

# DIPLOMARBEIT

## WebSecure

Ausgeführt im Schuljahr 2012/2013 von:

Paul Pfeiffer-Vogl 5AHITT

Harun Koyuncu 5AHITT

Patrick Ullrich 5AHITT

Kevin Schneider 5AHITT

Betreuer/Betreuerin:

Michael Borko, Bakk. techn.

Mag. Hans Brabenetz

Wien, am 14.05.2013

tgm | Technologisches Gewerbemuseum | Höhere Technische Bundes- Lehr- und Versuchsanstalt  
Wexstraße 19-23 | A-1200 Wien | ☎ +43 1 33126 | FAX: +43 1 33126 204 | E-Mail: info@tgm.ac.at

## Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

---

Ort, Datum

---

Paul Pfeiffer-Vogl (Product Owner)

---

Harun Koyuncu

---

Patrick Ullrich

---

Kevin Schneider

## INHALTSVERZEICHNIS

---

1. Abstract.....	5
2. Kurzfassung.....	6
3. Einleitung.....	7
4. Projektorganisation.....	8
4.1 Das Projektteam.....	8
4.1.1 Product Owner.....	8
4.1.2 Projektmitglieder.....	8
4.2 Scrum.....	9
5. Problem Beschreibung.....	11
5.1 Momentane Situation.....	11
5.2 Lösungsansatz.....	11
5.3 Zielsetzung.....	12
6. Kundenschnittstelle.....	13
6.1 PayPal Schnittstelle.....	13
6.1.1 Technologien.....	13
6.2 Server.....	14
6.2.1 Skripting unter Linux.....	14
6.2.2 Cron-Jobs.....	14
6.3 Webseite.....	15
6.3.1 Benutzerschnittstelle.....	15
6.3.2 Aufbau.....	15
6.3.3 Konfiguration.....	16
6.4 Datenbank.....	17
6.4.1 Schemadefinition (EER-Diagramm).....	17
7. BackTrack.....	19
8. Analyse.....	20
8.1 Nutch.....	20
8.1.1 Fazit.....	20
8.2 Heritrix.....	20
8.2.1 Architektur.....	20
8.2.2 Konfiguration.....	22
8.2.3 Verwendung.....	24
8.2.4 Log-Informationen des Scans.....	26
8.3 NMap.....	27

8.3.1	Architektur.....	27
8.3.2	Konfiguration.....	28
8.3.3	Verwendung.....	30
8.4	Nikto.....	31
8.4.1	Architektur.....	31
8.4.2	Konfiguration.....	32
8.4.3	Verwendung.....	33
9.	Angriff.....	34
9.1	SQL- Injektionen.....	34
9.1.1	Allgemein.....	34
9.2	SQLMap.....	36
9.2.1	Architektur.....	36
9.2.2	Konfiguration.....	37
9.2.3	Verwendung.....	38
9.3	W3af.....	40
9.3.1	Verwendung.....	41
9.3.2	Konfiguration.....	43
9.4	Metasploit.....	45
9.4.1	Architektur.....	46
9.4.2	Konfiguration.....	52
9.4.3	Verwendung.....	54
9.5	Externe Wissensdatenbanken.....	57
9.5.1	Exploit-Database.....	58
9.5.2	1337Day.....	59
9.5.3	Common Vulnerabilities and Exposures.....	59
9.5.4	National Vulnerability Database.....	60
9.5.5	Packet Storm Security.....	60
9.5.6	OSVDB.....	60
10.	Implementierung.....	61
10.1	Koordination.....	61
10.1.1	Space based computing.....	61
10.1.2	Containerstruktur.....	61
10.1.3	Koordinatoren.....	63
10.1.4	Koordinatoren.....	65
10.1.5	Pull- und Push prinzip.....	67

10.1.6	Notifications.....	67
10.1.7	Aspekte.....	69
10.1.8	Transaktionen.....	69
10.1.9	Webseiten Agent.....	71
10.1.10	Whiteboard Agent.....	72
10.1.11	Tool Agent.....	72
10.1.12	Aktivitätsdiagramm.....	74
10.1.13	Klassendiagramm.....	75
10.2	Webseite.....	75
10.2.1	Einleitung.....	75
10.2.2	Technologien.....	75
10.2.3	Grundfunktionen.....	76
10.2.4	Benutzerfunktionen.....	79
10.2.5	Sicherheitsaspekte.....	81
10.3	Cloudcomputing.....	82
10.3.1	Einleitung.....	82
10.3.2	Technologien.....	82
10.3.3	Leistungen und Preise.....	83
10.3.4	AMI Instanz starten.....	84
10.4	Kundenschnittstelle.....	91
10.4.1	PayPal.....	91
10.5	Heritrix.....	97
10.5.1	Befehle.....	97
10.5.2	Verwendung.....	98
10.6	NMap.....	99
10.6.1	Ablauf der Nmap-Analyse.....	99
10.7	Nikto.....	101
10.7.1	Ablauf der Nikto-Analyse.....	101
10.8	SQLMap.....	102
10.8.1	Ablauf des SQLMap-Tools.....	102
10.9	Metasploit.....	105
10.9.1	Ablauf des Metasploit-Tools.....	105
10.10	Externe Wissensdatenbanken.....	108
10.10.1	Exploit-Database.....	108
10.10.2	Suche.....	108

10.10.3	Ausführen der Exploits.....	108
11.	Wirtschaftliche Aussichten.....	114
11.1	Marktumfeldanalyse.....	114
11.2	Marketing.....	115
11.3	Paketbeschreibung.....	115
11.3.1	Arctic.....	115
11.3.2	Pyro.....	116
11.3.3	Twister.....	116
11.4	Zukunftsaussichten für das Projekt.....	116
12.	Rechtliche Lage.....	117
12.1	Aktuelle Rechtslage.....	117
12.2	Allgemeine Geschäftsbedingungen.....	117
13.	Conclusio.....	118
14.	Danksagung.....	118
15.	Glossar.....	118
16.	Literaturverzeichnis.....	119
17.	Abbildungsverzeichnis.....	124
18.	Tabellenverzeichnis.....	126
19.	Listingverzeichnis.....	127

## 1. ABSTRACT

---

WebSecure is an online service, which gives a service provider the possibility of checking his system on possible safety gaps or any technical weaknesses. In the case of the utilization of WebSecure-Service the customer is instantly informed, if there is an acute safety problem for his server. In order to make the management and handling of the service as easy as possible, a website has been set up, in which an automatic payment, authorization and execution system is provided.

So that the attack mechanism is able to work properly, the service itself has to come to knowledge of which possible ways of inspecting a server are given. At the same time, the service has to be updated constantly, in order to recognize even the newest safety gaps. These attack mechanisms get the information from so-called exploit-databases and the results of analysis tools. In this database any safety weaknesses are continually updated and laid off in a specified structure. This data information is processed by an Agent and then taken over into an own database. After this analysis of the system the attack mechanism can work properly.

Due to the fact that the attack from a single server on a target server can easily be traced with the help of the IP-address, modern blockmechanisms are able to impede further attacks on the server. This is where the Cloud-system comes into play. Several Agents are installed on each of these Cloud-servers to produce a dispersed system. Since the computing power is distributed, a performed attack according to the time can be completed.



WebSecure ist ein Online-Service, welcher einem Serverbetreiber die Möglichkeit bietet sein System auf Sicherheitslücken bzw. Schwachstellen zu überprüfen. Dabei soll der Kunde bei dem Einsatz vom WebSecure-Service aufmerksam gemacht werden, wenn ein akutes Sicherheitsrisiko auf seinem Server besteht. Um den Kunden eine möglichst einfache Bedienung des Services zu gewährleisten, wurde eine Webseite mit automatisierten Bezahlungs-, Autorisierungs- und Exekutionssystem bereitgestellt.

Damit überhaupt ein Angriff stattfinden kann, muss das Service selbst das Wissen erlangen, auf welche Art der Server untersucht werden kann. Genauso, muss der Service ständig aktuell gehalten werden, damit dieser weiß, wo neue Sicherheitslücken aufgetreten sind. Dieses Wissen beziehen die Angriff-Tools von sogenannten Exploit-Datenbanken und von Ergebnissen der Analyse-Tools. In dieser Datenbank werden die Sicherheitslücken ständig aktualisiert und in einer festgelegten Struktur abgespeichert. Die Daten werden von einem Agent ausgelesen und in eine eigene Datenbank übernommen.

Nach der Analyse des Systems können gezielte Angriffe auf den Server gestartet werden.

Da nun aber mit einem einzelnen Rechner die Untersuchung auf den Zielsystem leicht anhand der IP-Adresse zu identifizieren ist, blockieren moderne Sicherheitsmechanismen die weiteren Zugriffe auf den Server. Deshalb kommt ein Cloud-System ins Spiel.

Es werden nun mehrere Agents auf den Cloud-Rechnern installiert, um ein verteiltes System zu schaffen. Da die Rechenleistung verteilt ist, kann ein leistungsstarker Angriff ausgeführt werden.