art of defence

Sicherheit von Web-Applikationen

"Grünes Licht für verlässlichere Online-Services"

Deutschland sicher im Netz e.V.

Köln, 24.01.2008

Georg Heß

Agenda

- Kurzprofil der art of defence GmbH
- Sicherheitsleck Web-Applikationen
- Technologie im Überblick
- Chancen für ISPs

Kurzprofil

Deutscher Softwarehersteller

Entwicklung und Forschung in Regensburg

Enterprise Web Application Firewall

Plug-In für Webserver, Application Gateway, LoadBalancer und Firewall

Partnerschaften

Technologie Partnerschaften, vertriebliche Partnerschaften, ...

Partnerschaft mit Microsoft

- Tiefengefördertes Unternehmen der Microsoft High-Tech-Gründerinitiative “unternimm was”

Agenda

- Kurzprofil der art of defence GmbH
- Sicherheitsleck Web-Applikationen
- Technologie im Überblick
- Chancen für ISPs

Sponsored by

Sie sind Gast
Einloggen | Registrieren

Suche

los

Im Browser einrichten

News

- 7-Tage-Alerts
- 7-Tage-News
- News-Archiv
- Newsletter
- English News

Anzeige

Hintergrund

- BSI-Info
- Know-how
- Kommentar
- Praxis
- Produkte
- Hintergrund-Archiv

News

Meldung vom 04.10.2007 19:05 [<< Vorige] [Nächste >>]

Zehntausende Kartenhaus-Kunden von Kreditkartendaten-Diebstahl betroffen

vorlesen

Der Hamburger Ticketverkäufer Kartenhaus hat seine Kunden am heutigen Donnerstag darüber informiert, dass bislang unbekannte Täter Kreditkartennummern und Rechnungsanschriften gestohlen haben. Betroffen sollen 66.000 Kunden sein, die zwischen dem 24. Oktober 2006 und dem 30. September 2007 über die Website Kartenhaus.de mit Kreditkarten Tickets gekauft haben. Ausgenommen davon seien lediglich Kreditkartenkäufe von Eintrittskarten für Hertha BSC, HSV Handball und die Eisbären Berlin.

Die Muttergesellschaft Ticketmaster rät den Kunden "schnellstmöglich ihre Kreditkartenabrechnung zu prüfen, um mögliche Unregelmäßigkeiten oder Missbrauch zu identifizieren". Wie der oder die Täter an die Daten kamen, ist bislang nicht bekannt. Die Rede ist lediglich von einem Server, der betroffen gewesen sein soll. Man habe unmittelbar nach Bekanntwerden des Angriffs ein internes Team zusammengestellt, um die Sicherheitslücke zu identifizieren und alle notwendigen Stellen darüber zu informieren, erklärte der stellvertretende Vorsitzende von Ticketmaster Europe, Tommy Higgins.

Die eventuell betroffene Konsumenten seien gewarnt worden. Über eine spezielle Website sollen sie weitere Informationen erhalten. Dabei würde sehr eng mit den relevanten Banken und Karteninstituten zusammengearbeitet. Außerdem sei Anzeige erstattet worden, damit die Verantwortlichen juristisch belangt werden. Das zum IAC-Konzern gehörende Unternehmen Ticketmaster hatte die Kartenhaus GmbH im November 2005 übernommen. Im Jahr 2006 verkaufte Ticketmaster rund 128 Millionen Tickets im Wert von mehr als 7 Milliarden US-Dollar. (pmz/c't)

art of defence

SQL-Injection

Directory Traversal

Injection flaws

Cross-Site Scripting

Malicious File Execution

…

Webportal CMS Webshop OWA

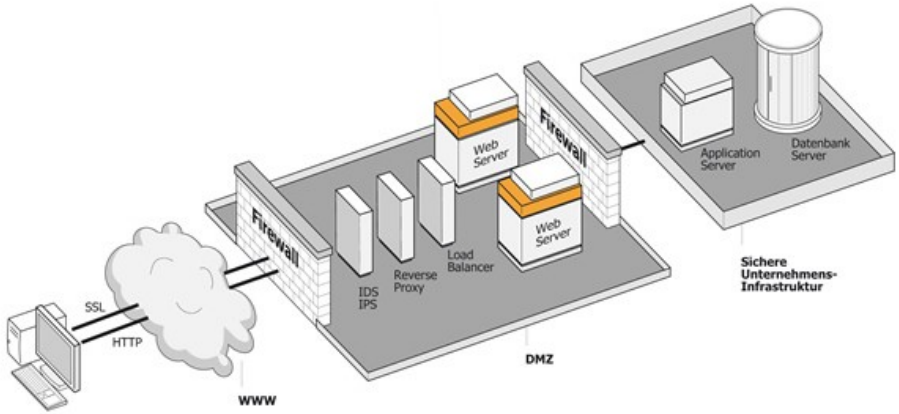
Anwendung

Framework

Webserver

application layer

network layer



art of defence

A1 – Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, etc.
A2 – Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 – Insecure Remote File Include	Code vulnerable to remote file inclusion allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise.
A4 – Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 – Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker.
A6 – Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to violate privacy, or conduct further attacks.
A7 – Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 – Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 – Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 – Failure to Restrict URL Access	Frequently, the only protection for sensitive areas of an application is links or URLs are not presented to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations.

OWASP TOP 10

2007 RELEASE CANDIDATE 1

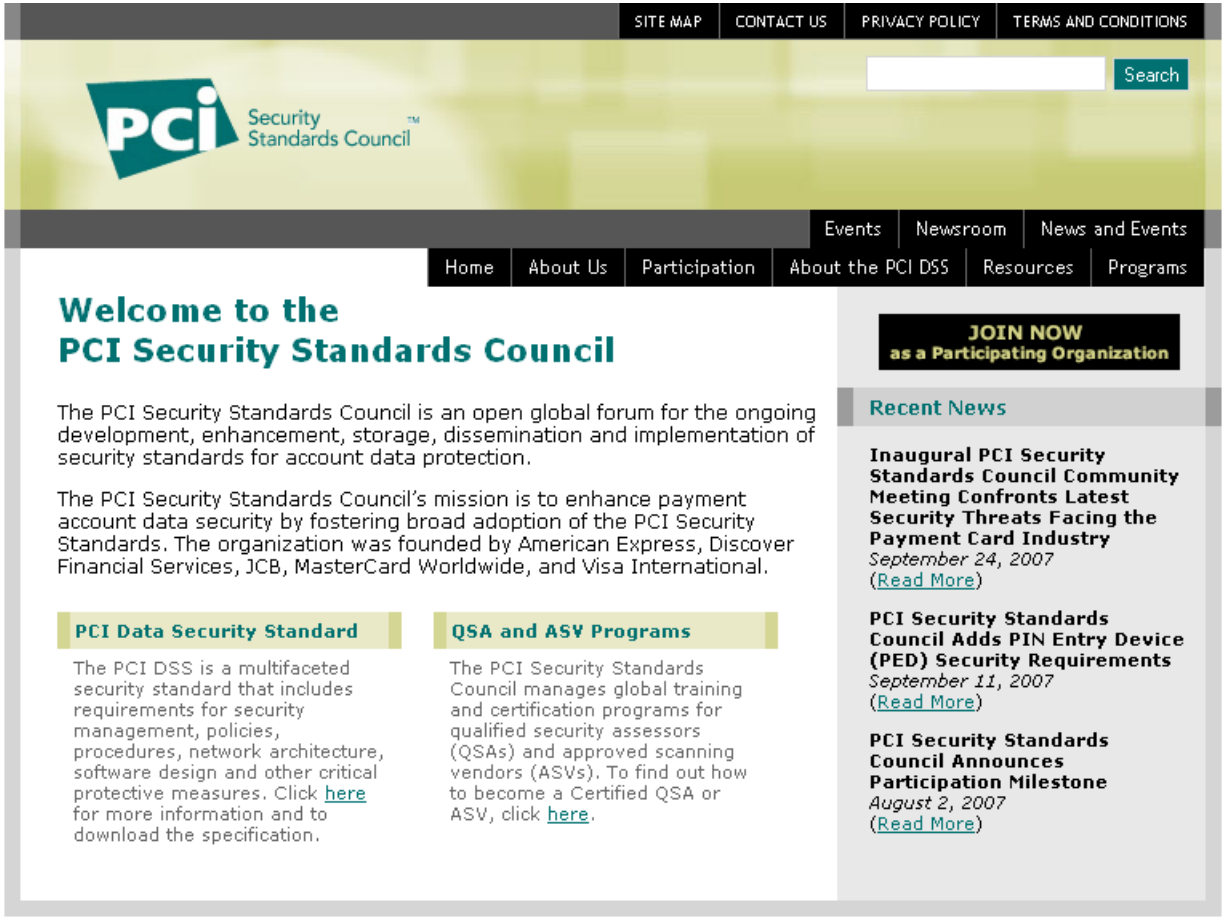
THE TEN MOST CRITICAL WEB APPLICATION SECURITY VULNERABILITIES

2007 UPDATE

art of defence

Beispiel: PCI Data Security Standard

Payment Card Industry



art of defence

PCI Data Security Standard 1.1

6.5 Entwickeln Sie alle Webanwendungen auf der Grundlage von sicheren Codierrichtlinien, z. B. den *Open Web Application Security Project-Richtlinien*. Überprüfen Sie benutzerdefinierten Anwendungscode auf Sicherheitsrisiken. Verhindern Sie häufig auftretende Codesicherheitsrisiken in Softwareentwicklungsprozessen, um Folgendes zu vermeiden:

- **6.5.1** Nicht überprüfte Eingaben
- **6.5.2** Unterbrochene Zugriffssteuerung (z. B. böswillige Verwendung von Benutzer-IDs)
- **6.5.3** Unterbrochene Authentifizierungs- und Sitzungsverwaltung (Verwendung von Kontoanmeldeinformationen und Sitzungscookies)
- **6.5.4** XSS (Cross-Site-Scripting)-Angriffe
- **6.5.5** Pufferüberläufe
- **6.5.6** Injektionslücken (z. B. SQL (Structured Query Language)-Injektion)
- **6.5.7** Nicht ordnungsgemäße Fehlerbehandlung
- **6.5.8** Unsichere Speicherung
- **6.5.9** Denial of Service
- **6.5.10** Unsichere Konfigurationsverwaltung

6.6 **Stellen Sie sicher, dass alle Webanwendungen durch eine der folgenden Methoden vor bekannten Angriffen geschützt werden:**

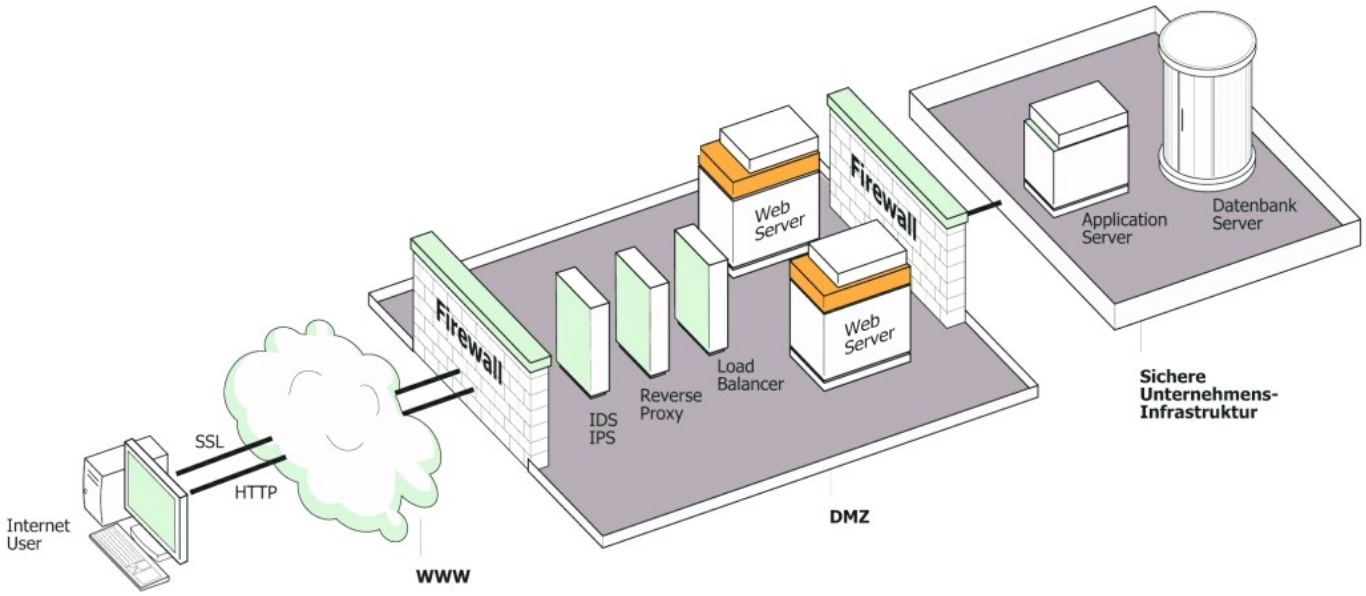
- **Überprüfung sämtlichen benutzerdefinierten Anwendungscodes auf häufig auftretende Sicherheitslücken durch eine auf Anwendungssicherheit spezialisierte Organisation**

Hinweis: Diese Methode gilt bis zum 30. Juni 2008 lediglich als Best Practice, wird dann jedoch obligatorisch.

Agenda

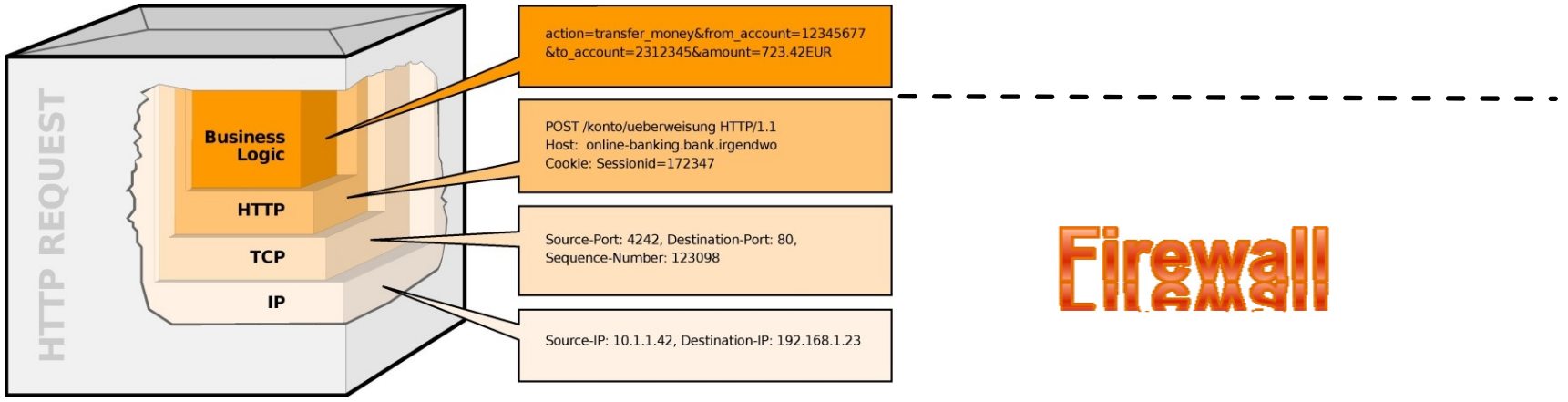
- Kurzprofil der art of defence GmbH
- Sicherheitsleck Web-Applikationen
- Technologie im Überblick
- Chancen für ISPs

Einsatzszenario



u.a. Plug-In in Webserver – MS IIS 6.0 und 7.0

HTTP-Request-Analyse



Es werden alle eingehenden Anfragen
und die Antworten des Web-Servers untersucht

Agenda

- Kurzprofil der art of defence GmbH
- Sicherheitsleck Web-Applikationen
- Technologie im Überblick
- Chancen für ISPs

Chancen für ISPs

Vermarktung von

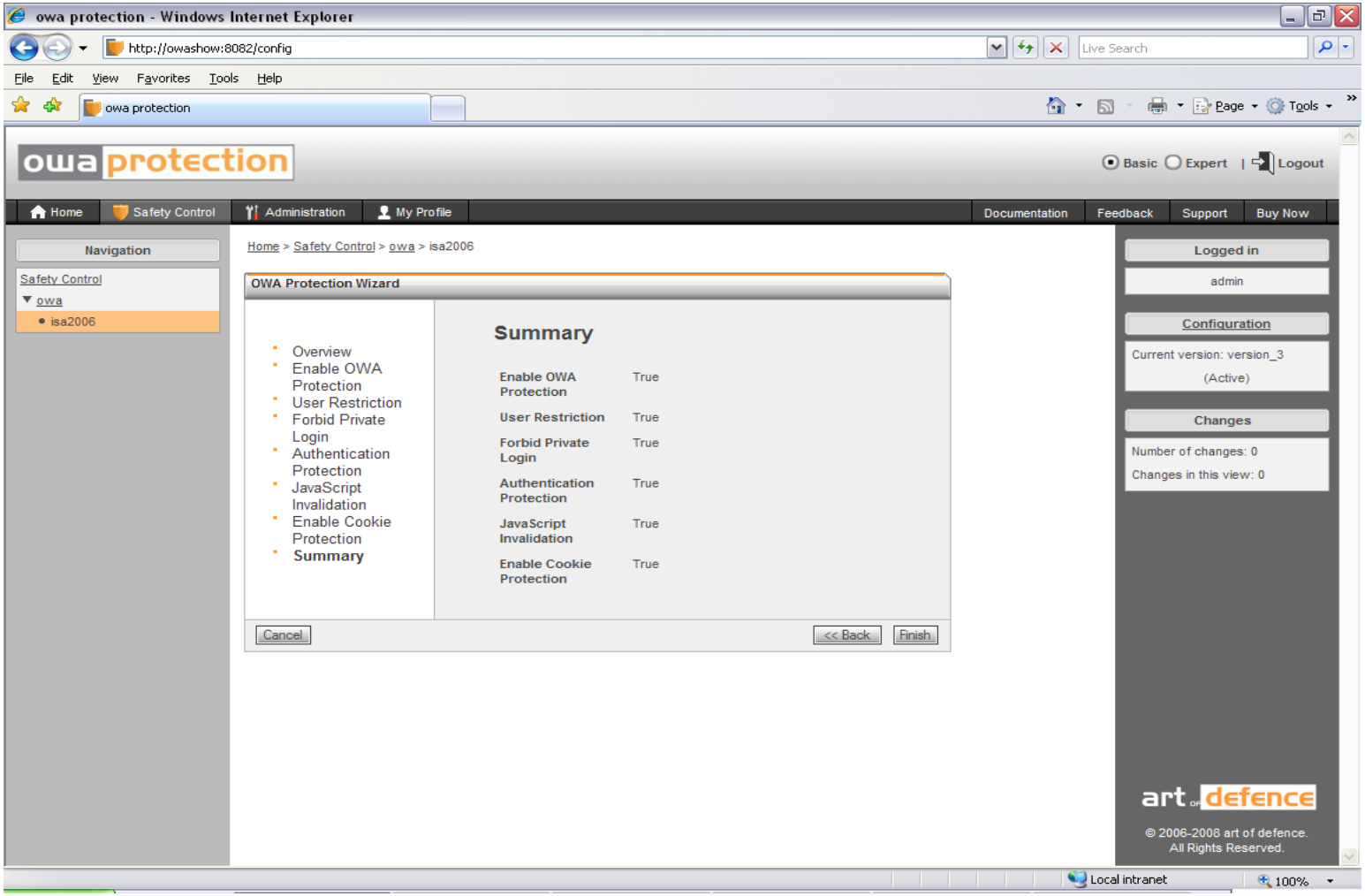
- Speziell abgesicherten "Standard Web Apps"
- "Grundschutz inkl. Updates" für Kunden Web-Apps
- Konfigurierbarer Enterprise Web Application Firewall mit zentraler Administration

Einsatz zur Absicherung eigener kritischer Web-Applikationen (z. B. Admin-Interfaces)

Abgesicherte “Standard Web Apps”

- Problemstellung
  - Weit verbreitete Web-Applikationen wie z. B. Outlook Web Access, Sharepoint oder CMS-Systeme weisen Schwachstellen auf Web-Anwendungs-Ebene auf.
- Lösung
  - art of defence bietet – sehr einfach zu konfigurierende –Schutz-regelwerke (“White-Lists”) für Standard-Applikationen und bietet hierfür einen Update-Service.
- Chance für den ISP
  - Ist die Standard-Applikation Teil seines Hosted-Services-Angebot, so ist die zusätzliche Absicherung gegen Angriffe auf Web-App-Ebene ein Alleinstellungsmerkmal im Wettbewerb.
  - Chance auf höheren Umsatz pro Kunde

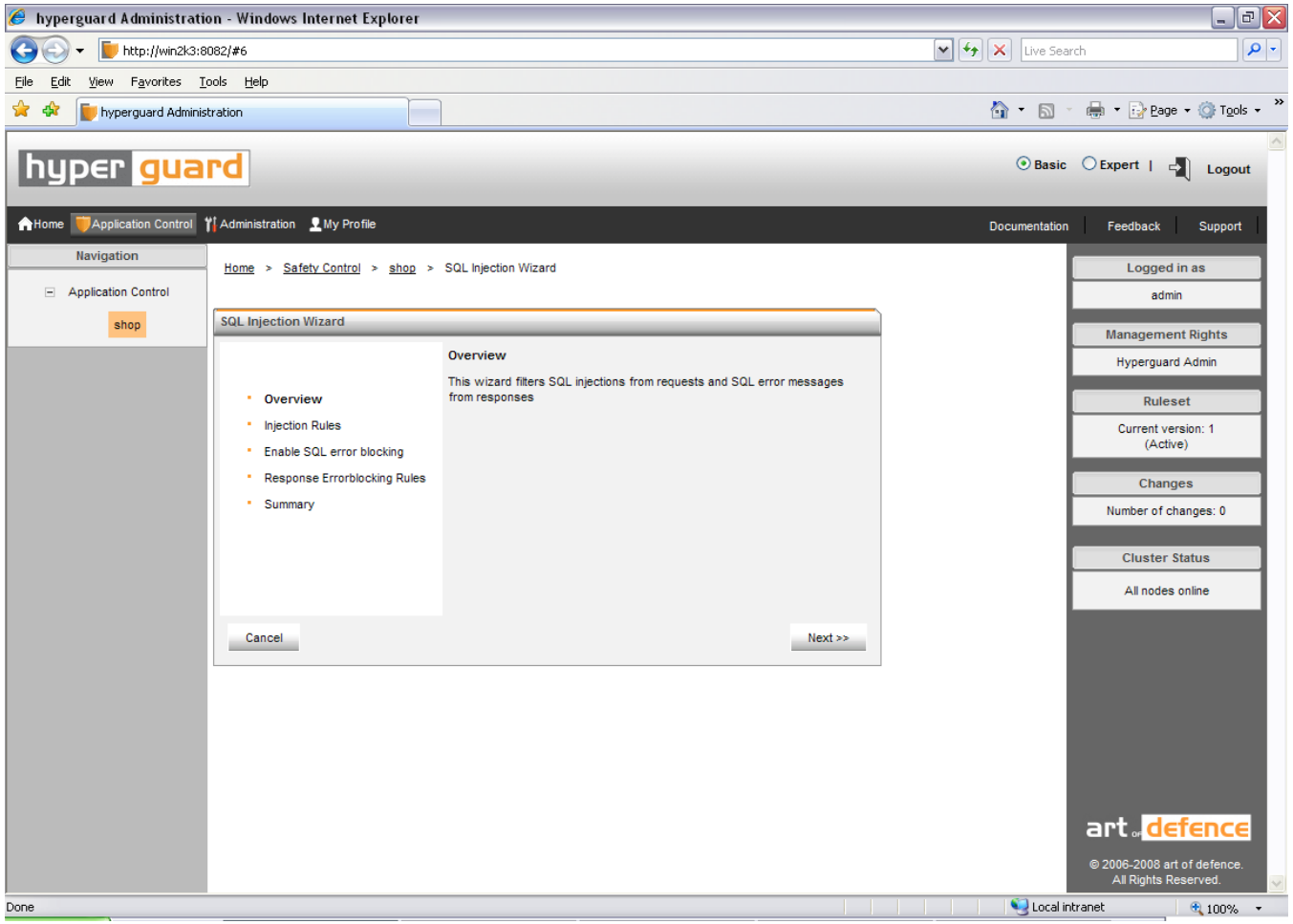
Beispiel: OWA Protection



Grundschutz für Kunden Web Apps

- Problemstellung
  - Kundenspezifische Web Apps weisen oft erhebliche Schwachstellen auf Web-App-Ebene auf (Kontakt-Formulare als "Spam-Relay", Anfälligkeiten bzgl. "altbekannter" Schwachstellen (Patching ?))
- Lösung (1. Schritt ;-))
  - Grundschutz (unabhängig von konkreter Web App !) inkl. Updates:
  - Erkennung bekannter Angriffsmuster (SQL-Injection, XSS etc.)
  - Absicherung bekannter Schwachstellen, z.B. Sicheres Session Management durch Secure CookieJar
  - Erkennung von ungewöhnlichem Verhalten des Clients
- Chance für den ISP
  - Vermarktung des Grundschutzes – ähnlich zu "Shared Firewalls"
  - Reduktion von lästigen "Aufräumarbeiten" nach erfolgreichen Angriffen

Beispiel: SQL-Injection Wizard



"Shared" Enterprise WAF

- Problemstellung
  - Hosting von unternehmenskritischen Web Apps von "Premium Kunden" erfordert ggfs. einen auf die Web App im Detail möglichst optimal angepassten Schutz
- Lösung
  - Die frei konfigurierbare Enterprise Web Application Firewall hyperguard wird als Hosted Service vom ISP mit angeboten.
- Chancen für den ISP
  - Kunde übernimmt Konfiguration und Pflege des Regelwerks selbst – monatliche Nutzungsgebühr für hyperguard
  - hyperguard als Teil von "Managed Security Services" (Expertise intern erforderlich !) - Nutzungs- und Dienstleistungs-Umsatz

Zentrales Management und Reporting

Vielen Dank!

Georg Heß