HE Übungen 5

Diese Übung ist Teil der Vorlesung Hacking Exposed an der Juventus Technikerschule HF in Zürich.

1 Warm-Up

Aussage	Wahr	Falsch
Phishing ist als Angriffsvektor in den OWASP Top 10 aufgelistet.		
Die Burp Suite ist ein Reverse Web Proxy.		
HTTP ist statuslos (stateless), weshalb Sessions mit Cookies realisiert werden.		
CSP Regeln werden vom Server an den Client geschickt und vom Browser ausgewertet.		
SOP wird serverseitig erzwungen, der Client kann dieses Sicherheitskonzept aber umgehen.		
CORS ist ein Ansatz die Einschränkungen von SOP aufzulockern.		
SOP nützt nicht gegen XSS-Attacken.		
XSS ist eine serverseitige Schwachstelle.		
Bei einem Reflected XSS ist ein Attack-Server zwingend notwendig.		
Bei einer Stored XSS wird zwingend ein DOM vorausgesetzt.		

2 XSS

1. Wie gross sind die Auswirkungen einer XSS-Attacke auf untenstehende Kategorien von Webservices?

Kategorie	minimal	ernsthaft	kritisch
Single Page Application (SPA) einer Firma			
Email Web Interface			
Admin Web Interface einer Datenbank			

2. Begründen Sie obige Auswahl.

3. Was sind wirksame Massnahmen eine XSS-Attacke zu verhindern? Nennen Sie mindestens drei:
