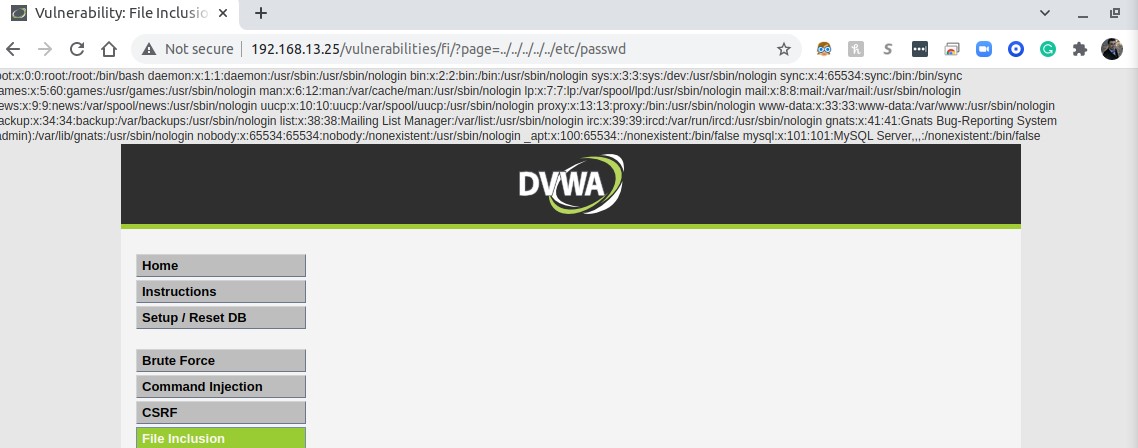
**Web Application 1: *Your Wish is My Command Injection***



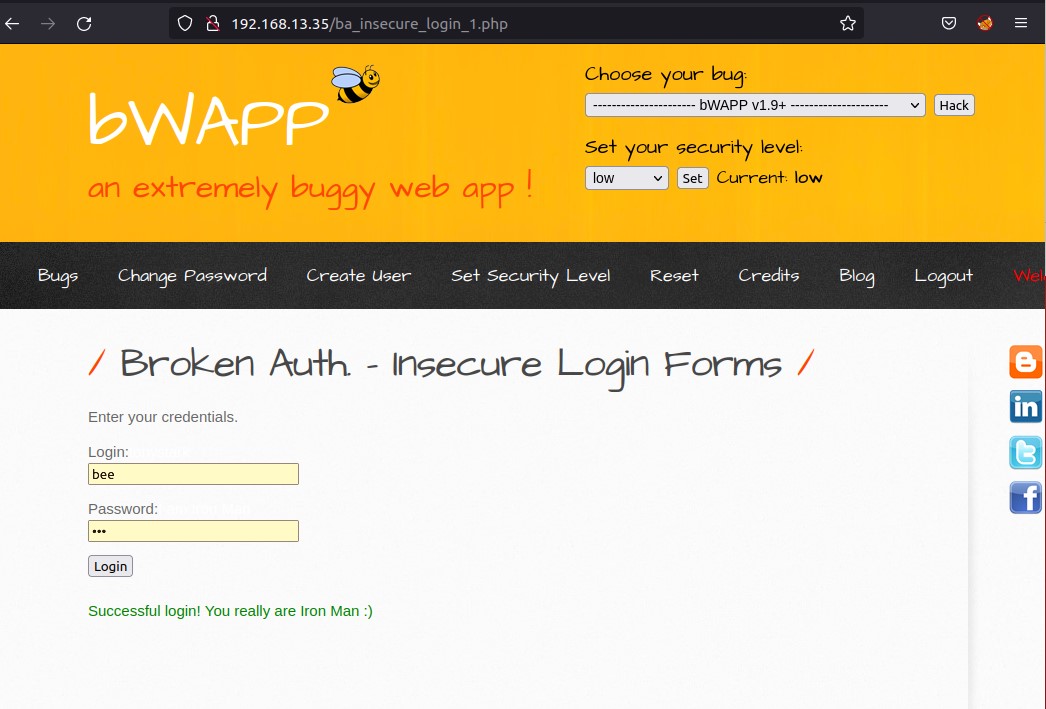


**Command Injection Prevention**

**Avoid system calls and user input**—to prevent threat actors from inserting characters into the OS command. Set up input validation—to prevent attacks like XSS and SQL Injection. Create a white list—of possible inputs, to ensure the system accepts only pre-approved inputs.

**https://www.imperva.com/learn/application-security/command-injection/**

**Web Application 2: *A Brute Force to Be Reckoned With***

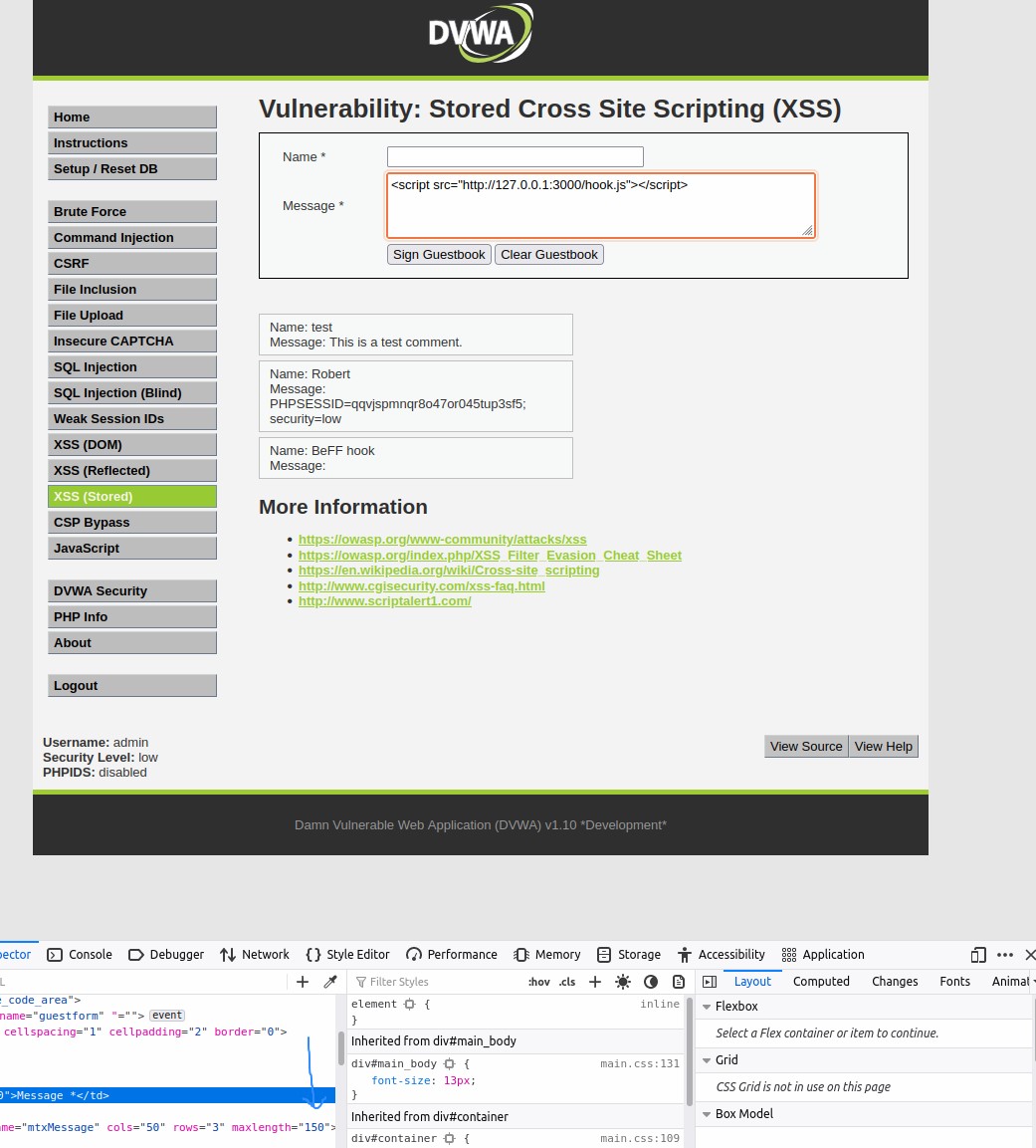


**What is the prevention for brute force attack?**

**Brute force** attacks are entirely preventable. You can keep brute force attacks at bay and drastically improve your data security by having a **strong password policy,** limiting login attemts, enabling two-factor authentication, using CAPTCHA’s, and blocking malicious IP addresses.

[**https://www.itsasap.com/blog/how-to-stop-brute-force-entry**](https://www.itsasap.com/blog/how-to-stop-brute-force-entry)

**Web Application 3: *Where's the BeEF?***



# 

# 

# Mitigation

Man-in-the-browser attacks are client-based and very hard to detect from a network traffic perspective. Moreover, no new processes are created and sometimes the malicious code will live entirely “off the land”.

Some approaches to detection and prevention may be:

* Out-of-Band Notice/Confirmation (Server-Side) – Expanding on out-of-band authentication, the user is sent a summary of the actions performed in a service. In certain cases, the notice may even be used as an integral part of the transaction. For example, when transferring funds online, the client may have to confirm the transaction with an out-of-band OTP included in an e-mail with details about the transaction.
* Malware Detection (Client-Side) – as many MITB malwares contain static code files, they may be signed, blocked and removed by antivirus software. Runtime detection techniques can also be used[9].
* User Training – Endpoint users should be trained to identify suspicious browser extensions, close browser sessions regularly when they’re no longer needed and avoid social engineering attempts.

**https://www.cynet.com/attack-techniques-hands-on/man-in-the-browser-attacks/**