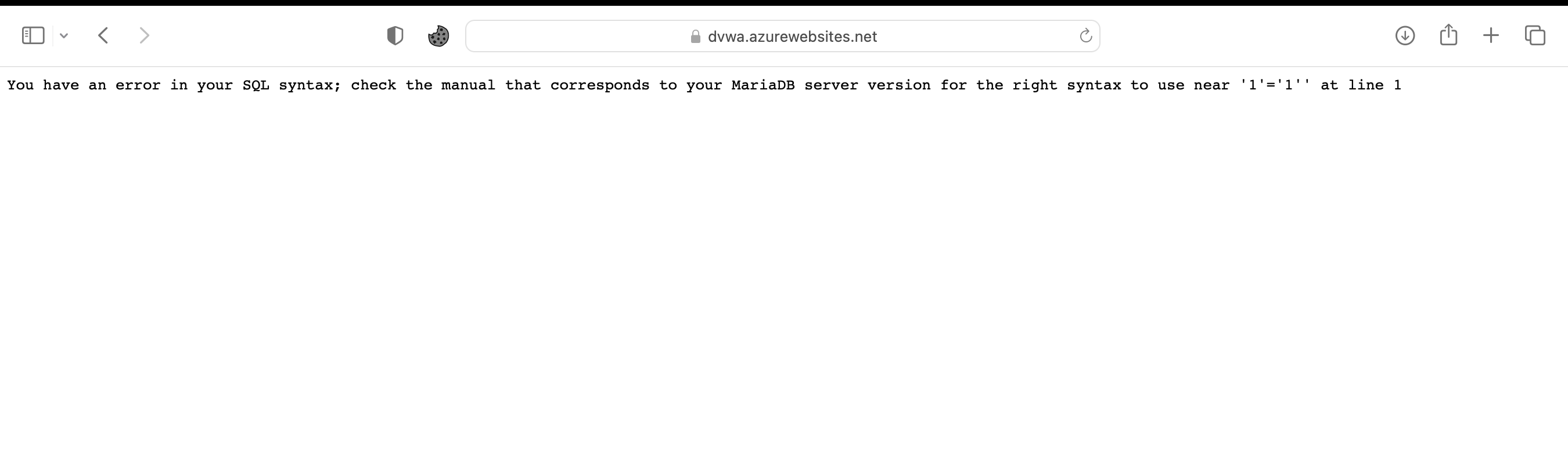
Command injection

127.0.0.1; Is



XSS Stored



**Attacks with the Firewall**

Conclusions:  
Deploying the Damn Vulnerable Web Application (DVWA) on Azure and securing it with Azure's Web Application Firewall (WAF) serves as a practical exercise in understanding cloud deployment and web application security. The process involved setting up DVWA on Azure Web App, which simplifies the hosting and management of web applications. This was followed by configuring and activating the Azure WAF on an Application Gateway to safeguard the application.

Initially, the WAF was set to detection mode to log potential threats, allowing observation of the attack types without interference. Subsequently, it was switched to prevention mode to actively block threats, using predefined security rules aligned with common vulnerabilities and exposures.

The successful deployment and subsequent security enhancement through WAF demonstrated Azure’s capabilities in effectively protecting web applications from known security vulnerabilities. This approach highlights the importance of integrating robust security measures in the deployment phase, ensuring applications are not only functional but also secure from potential threats.

**Bibliography**

Azure. (s/f). Azure Web Application Firewall. Retrieves from <https://azure.microsoft.com/en-us/products/web-application-firewall#:~:text=Azure%20Web%20Application%20Firewall%20is,such%20as%20cross%2Dsite%20scripting>.

HackerOne. (s/f). What is Azure Application Firewall (WAF)?. Retrieved from <https://www.hackerone.com/knowledge-center/what-is-azure-web-application-firewall>