OWASP #1- Broken Access Control

Gavin Lillard (IST-103)

Firstly, let me explain to you what access control is. Access control is the rule set for the application meaning who or what is authorized to perform specific actions or access specific data (PortSwigger, 2023). Using common sense, broken access control would imply that the rule set was breached by someone or something that did not have the authorization to do so. Sadly, access control design has to be created by humans, leaving a high likelihood for there to be human error. Broken access controls are present whenever a user can use a rule set that they are not authorized to. Examples provided by PortSwigger.com, Vertical Privilege Escalation, where a non-admin user can use an admin rule set to delete user accounts. Another example would include Unprotected Functionality; if administrative functions are embedded from an administrator's welcome page, potential attackers could be able to access administrative functions by searching for the relevant admin URL. My source provided an example URL that would be easily accessed by not only admin users but also potential attackers: [<https://insecure-website.com/admin>].

Preventing broken access controls can easily be achieved by discipline with a well, thought-out approach. OWASP (2023) suggests, unless a resource is meant to be public, deny the access by default. Follow that up with using a single application-wide mechanism for upholding access controls. Next, ensure developers declare access for which is allowed in each resource. Finally, back-track, examine, and test the access controls to make sure they work as they are intended to.

Works Cited

PortSwigger. “Access Control Vulnerabilities and Privilege Escalation | Web Security

Academy.” *Portswigger.net*, 2023, portswigger.net/web-security/access-control.