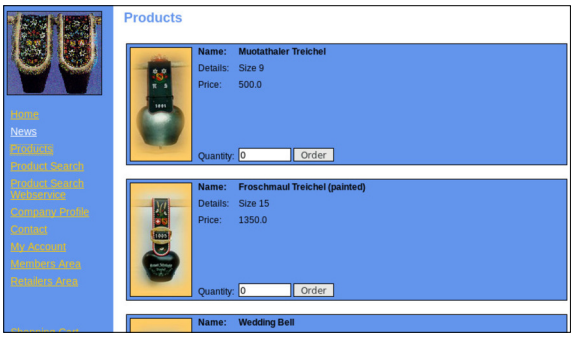
Sven Defatsch

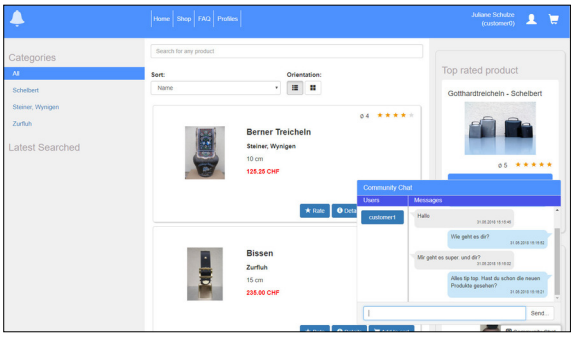
Patrick Steinhäusl

| | |
|---|---|
| Diplomanden | Sven Defatsch, Patrick Steinhäusl |
| Examinator | Cyrill Brunschwiler |
| Experte | Dr. Christian Folini, netnea AG, Liebefeld, BE |
| Themengebiet | Sicherheit |

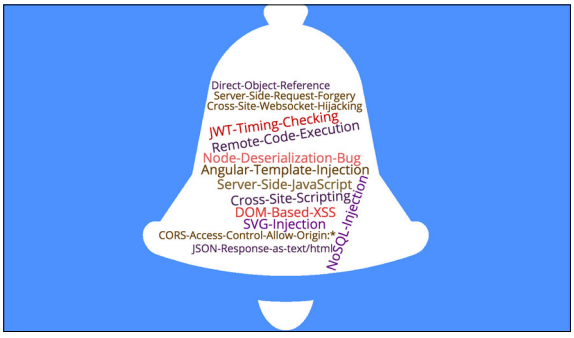
# Emil on Steroids




Bestehender Webshop




Neuer Webshop mit 14 Verwundbarkeiten




Alle implementierten Verwundbarkeiten

Einleitung: Die HSR nutzt das Hacking-Lab, eine Plattform mit diversen Security Challenges, für die praxisbezogene Ausbildung im Themengebiet der Informationssicherheit (Modul InfSi3, Challenge Projekt und CAS Frontend Engineering). Eine für mehrere Challenges genutzte Applikation ist der sogenannte "Glockenshop". Dieser fiktive Webshop beinhaltet verschiedenste Sicherheitslücken, welche in diversen Aufgaben gefunden und ausgenutzt werden müssen. Zudem sind die Studenten angehalten, Empfehlungen für die Vermeidung der Fehler abzugeben.

Vorgehen / Technologien: Der in die Jahre gekommene Webshop wurde im Rahmen einer Studienarbeit neu aufgebaut. Der eingesetzte Technologie Stack basiert auf MongoDB, Express, AngularJS und Node.js, auch "MEAN" Stack genannt. Mit der aktuellen Arbeit wurde dieses Grundgerüst überarbeitet, Fehler behoben und die Anwenderfreundlichkeit verbessert. Des Weiteren wurden sehr viele Sicherheitslücken in die Applikation eingebaut. Die gewählten Schwachstellen gehören zu den aktuellsten und häufigsten (OWASP Top 10) um möglichst realistische Szenarien darzustellen. Nebst den bekannten Angriffsvektoren "Cross-Site Scripting (XSS)", "NoSQL Injection" oder "Remote Code Execution (RCE)" sind auch weniger geläufige wie "Cross-Site WebSocket Hijacking (CSWSH)" und De-Serialisierungs-Probleme implementiert worden.

Ergebnis: Als Voraussetzung galt die Auslieferung der Anwendung als fertiges Docker Image. Dies garantiert die Lauffähigkeit auf Fremdsystemen und die Reibungslose Integration in die bestehende Umgebung des Hacking-Lab. Mittels Docker kann jeder Benutzer seine private Instanz der Applikation starten. Das Ausutzen der Schwachstellen hat somit keine Seiteneffekte für andere Anwender der Plattform.
Der zweite grosse Aspekt der Arbeit war die Formulierung der Aufgabenstellungen. Für jede Lücke musste ein realistisches Szenario ausgedacht werden, für welches wiederum eine Aufgabenstellung inklusive Musterlösung erstellt wurde. Diese Aufgaben gilt es im Rahmen der praktischen Übungen zu lösen.