

Hochschule Heilbronn
Fakultät für Informatik

Bachelorarbeit

Evaluation von Web Application Vulnerability Scannern

**vorgelegt an der Hochschule Heilbronn, Fakultät für Informatik zum Abschluss
eines Studiums im Studiengang Angewandte Informatik**

Henning Janning

Matrikelnummer: 192972

Eingereicht am: 04.04.2019

Erstprüfer: Prof. Dr.-Ing. Andreas Mayer
Zweitprüferin: Susanne Steuer, M.Sc.

Zusammenfassung

Cyberangriffe von kriminellen Hackern nehmen weltweit zu und stellen sowohl für Unternehmen als auch für Privatpersonen eine reale Bedrohung dar. Das Thema Sicherheit spielt eine immer größer werdende Rolle im IT-Bereich, insbesondere Webanwendungen stehen hier im Fokus, da sie in der Regel weltweit erreichbar sind. Um sie gegen Angriffe abzusichern, ist es unter anderem notwendig, sie auf Schwachstellen zu testen, so wie es auch ein potenzieller Angreifer täte.

In dieser Thesis werden die dafür verwendeten Tools, die Web Vulnerability Scanner (WVS) auf ihre Tauglichkeit überprüft. Aus der großen Menge an Open Source und kommerziellen WVS werden die vielversprechendsten herausgefiltert und mittels Angriffe auf mehrere verwundbare Webanwendungen verglichen. Neben der Anzahl der gefundenen Schwachstellen wird auch ermittelt, wie sich die WVS in den Kategorien Bedienung, Reporting und Geschwindigkeit unterscheiden, welche WVS insgesamt am besten abschneiden und ob die Open Source WVS im Vergleich mit den kommerziellen Produkten bestehen können.

Im Gesamtranking schneidet kommerzielle WVS "BurpSuite Pro" am besten ab, aber auch Open Source WVS wie Arachni oder OpenVAS sind auf den vorderen Plätzen zu finden. Sie stellen damit eine vollwertige, kostengünstige Alternative dar. Bei der Anzahl der Schwachstellen fallen die Ergebnisse der WVS sehr unterschiedlich aus, auffällig ist das Fehlen von Mustern oder Regelmäßigkeiten.

Ein Ansatz für weiterführende Forschungen ist das Verifizieren der Funde, um fälschlicherweise gefundene Schwachstellen auszusortieren und exaktere Ergebnisse zu erhalten.

Abstract

Cyber-attacks by criminal hackers are increasing worldwide, posing a real threat to both businesses and individuals. Security is playing an increasingly important role in the IT sector, with web applications in particular, as they are generally accessible worldwide. Among other things, in order to protect them against attacks, it is necessary to test them for vulnerabilities, just as a potential attacker would do.

In this thesis, the tools used for this, the Web Vulnerability Scanners (WVS), are checked for suitability. From the vast amount of open source and commercial WVS, the most promising are filtered out and compared by attacks on several vulnerable web applications. In addition to the number of vulnerabilities found, it is also determined how the WVS differ in terms of handling, reporting and speed, which WVS performs best and whether open source WVS can compete with commercial products.

In the overall ranking, commercial WVS 'BurpSuite Pro' performs best, but open source WVS such as Arachni or OpenVAS are also in the lead. They therefore represent a full-fledged, cost-effective alternative. About the number of vulnerabilities, the results of the WVS are very different, with the striking lack of patterns or regularities.

One approach to further research is to verify the findings in order to sort out wrongly found vulnerabilities and obtain more accurate results.

Inhaltsverzeichnis

Abbildungsverzeichnis	vi
Tabellenverzeichnis	vii
Abkürzungsverzeichnis	ix
1 Einführung	1
2 Grundlagen	5
2.1 Webanwendung	5
2.2 Schwachstellen	6
2.3 Web Application Security	9
2.3.1 Bedrohungen und Risiken	9
2.3.2 Sicherheitsmaßnahmen	10
2.3.2.1 Security Tests	10
2.3.2.2 Penetration Testing	12
2.3.2.3 Web Application Firewalls	14
2.4 Funktionsweise WVS	15
3 Methodik	17
3.1 Testaufbau	17
3.2 Web Application Vulnerability Scanner	19
3.2.1 Auswahlkriterien	19
3.2.2 Nicht ausgewählte WVS	19
3.2.2.1 Kommerzielle WVS	19
3.2.2.2 Open Source WVS	20
3.2.3 Ausgewählte WVS	22
3.2.3.1 Open Source WVS	22
3.2.3.2 Kommerzielle WVS	22
3.3 Verwundbare Webanwendungen	23
4 Evaluation	24
4.1 Scanzeiten	24
4.2 Gefundene Schwachstellen per Webanwendung	25
4.3 Bedienung, Reporting und Geschwindigkeit	26
4.3.1 Open Source	26

4.3.2	Kommerziell	30
4.3.3	Gesamtbewertung und Ranking	34
5	Diskussion	35
5.1	Anzahl der gefundenen Schwachstellen	35
5.2	Bedienung, Reporting und Scan-Geschwindigkeit	36
5.2.1	Bedienung	36
5.2.2	Reporting	37
5.2.3	Scan-Geschwindigkeit	37
5.3	Ranking	37
5.4	Open Source im Vergleich mit kommerziellen WVS	38
6	Fazit und Ausblick	39
	Quellenverzeichnis	41
	Anhang	
A	Screenshots der Berichte	44
	Eidesstattliche Erklärung	51

Abbildungsverzeichnis

1.1	Gefundene Schwachstellen pro Jahr	1
1.2	Bitkom Studie - Bedrohungsszenarien	2
2.1	3-Tier-Architektur einer Webanwendung	6
2.2	Lebenszyklus einer Schwachstelle	8
3.1	Testaufbau	18
3.2	W3af: Fehlende Module	21
4.1	Arachni WebUI 0.5.12	27
4.2	OpenVAS im Greenbone Security Assistant	28
4.3	Grafische Benutzeroberfläche von ZAP	29
4.4	Grafische Benutzeroberfläche von Netsparker	30
4.5	Weboberfläche von Acunetix	31
4.6	Grafische Benutzeroberfläche von Nessus	32
4.7	Dashboard von BurpSuite Pro	33
4.8	Confidence-Tabelle im Report von BurpSuite Pro	33
A.1	Bericht Acunetix	44
A.2	Bericht BurpSuite Pro	45
A.3	Bericht Nessus	46
A.4	Bericht Netsparker	47
A.5	Bericht Arachni	48
A.6	Bericht OpenVAS	48
A.7	Bericht Nikto	49
A.8	Bericht Wapiti	50
A.9	Bericht ZAP	50

Tabellenverzeichnis

3.1	Ausgewählte Free und Open Source WVS	22
3.2	Ausgewählte kommerzielle WVS	22
4.1	Scanzeiten der Open Source WVS in Minuten	24
4.2	Scanzeiten der kommerziellen WVS in Minuten	24
4.3	Gefundene Schwachstellen der Open Source WVS	25
4.4	Gefundene Schwachstellen der kommerziellen WVS	25
4.5	Bewertung der Open Source WVS	34
4.6	Bewertung der kommerziellen WVS	34
4.7	Ranking aller WVS	34

Abkürzungsverzeichnis

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CGI	Common Gateway Interface
CPU	Central Processing Unit
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Testing
DoS	Denial of Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
JSP	JavaServer Pages
LDAP	Lightweight Directory Access Protocol
NTLM	New Technology Lan Manager
OS	Operating System
OWASP	Open Web Application Security Project
RAM	Random-Access Memory
REST	Representational State Transfer

SAST	Static Application Security Testing
SCA	Statische Code Analyse
SPA	Single Page Application
SSL	Secure Sockets Layer
SQL	Structured Query Language
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAF	Web Application Firewall
WASC	Web Application Security Consortium
WVS	Web Vulnerability Scanner
WWW	World Wide Web
XML	Extensible Markup Language
XSS	Cross Site Scripting
ZAP	Zed Attack Proxy

1 Einführung

In den letzten zwei Jahrzehnten hat sich das World Wide Web (WWW) von einem reinen Informationsspeicher in eine Plattform mit hochfunktionalen Anwendungen verwandelt, die nicht nur sensible Daten verarbeiten, sondern auch Aktionen durchführen, die einflussreiche Auswirkungen auf die reale Welt haben. Mit jeder Weiterentwicklung bringen Webanwendungen neue Sicherheitslücken mit sich und so verändern sich auch die Art und die Anzahl der am häufigsten auftretenden Fehler. Es gibt Angriffe auf Schwachstellen, die bei der Entwicklung der Webanwendungen noch nicht bekannt waren und daher nicht berücksichtigt wurden. Andere Attacks haben an Bedeutung verloren, da das Bewusstsein für sie gestiegen ist oder aufgrund von Verbesserungen der Web-Browser Software. Neue Technologien bergen jedoch auch immer das Risiko von neuen Sicherheitslücken und so ist "...in gewissem Maße die Sicherheit von Webanwendungen heute das bedeutendste Schlachtfeld zwischen Angreifern und solchen, die Daten schützen und Computerressourcen verteidigen müssen, und dies wird wahrscheinlich auf absehbare Zeit so bleiben." [1, S.6]

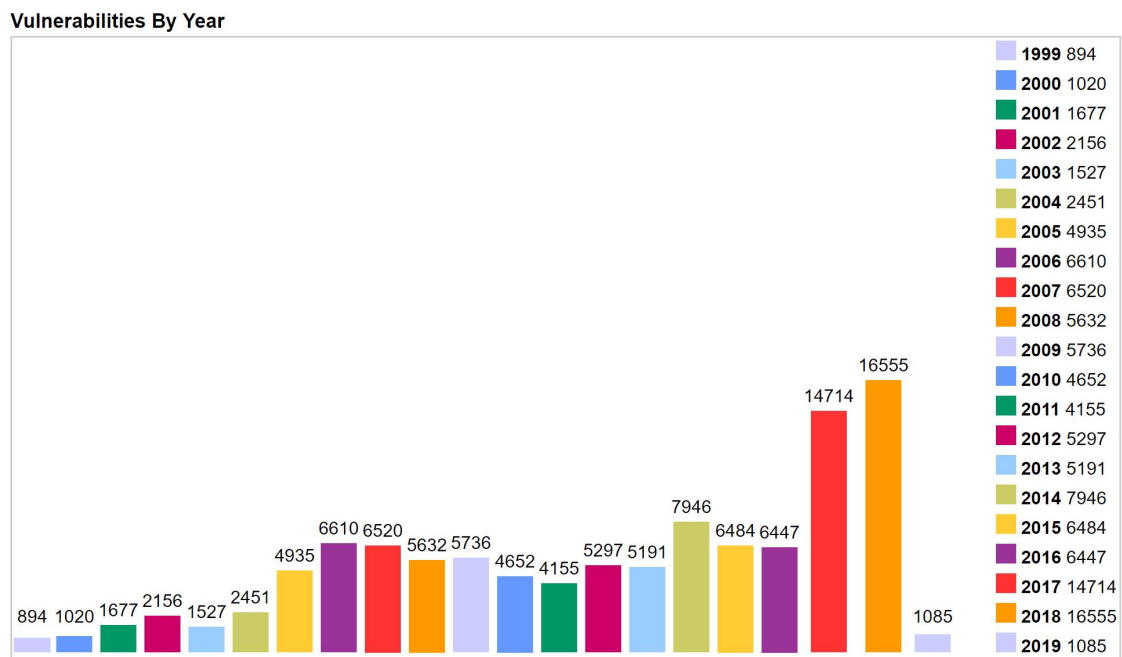


Abbildung 1.1: Gefundene Schwachstellen pro Jahr [2]: Die Anzahl hat sich in den letzten zwei Jahren mehr als verdoppelt.

Mit der Anzahl der Webanwendungen steigt auch der Einfluss des WWW auf alle Lebensbereiche, sei es beim Einkaufen im Online-Shop einschließlich diverser Bezahlssysteme, dem Nachrichtenaustausch über Social-Media-Kanäle oder nur zur Informationsgewinnung auf Nachrichtenseiten.

Fortschreitende Digitalisierung und weltweite Vernetzung verursachen jedoch auch immer mehr Sicherheitslücken: Abb. 1.1 zeigt, dass sich die Anzahl der gefundenen Schwachstellen in den letzten zwei Jahren mehr als verdoppelt hat.

Zunehmende Cyberangriffe von kriminellen Hackern, aber auch von politisch oder ideologisch motivierten Angreifern sind die Folge. Aktuelle Beispiele sind der Angriff auf die Münchner Firma Krauss Maffai im Dezember 2018, der die Produktion des Maschinenbauunternehmens für mehrere Tage lahmlegte oder die Attacke auf das Datennetz des Deutschen Bundestags im Oktober 2018. Das Datenleck „Collection #1“, das im Januar 2019 auftauchte, ist das Ergebnis einer Vielzahl von Cyberattacken, es enthält über 2,6 Milliarden Datensätze mit Zugangsdaten und Passwörtern für hunderte Webseiten.

Für die betroffenen Firmen ist der Schaden enorm: Laut einer Studie des Digitalverbands Bitkom lag der durch Cyberattacken verursachte wirtschaftliche Gesamtschaden für Industrieunternehmen in Deutschland innerhalb der letzten zwei Jahre bei über 43 Milliarden Euro [3]. Aus der gleichen Studie geht hervor, dass unentdeckte Sicherheitslücken von Unternehmen als größte Bedrohung angesehen werden (siehe Abb. 1.2).

Unentdeckte Sicherheitslücken als größte Bedrohung

Inwieweit betrachten Sie die folgenden Szenarien als zukünftige Bedrohung für die IT-Sicherheit Ihres Unternehmens?

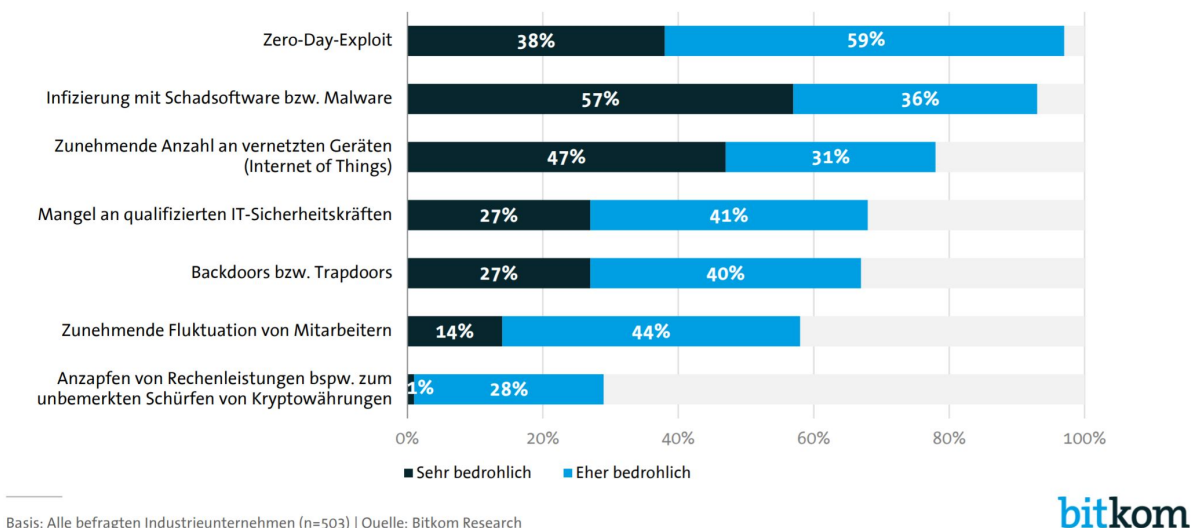


Abbildung 1.2: Bitkom Studie [3]: Unentdeckte Sicherheitslücken werden von Unternehmen als größte Bedrohung angesehen.

Es gibt mehrere Ansätze, diesem Risiko zu begegnen: Grundsätzlich sollte der Entwickler einer Webseite von Beginn an eine Programmierung anstreben, die bereits bekannte Sicherheitslücken vermeidet und so potenziellen Angreifern möglichst wenig Angriffsfläche bietet. Hier gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem “Leitfaden zur Entwicklung sicherer Webanwendungen” [4] Hilfestellung. Fehler in der Programmierung lassen sich jedoch nicht immer ausschließen, zudem ist auch ein Schutz gegen unentdeckte Sicherheitslücken vonnöten.

Neben dem Einsatz von Web Application Firewalls (WAFs), die den Datenstrom zwischen Browser und Webapplikation überwachen, ist die Verwendung von WVS im Rahmen von Penetration Tests ein wesentlicher Bestandteil von Sicherheitskonzepten.

WVS überprüfen Webanwendungen automatisiert auf Schwachstellen und unterstützen dadurch den Penetration Tester beim Aufspüren von Sicherheitslücken.

Die vorliegende Arbeit macht sich die Evaluation von WVS zur Aufgabe, da die wenigen bisherigen Ausarbeitungen zu diesem Thema veraltet sind und teilweise andere Ansätze verfolgen:

- Holm vergleicht in seiner Studie aus dem Jahr 2011 lediglich kommerzielle Scanner und verzichtet auf Bewertungskategorien wie Bedienung und Reporting. [5]
- Wundram behandelt das Thema zweimal, in seinen Vergleichen von 2011 und 2012 finden sich veraltete Programme wie Watobo oder das inzwischen nicht mehr lauffähige W3af. [6, 7]

Zusätzliche Motivation ist die große Anzahl und Vielfalt der Scanner: Das Open Web Application Security Project (OWASP) listet allein eine Sammlung von 50 verschiedenen WVS auf [8]. Sie unterteilen sich in freie, Open Source und kommerzielle WVS und sind für unterschiedliche Plattformen erhältlich. Das Ziel dieser Arbeit ist es, aus dieser bunten Mischung diejenigen WVS herauszufiltern, für die eine nähere Betrachtung lohnend erscheint und diese im Hinblick auf folgende Fragestellungen zu evaluieren:

- 1. Wie viele Schwachstellen werden von den WVS gefunden?**
- 2. Wie unterscheiden sich die WVS in den Kategorien Bedienung, Reporting und Scan-Geschwindigkeit?**
- 3. Welcher WVS schneidet insgesamt am besten ab?**
- 4. Wie schneiden die Open Source WVS im Vergleich mit kommerziellen WVS ab?**

Für die Tests werden zunächst mehrere verwundbare Webanwendungen ausgesucht, die von den WVS gescannt werden. Von den WVS wird zu jedem Scan ein Bericht mit den gefundenen Schwachstellen generiert. Zusätzlich zu diesen Ergebnissen sollen subjektive Eindrücke wie Handhabung und Qualität des Reportings in die Bewertung mit einfließen. Die Evaluation soll mit Hilfe eines Punktesystems erfolgen und schließlich in einem Ranking resultieren, das die Tauglichkeit und Qualität der getesteten WVS anhand ihrer Platzierungen aufzeigt.

Die Arbeit gliedert sich wie folgt:

Das zweite Kapitel vermittelt die Grundlagen über Webanwendungen, Schwachstellen, Sicherheitsmaßnahmen wie Web Application Firewalls und Penetration Testing sowie die Arbeitsweise von WVS. Kapitel drei beinhaltet die Methodik, hier wird der Testaufbau einschließlich der Auswahlkriterien für die WVS und des Punktesystems für die Bewertung beschrieben. Zudem werden nicht berücksichtigte WVS genannt und die verwundbaren Webanwendungen vorgestellt, die für die Tests verwendet werden. Im vierten Kapitel folgt die Evaluation mitsamt den Ergebnissen, zum einen die Anzahl der gefundenen Schwachstellen per WVS, zum anderen eine Beschreibung der WVS einschließlich der Bewertung in den Kategorien Bedienung, Reporting und Scangeschwindigkeit. Im nachfolgenden fünften Kapitel werden die Ergebnisse der Evaluation im Hinblick auf die Forschungsfragen diskutiert, im letzten Kapitel wird schlussendlich die Studie nochmals kurz zusammengefasst und auf mögliche Ansätze für zukünftige Arbeiten eingegangen.

2 Grundlagen

Dieses Kapitel vermittelt Grundlagenwissen über Webanwendungen, Schwachstellen, Sicherheitsmaßnahmen wie WAFs und Penetration Testing sowie die Arbeitsweise von WVS.

2.1 Webanwendung

Zu Beginn sollte der Begriff “Webanwendung” geklärt werden. Eine Webanwendung muss nicht zwingend über das WWW erreichbar sein, auch in vielen Unternehmen kommen Webanwendungen zum Einsatz. Ob eine Anwendung als Webanwendung bezeichnet werden kann, hängt vom Einsatz von Webtechnologien ab. Daraus kann folgende Begriffsdefinition abgeleitet werden [9, S.1]:

“Eine Webanwendung ist eine Client-Server-Anwendung, die auf Webtechnologien (HTTP, HTML etc.) basiert.”

Eine Webanwendung wird über einen Browser aufgerufen, der den serverseitig bereitgestellten HTML-, Java-Script oder CSS-Code interpretiert und darstellt. Daneben kann auch über ein Skript oder von einer Kommandozeile aus auf Webanwendungen zugegriffen werden, man spricht hier von einem User Agent oder Client. Zur Kommunikation zwischen Browser (also Client) und Server wird das HTTP-Protokoll verwendet oder das darauf aufsetzende HTTPS-Protokoll. Serverseitig werden Webanwendungen auf Web- und Applikationsservern oder Laufzeitumgebungen ausgeführt, die dann wiederum auf Hintergrundsysteme wie Datenbanken zugreifen können. Daraus ergibt sich eine dreischichtige Architektur, auch 3-Tier-Architektur genannt (siehe Abb. 2.1).

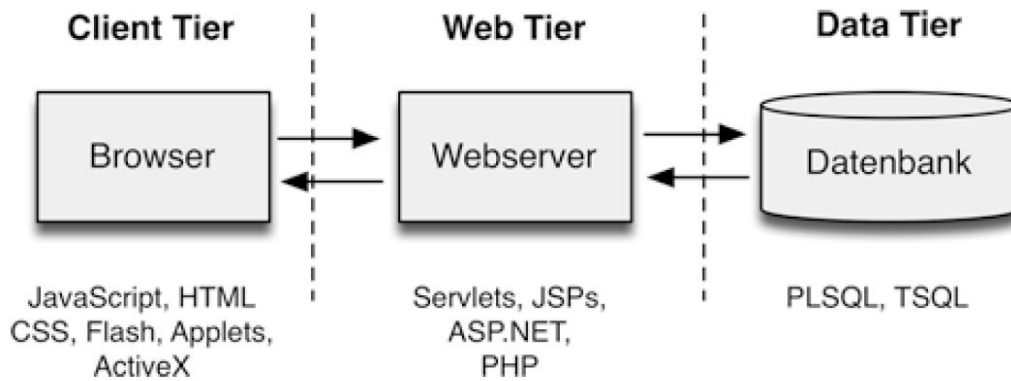


Abbildung 2.1: 3-Tier-Architektur einer Webanwendung [9, S.2]: Der Browser (Client) kommuniziert mit dem Webserver per HTTP(S), der wiederum auf die Datenbank zugreift.

Moderne Webanwendungen lassen sich jedoch - insbesondere im Enterprise-Umfeld - nicht als einzelne Anwendungen sehen, sondern als Zusammenschluss verschiedener eigenständiger Dienste wie REST- oder Microservices zu einer Plattform.

Im Zuge der Weiterentwicklung von Webanwendungen werden immer mehr Aspekte der Benutzerschnittstelle Client-seitig, vor allem über JavaScript-Code umgesetzt, der im Hintergrund serverseitige Webdienste aufruft. Diese Verlagerung von Anwendungslogik vom Server auf den Client resultieren in sogenannten Single Page Applications (SPAs), die nur noch aus einer einzigen HTML-Seite mit sehr viel JavaScript-Code bestehen, der im Hintergrund auf der Serverseite mit REST-Services kommuniziert und die Anzeige der Seiteninhalte steuert. Ein bekanntes Beispiel für solch eine SPA ist Google Mail. [9]

2.2 Schwachstellen

Das BSI definiert eine Schwachstelle wie folgt:

“Eine Schwachstelle (englisch “vulnerability”) ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.” [10, S.107]

Im Idealfall entdeckt ein Hersteller Schwachstellen selbst und kann sie beheben, bevor sie öffentlich bekannt werden. Sollte die Sicherheitslücke jedoch durch Dritte gefunden werden, kann ihr Lebenszyklus und die Gefährdung für die Nutzer unterschiedlich verlaufen. Der Verlauf hängt in erster Linie vom Entdecker, aber auch von der Reaktion der Hersteller ab [11]:

- Möchte der Entdecker die IT-Sicherheit verbessern, oder hat er kriminelle Absichten und benutzt die Schwachstelle für eigene Interessen?
- Inwieweit wird die Öffentlichkeit über die Schwachstelle informiert?
- Ist der Hersteller in der Lage, die Sicherheitslücke schnell zu beheben?

Um bekannte Schwachstellen herstellerübergreifend einheitlich benennen zu können, wurde der Industriestandard Common Vulnerabilities and Exposures (CVE) etabliert, der gewährleistet, dass Hersteller, Entdecker und weitere Beteiligte jeweils über dieselbe Schwachstelle diskutieren. Der CVE sammelt vorhandene Informationen über die Schwachstelle und bietet die Möglichkeit zu statistischen Auswertungen.

Wie in Abbildung 2.3 dargestellt, lässt sich der Lebenszyklus einer Schwachstelle, die durch Dritte entdeckt wurde, auf das folgende Schema zurückführen[11]:

1. Entdeckung der Schwachstelle durch einen Dritten.
2. Es gibt mehrere Möglichkeiten, wie der Hersteller von der Schwachstelle erfährt:
 - „Full Disclosure“: Alle Informationen über die Schwachstelle werden vom Entdecker öffentlich gemacht.
 - „Coordinated Disclosure“: Der Entdecker kontaktiert direkt den Hersteller und koordiniert mit ihm das weitere Vorgehen, hier werden zunächst keine Informationen an die Öffentlichkeit gegeben.
 - „Zero-Day-Exploit“: Niemand wird über die Schwachstelle informiert, stattdessen wird sie für Angriffe ausgenutzt. Öffentlichkeit und Hersteller erfahren erst nach erfolgreichen Angriffen von der Schwachstelle.
 - Indirekte Benachrichtigung an den Hersteller über einen sogenannten Schwachstellen-Broker.
3. Der Hersteller beginnt damit, die Sicherheitslücke zu schließen, indem er die Software nachbessert und einen Patch entwickelt.
4. Veröffentlichung eines „Advisorys“, einer Schwachstellenwarnung, die Informationen

über die Sicherheitslücke, eine Gefährdungsbewertung und vorläufige Gegenmaßnahmen beinhaltet. Die Warnung erscheint in der Regel zeitgleich mit dem Patch, bei hoher Gefährdung und wenn die Öffentlichkeit schon von der Schwachstelle erfahren hat, kann sie auch vor der Fertigstellung des Patches veröffentlicht werden.

5. Der Patch ist fertiggestellt und wird vom Hersteller mit einer entsprechenden Beschreibung (Bulletin) zur Verfügung gestellt. Mit der Veröffentlichung des Patches und dem Bulletin steigt die Gefahr für ungepatchte Systeme, da nun auch potenzielle Angreifer umfangreiche Informationen über die Schwachstelle erhalten.

6. Der Patch wird von den Benutzern der betroffenen Software installiert und die Sicherheitslücke dadurch geschlossen.

Der Ablauf kann von diesem Schema abweichen; wenn beispielsweise eine Schwachstelle vom Hersteller zunächst als nicht kritisch eingestuft und daher auf die Entwicklung eines Patches verzichtet wird, kann dies dazu führen, dass zu einem späteren Zeitpunkt schnell reagiert werden muss, wenn sich die Schwachstelle doch als ausnutzbar erweist. [11]

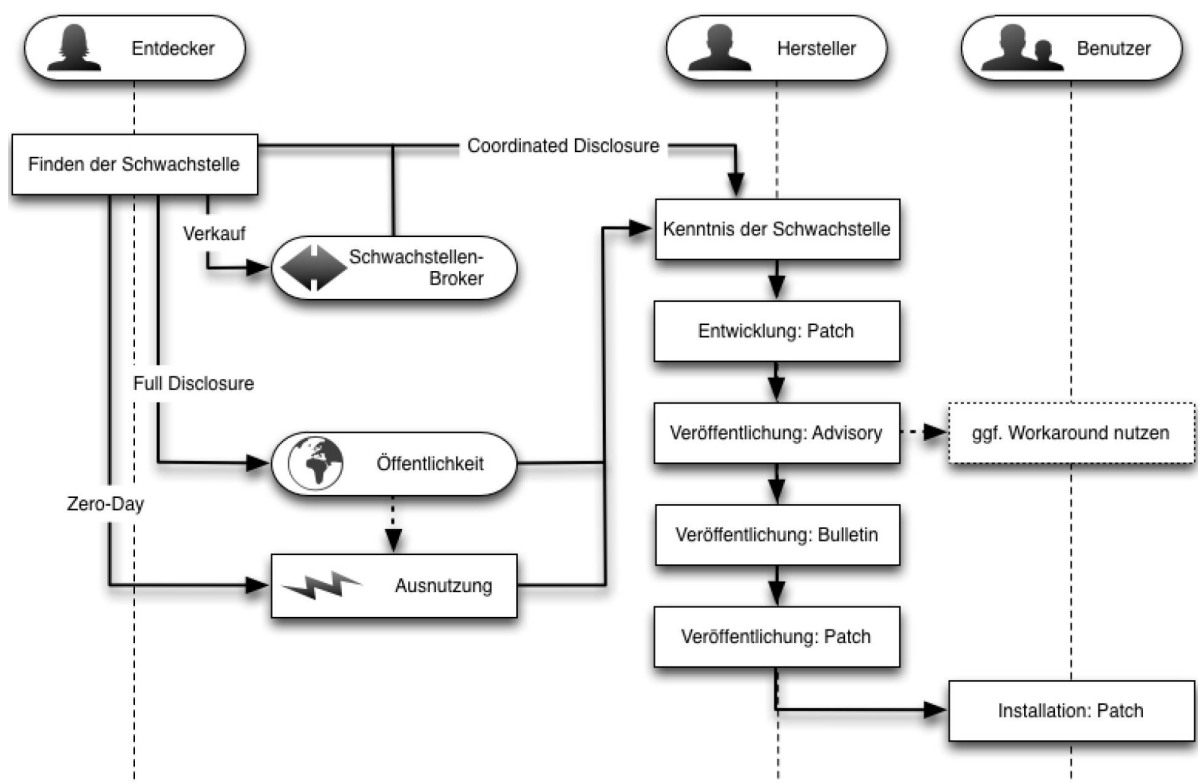


Abbildung 2.2: Lebenszyklus einer Schwachstelle [11, S.2]

2.3 Web Application Security

Die Webanwendungssicherheit ist ein Teilgebiet der IT-Sicherheit und befasst sich vor allem mit dem Schutz von Assets einer Webanwendung. Als Assets werden Bestandteile einer Webanwendung wie Daten, Systeme oder Funktionen bezeichnet, die Schutzbedarf im Hinblick auf die primären Schutzziele haben [4].

Diese primären Schutzziele lauten [4]:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Aus diesen primären Schutzzielen lassen sich auch sekundäre Schutzziele wie z.B. Authentizität oder Nicht-Abstreitbarkeit ableiten.

Das Thema Webanwendungssicherheit bezieht sich auf den gesamten Lebenszyklus einer Webanwendung und ist ein wichtiger Bestandteil der Qualitätssicherung. Neben der Bedrohungsabwehr und der Vorbeugung von Sicherheitslücken befasst sie sich auch mit deren Identifizierung und Behebung. [4]

2.3.1 Bedrohungen und Risiken

Die schwerwiegendsten Angriffe auf Webanwendungen sind sicherlich diejenigen, die sensible Daten verfügbar machen oder uneingeschränkten Zugriff auf die Systeme ermöglichen, auf denen die Anwendung ausgeführt wird. Hierzu gehören Angriffe per Cross Site Scripting (XSS) oder SQL-Injection. Aber auch Angriffe, die Systemausfälle verursachen (Denial of Service (DoS)-Attacken), stellen für viele Unternehmen ein sehr kritisches Ereignis dar.

Mehrere Organisationen haben es sich zur Aufgabe gemacht, Sicherheitsrisiken für Webanwendungen zu katalogisieren und zu klassifizieren. Das Web Application Security Consortium (WASC), ein Zusammenschluss von Experten, die an Sicherheitsstandards für Webanwendungen arbeiten, hat mit seiner “WASC Threat Classification v.2.0” einen umfassenden Katalog mit Bedrohungen herausgegeben [12].

OWASP veröffentlicht alle drei bis vier Jahre mit den “OWASP Top Ten” [13] eine Liste mit den 10 häufigsten Sicherheitsrisiken für Webanwendungen, die durch die große Akzeptanz in der Fachwelt als Sicherheitsrichtlinie angesehen werden kann.

2.3.2 Sicherheitsmaßnahmen

Das BSI definiert den Begriff wie folgt:

“Als Sicherheitsmaßnahmen werden alle Aktionen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und diesen entgegenzuwirken. Dies schließt sowohl organisatorische als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt.” [10, S.107-108]

Zu den Maßnahmen, die bereits während der Entwicklung ergriffen werden sollten, gehören umfangreiche Security Tests. Nach Inbetriebnahme der Webanwendung kann mit Hilfe von Penetration Tests nach Sicherheitslücken gesucht werden, zusätzlichen Schutz bieten Web Application Firewalls.

2.3.2.1 Security Tests

Bevor eine Webanwendung ausgeliefert wird, sollte sie mit Hilfe von Security Assessments auf Sicherheitsmängel getestet werden. Security Assessments stellen dabei die korrekte Umsetzung sowie die Effektivität der definierten Sicherheitsanforderungen und Spezifikationen sicher. Das bedeutet, die Anforderungen an die Sicherheit werden auf Angemessenheit und Wirksamkeit überprüft [4].

In der Regel werden Security Assessments in folgende Phasen eingeteilt [4]:

- Planung: In der initialen Planungsphase werden alle Informationen gesammelt, die notwendig sind, um das Assessment durchzuführen.
- Durchführung: In dieser Phase wird nach Schwachstellen gesucht, die anschließend bewertet werden.
- Auswertung: Die Auswertungsphase beinhaltet die Analyse der gefundenen Schwachstellen sowie die Bestimmung von Ursachen und Gegenmaßnahmen. Die Resultate werden in einem Bericht zusammengefasst und an die Entwickler weitergeleitet. Sobald die Schwachstellen behoben wurden, werden sie nochmals überprüft.

Für die Überprüfung gibt es mehrere unterschiedliche Testverfahren für verschiedene Aufgaben, die jeweils unterschiedliche Resultate liefern. So untersuchen Unit Tests zum Beispiel, ob eine Funktionalität korrekt und vollständig abgedeckt ist, Code Reviews überprüfen hingegen die fehlerfreie Implementierung [4].

Während der Implementierung können bereits folgende Testverfahren durchgeführt werden [4]:

- **Security Test Cases:** Test Cases sind Softwaretests, die überprüfen, ob vorher definierte Sicherheitsanforderungen an die Funktionalität der Webanwendung eingehalten werden. Dafür werden sogenannte erwartete Ergebnisse definiert, deren Einhaltung im Zuge der Tests überprüft wird. Dabei wird zwischen Positiv- und Negativtests unterschieden: ein Positivtest überprüft, wie sich die Webanwendung mit gültigen Eingaben und Rahmenbedingungen verhält, der Negativtest untersucht das Verhalten mit ungültigen Eingaben und Rahmenbedingungen.
- **Security Unit Tests:** Unit Tests überprüfen, ob die Softwareeinheiten (Units) einer Webanwendung fehlerfrei funktionieren. Dazu werden Klassen, Methoden und Funktionen mit unterschiedlichen Parametern aufgerufen und überprüft, ob die erwarteten Ergebnisse ausgegeben werden.
- **Design Review:** Bei Design Reviews wird die Architektur der Webanwendung auf konzeptionelle Fehler und Schwachstellen überprüft. Zudem sollen sie sicherstellen, dass Sicherheitsmechanismen und -anforderungen vollständig umgesetzt wurden.
- **Code Reviews:** Bei Code Reviews handelt es sich um manuelle Überprüfungen des Programmcodes. Wichtig ist hierbei, dass die prüfende Person den Code nicht selbst geschrieben hat, da dies leicht dazu führen kann, dass Fehler übersehen werden. Überprüft wird, ob Standards eingehalten und Anforderungen erfüllt werden, zudem können Designfehler und Verwundbarkeiten aufgedeckt werden.
- **Statische Code Scanner:** Diese Tools führen eine Statische Code Analyse (SCA) durch, um Schwachstellen zu finden. Da dieses Testverfahren vor der eigentlichen Ausführung der Software angewendet wird, müssen die Scanner Kenntnis von den verwendeten APIs haben, die normalerweise nicht im Quellcode vorliegen. Zudem müssen die Ergebnisse von qualifiziertem Personal verifiziert werden, da diese Tools oft eine große Menge an False-Positives produzieren.
- **Web Application Vulnerability Scanner:** siehe Abschnitt 2.4
- **Fuzz Testing:** Beim Fuzz Testing werden ungültige oder unerwartete Eingabewerte an die Webanwendung übergeben und überprüft, ob dabei ein Fehlverhalten auftritt. Dadurch können einfache Programmfehler entdeckt werden, die sonst leicht zu übersehen sind. [4]

2.3.2.2 Penetration Testing

Nach Fertigstellung der Webanwendung kommen Penetration Tests zum Einsatz. Sie können als legaler und autorisierter Versuch definiert werden, Computersysteme anzugreifen, mit dem Ziel, diese sicherer zu machen. Der Prozess umfasst die Suche nach Schwachstellen sowie die Demonstration von Beispielangriffen, um zu zeigen, dass die Bedrohungen real sind. Ein ordnungsgemäßer Penetration Test resultiert immer in spezifischen Empfehlungen für das Beheben der während des Tests aufgetretenen Probleme. Insgesamt wird dieses Verfahren dazu verwendet, Computer und Netzwerke gegen zukünftige Angriffe abzusichern. Die allgemeine Idee besteht darin, Sicherheitslücken mithilfe der gleichen Tools und Techniken zu finden, die auch ein Angreifer benutzt. Die Lücken können so geschlossen werden, bevor ein realer Hacker sie ausnutzt. [14]

Üblicherweise lassen sich Penetration Tests in mehrere Phasen unterteilen [4]:

- Informationsgewinnung
- Identifizierung der Angriffsfläche
- Identifizierung von System und Anwendungen
- Schwachstellenrecherche und Priorisierung der Schwachstellen nach Ausnutzbarkeit und Auswirkung
- Angreifen und Ausnutzen der Schwachstellen

Man unterscheidet beim Penetration Testing zwischen drei unterschiedlichen Ansätzen, dem Black-Box, Grey-Box und White-Box Testing:

Black-Box Testing Beim Black-Box Testing befindet sich der Tester in der Rolle eines typischen Hackers von außen, der kein Wissen über die innere Arbeitsweise der Anwendung hat, weder Architektur noch Quellcode sind bekannt. Der Angreifer muss mit manuellen Methoden sowie speziellen Tools des Penetration Testings vertraut sein, um Schwachstellen zu lokalisieren und auszunutzen. Für die dynamische Analyse des anzugreifenden Netzwerks benötigt er Scanning Tools, die in der vorliegenden Arbeit evaluiert werden.

Grey-Box Testing Während der Black-Box-Tester ein System aus der Sicht eines Außenseiters untersucht, hat ein Grey-Box Tester bereits Zugriff auf das System auf Benutzerebene, möglicherweise sogar mit erhöhten Berechtigungen eines Administrators. In

der Regel liegt eine Dokumentation über Design und Architektur des Netzwerks vor, die internen Komponenten sind bekannt. Dies hat den Vorteil, dass die Sicherheit des Netzwerks gezielter und effizienter beurteilt werden kann, der Tester kann sich sofort auf die Systeme konzentrieren, die am wichtigsten sind oder ein besonders hohes Risiko haben. Zudem kann durch das interne Benutzerkonto ein Angriff innerhalb des abgesicherten Systems mit umfassendem Zugriff auf das Netzwerk simuliert werden.

White-Box Testing Der White-Box Tester hat schließlich uneingeschränkten Zugriff auf ein System, er besitzt alle nötigen Berechtigungen und kennt Netzwerkarchitektur und Design. Überdies hat er Zugang zum Quellcode, was es ihm erlaubt, statische Code-Analysen durchzuführen. Durch das Auffinden sowohl interner als auch externer Schwachstellen ist das White-Box Testing maximal effektiv, aber auch sehr aufwandsintensiv, da der Tester sehr große Datenmengen untersuchen muss.

Penetration Tests sind nicht auf technische Systeme beschränkt. Angriffe mittels Social Engineering zielen zum Beispiel auf die personelle Infrastruktur, aber auch Angriffe auf die organisatorische Infrastruktur lassen sich realisieren[4].

Generell haben Penetration Tests folgende Ziele: [4]:

- Verbesserung der Sicherheit der IT-Systeme
- Erkennung von Sicherheitslücken
- Nachweis der Sicherheit von unabhängigen Dritten
- Verbesserung der Sicherheit von personeller und organisatorischer Infrastruktur

Penetration Tests zeigen die Sicherheitslücken zwischen Planung und Implementierung auf. Um die Lücken zu schließen, müssen geeignete Maßnahmen getroffen werden. Im letzten Schritt sollte überprüft werden, ob die getroffenen Maßnahmen tatsächlich das Risiko gesenkt oder beseitigt haben, da ansonsten die Gefahr eines falschen Sicherheitsgefühls entsteht. [4]

2.3.2.3 Web Application Firewalls

Zusätzlichen Schutz von Angriffen auf Webapplikationen bieten WAFs, die auf Anwendungsebene den Verkehr zwischen Clients und Webservern überprüfen. Sie sind in der Lage, HTTP-Traffic zu filtern und gegebenenfalls zu blockieren, um die Webanwendung zu schützen. Eine WAF überprüft dabei alle eingehenden Anfragen und die ausgehenden Antworten des Webserver. Erkennt sie dabei gefährliche Muster, verhindert sie die weitere Kommunikation mit dem Client.

Eine WAF kann zentralisiert hinter der Netzwerk Firewall und vor dem Webserver positioniert oder Host-basiert als Software-Lösung direkt auf dem Webserver installiert werden. Häufig wird der sogenannte Reverse-Proxy-Modus verwendet, bei dem der Proxy sich zwischen Webserver und Firewall befindet und Zugriffe im Namen des Clients durchführt. Im zweiten Schritt werden die Anfragen an den wirklichen Webserver analysiert und die Websessions bei Bedarf terminiert.

Zu den Angriffen, die eine WAF üblicherweise verhindern kann, zählen Cross-Site-Scripting, SQL-Injection, Angriffe per Pufferüberlauf oder auch Konfigurationsfehler. Der Schutz ist hier stets nur als zusätzlicher Schutzmechanismus zu verstehen, der keinesfalls die Notwendigkeit ersetzt, Webanwendungen zu entwickeln, die ausreichend sicher sind und getestet wurden. Bei der Durchführung von Tests sollte eine WAF stets deaktiviert sein, um die Testergebnisse nicht zu verfälschen. Um aus einer WAF den größtmöglichen Nutzen zu ziehen, sollte die Konfiguration möglichst durch Fachleute auf die jeweilige Webanwendung angepasst werden. [4, 15]

Bekannte Hersteller von WAFs sind Imperva, Akamai, F5, Fortinet, Citrix, Cloudflare und Barracuda.

2.4 Funktionsweise WVS

WVS sind automatisierte Werkzeuge, die Webanwendungen - in der Regel von außerhalb - nach Sicherheitslücken wie Cross-Site Scripting, SQL-Injection, Command Injection, Path Traversal und unsicheren Serverkonfigurationen absuchen. Diese Kategorie von Werkzeugen wird häufig auch als “Dynamic Application Security Testing (DAST) Tools” bezeichnet [8]. Im Gegensatz zum “Static Application Security Testing (SAST)”, bei dem der Quell-, Binär- oder Bytecode auf mögliche Implementierungs- und Konstruktionsfehler überprüft wird, testen DAST-Tools die laufende Webanwendung auf ihr Verhalten während des Betriebs. Es werden die gleichen Techniken angewendet, die auch ein realer Angreifer nutzen würde, um potenzielle Sicherheitslücken zu finden.

Um Webanwendungen zu analysieren, befindet sich der WVS auf einem Client-Computer, in der Regel werden bei der Analyse vier Phasen durchlaufen [16]:

- **Crawl/Scan:** Ähnlich einer Suchmaschine inspiziert der WVS die komplette Webanwendung, besucht dabei alle Links und füllt gegebenenfalls Formfelder mit Testwerten aus. So erlangt der WVS Kenntnis über Aufbau und Funktionsweise der Webanwendung und Inhalten von Formularseiten. Häufig wird die Webanwendung auch auf vorhandene Verzeichnisse oder Dateien durchsucht, die Informationen beinhalten. Die Scan-Phase kann durch die Verwendung von öffentlichen Suchmaschinen wie Google unterstützt werden, die gezielt nach Informationen über die anzugreifende Webanwendung sucht. Für die Automatisierung dieser Abfragen und das Erstellen von Suchmustern gibt es spezielle Tools.
- **Analyse:** Im zweiten Schritt analysiert der WVS die Webanwendung auf ihre Sicherheit und speichert die relevanten Erkenntnisse in einer Datenbank. Interessant sind hier zum Beispiel die Art des Webservers, welche Technologien und Tools verwendet werden (CGI, PHP, JavaScript, JSP usw.) oder Mechanismen zum Session-Tracking (Cookies).
- **Audit/Penetrationstest:** Die Erkenntnisse aus der Analysephase werden nun dazu verwendet, fehlerhafte und nicht zulässige Eingabemuster zu erzeugen, die dann an die Webanwendung geschickt werden. Diese Phase wird von einigen WVS in eine “schadlose” und “potenziell schadhafte” Prüfung unterteilt.
- **Reporting:** Am Schluss werden die Ergebnisse in Berichten zusammengefasst. Je nach WVS variiert hier der Umfang, teilweise werden nur kritische Sicherheitslücken genannt, teilweise gibt es detaillierte Beschreibungen von allen Schwachstellen mit Hinweisen zur Behebung der Probleme. Bei den meisten WVS hat sich ein System etabliert, bei dem die gefundenen Schwachstellen je nach Schweregrad in vier Kategorien eingeteilt werden [17]:

- High: Schwachstellen, die es Angreifern erlauben, die komplette Kontrolle über die Webanwendung einschließlich Server zu übernehmen. Angreifer können auf die Datenbank der Anwendung zugreifen, Konten ändern und vertrauliche Informationen stehlen. Schwachstellen, die beispielsweise XSS und SQL-Injection erlauben, haben einen hohen Schweregrad und sollten bei der Erkennung durch einen Scanner oberste Priorität haben.
- Medium: Sicherheitslücken, die Angreifern den Zugriff auf ein angemeldetes Benutzerkonto ermöglichen, um vertrauliche Inhalte anzuzeigen. Angreifer erhalten Zugriff auf Informationen, mit denen sie zusätzlich andere Schwachstellen ausnutzen können oder das System besser verstehen, damit sie ihre Angriffe verfeinern können. Open Redirection ist ein Beispiel für eine Schwachstelle mit mittlerem Schweregrad, durch die ein Angreifer einen Benutzer auf eine schädliche Website umleiten kann. Schwachstellen mit mittlerem Schweregrad sollten so schnell wie möglich behoben werden, wenn sie von einem Scanner erkannt werden.
- Low: Diese Schwachstellen haben nur minimalen Einfluss oder können von einem Angreifer nicht ausgenutzt werden. Cookies, die nicht als “Http Only” gekennzeichnet sind, sind ein Beispiel für eine Sicherheitsanfälligkeit mit niedrigem Schweregrad. Das Markieren von Cookies als Http Only macht das Cookie für clientseitige Skripts unlesbar und bietet somit eine zusätzliche Schutzschicht gegen XSS-Angriffe. Schwachstellen mit geringem Schweregrad sollten untersucht und korrigiert werden, wenn Zeit und Budget dies zulassen.
- Informational: Dies sind keine Schwachstellen, sondern lediglich Warnungen, die Informationen über die Webanwendung enthalten. Beispiele sind die erforderliche NTLM-Autorisierung oder die Ermittlung des Datenbanksystems. Für diese Informationsalarme ist keine Aktion erforderlich.

3 Methodik

In diesem Kapitel wird der Testaufbau beschrieben einschließlich der Auswahlkriterien für die WVS und des Punktesystems für die Bewertung. Zudem werden nicht berücksichtigte WVS genannt und die Webanwendungen vorgestellt, die für die Tests verwendet werden.

3.1 Testaufbau

Für die Tests wird der Ansatz des Black-Box Testings (siehe Abschnitt 2.3.2.2) verfolgt, der Testablauf ist für jeden WVS identisch. Nach dem Scannen der sieben verwundbaren Web-Applikationen wird jeweils ein entsprechender Bericht in Form einer HTML-Datei generiert, der die gefundenen Schwachstellen und je nach WVS auch die benötigte Zeit für den Scan auflistet. Bei den WVS, die die Scanzeit nicht im Report aufführen, wird manuell gemessen. Neben diesen evidenten Daten fließen subjektive Eindrücke wie Handhabung und Bedienbarkeit der Software und die Qualität der erstellten Berichte in die Evaluation mit ein.

Um dies messbar zu machen und um am Ende ein Ranking der getesteten WVS abbilden zu können, wird ein Bewertungssystem etabliert, das nachfolgend beschrieben wird.

Für die Bewertung wird eine Skala mit fünf Skalenwerten von 0 bis 4 Punkten herangezogen:

- 0 **ungenügend**
- 1 **unterdurchschnittlich**
- 2 **durchschnittlich**
- 3 **überdurchschnittlich**
- 4 **überragend**

Das Gesamtergebnis setzt sich aus den Bewertungen für die Bedienung, Qualität des Reportings, der Geschwindigkeit und dem Scanergebnis zusammen, wobei für die Kategorien unterschiedliche Gewichtungen festgelegt werden. Die Einteilung entspricht der subjektiven Einschätzung der Wichtigkeit der einzelnen Kategorien. Das Scanergebnis

wird als wichtigste Kategorie angesehen und erhält daher mit 50% die höchste Gewichtung. Die Gewichtung von Bedienung und Reporting wird mit jeweils 20% angesetzt und die Scangeschwindigkeit mit 10%. Für die Auswertung und das Erstellen des Rankings werden die Werte für das Scanergebnis mit 5 und die Werte für Bedienung und Reporting jeweils mit 2 multipliziert, die höchste zu erreichende Punktzahl ist somit 40.

Angesichts zahlreicher Abstürze der Software Acunetix unter Windows (siehe Abschnitt 4.2.2) wurde eine weitere Bewertungskategorie "Stabilität" in Betracht gezogen, aber im Hinblick auf die Ununterscheidbarkeit aller anderen stabil laufenden WVS wieder verworfen. Die Abstürze der Acunetix-Software werden schließlich durch einen Abzug bei der Gesamtpunktzahl berücksichtigt.

Für das Scanergebnis wird die reine Anzahl der gefundenen Schwachstellen zu Grunde gelegt. Für eine tiefergehende Evaluation ist eine manuelle Validierung aller Schwachstellen auf True- und False-Positives in Erwägung zu ziehen, was jedoch angesichts der Vielzahl an Funden (über 3000) den Rahmen dieser Ausarbeitung sprengen würde.

Für die Tests wird folgendes System verwendet:

- Intel Core i7-8700K CPU mit 32 GB RAM
- Microsoft Windows 10 pro, Version 1809 (64 bit)
- Als Virtuelle Maschinen innerhalb von VirtualBox: Kali Linux 18.4 und Parrot OS 4.5.1, jeweils ausgestattet mit 2 Kernen und 8 GB RAM.

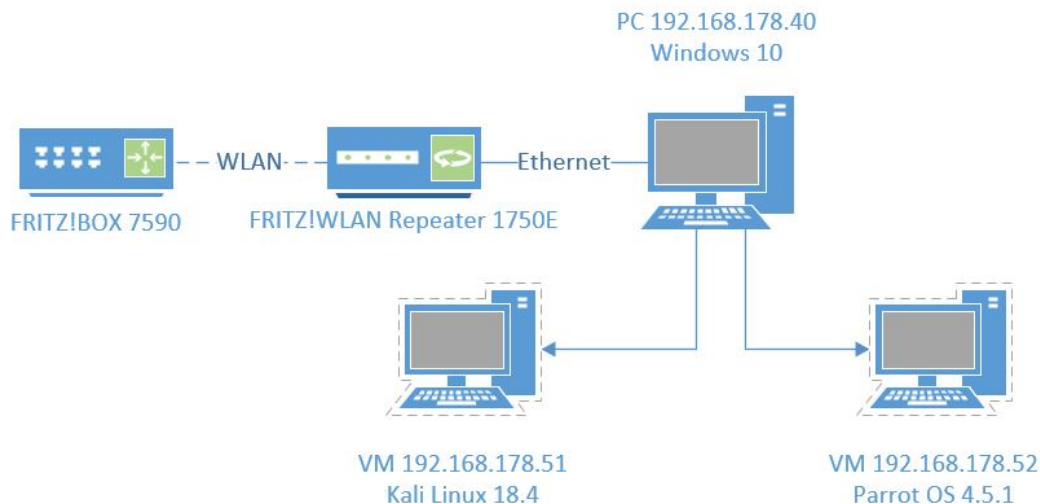


Abbildung 3.1: Testaufbau

3.2 Web Application Vulnerability Scanner

3.2.1 Auswahlkriterien

OWASP listet 50 verschiedene Tools zum Scannen von Webanwendungen auf [8]. Die Auswahl wurde auf WVS mit folgenden Eigenschaften eingegrenzt:

- Free und Open Source WVS.
- Kommerzielle WVS, die eine voll funktionsfähige Testversion anbieten.
- WVS, deren aktuelles Release nicht älter als 2 Jahre ist oder innerhalb der letzten 2 Jahre modifiziert wurde.
- WVS, die in der Lage sind, umfassende Scans auszuführen, um möglichst viele verschiedene Schwachstellenarten aufzuspüren.

Bei den bekanntesten Anbietern kommerzieller WVS wurde jeweils eine Testversion angefragt, um ein realistisches Abbild der aktuell meistgenutzten Tools zu erhalten und um die Ergebnisse der kostenlosen denen der kommerziellen Scanner gegenüberzustellen. Es handelt sich um folgende Firmen:

Acunetix, Beyond Security (WSSA), Beyond Trust (Retina), Netsparker, N-Stalker, Portswigger (BurpSuite Pro), Rapid 7 (Nexpose) und Tenable (Nessus).

Von den angefragten Firmen stellten Acunetix, Netsparker, N-Stalker, Portswigger und Tenable jeweils eine Testversion zur Verfügung.

3.2.2 Nicht ausgewählte WVS

Nachfolgend werden alle WVS aufgelistet, die als Anwärter für die Evaluation in Erwägung gezogen wurden, bei näherer Betrachtung jedoch nicht die erforderlichen Voraussetzungen erfüllten.

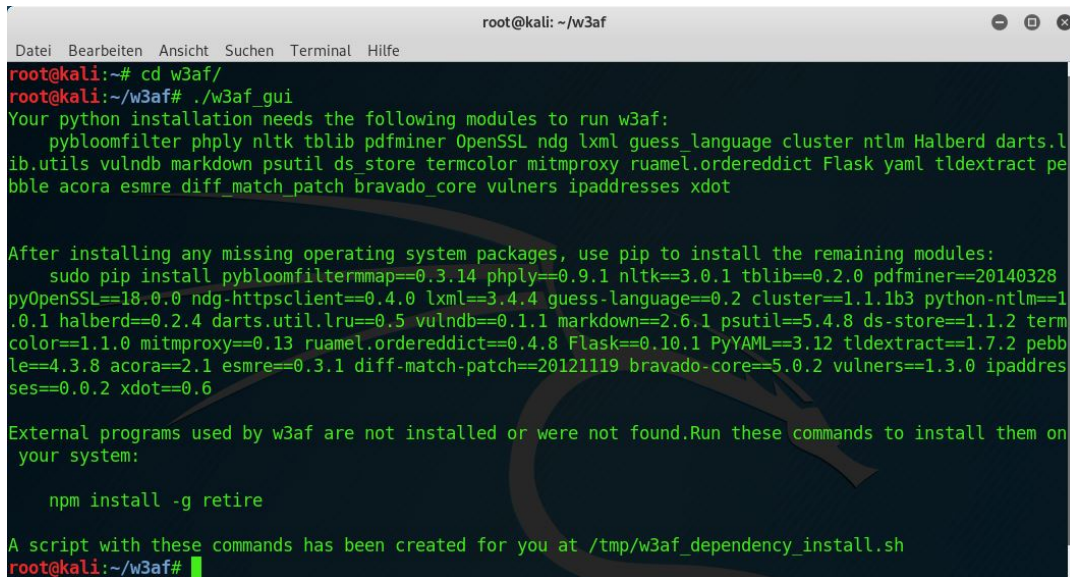
3.2.2.1 Kommerzielle WVS

- N-Stalker [18]: Die angebotene “7-Day Evaluation Licence” erlaubt nur das Scannen einer einzigen, vorher festgelegten URL und ist daher für den geplanten Testaufbau nicht geeignet.

3.2.2.2 Open Source WVS

- GoLismero [19]: GoLismero ist ein in Python geschriebenes Framework, das verschiedene Penetration Testing-Tools in sich vereint. Theoretisch sollten bei einem Angriff alle Tools angewendet und die jeweiligen Ergebnisse in einem einzigen Report gebündelt werden. In der Praxis hängte sich das Programm jedoch jedes Mal nach einer Weile auf, sowohl unter Kali-Linux und Parrot OS als auch unter Windows. Es werden zwar Teilergebnisse auf dem Bildschirm angezeigt, dies reicht aber nicht aus, um in die Evaluation aufgenommen zu werden.
- Grabber [20]: Das von Romain Gaucher entwickelte Programm ist zwar noch Bestandteil von Kali-Linux, ist aber schon über 12 Jahre alt (Latest Release 2006).
- Grendel-Scan [21]: Seit 2013 gibt es auf dem SourceForge-Repository von David Byrne keine Veränderung.
- Iron Wasp [22]: Die aktuelle Version des Windows-Programms von Lavakumar Kuppan ist ein Beta-Release aus dem Jahr 2015.
- Ratproxy [23]: Die Entwicklung wurde 2009 von Google eingestellt.
- Skipfish [24]: Ein weiteres Projekt von Google, das 2012 eingestellt wurde.
- SQLmap [25]: SQLmap ist ein beliebtes Tool zum Auffinden von SQL-Injection Schwachstellen, ist aber darauf beschränkt.
- Vega [26]: Das aktuelle Release ist aus dem Jahr 2014. Seit diesem Jahr wird in regelmäßigen Abständen angekündigt, ein Feature zum Exportieren der Ergebnisse hinzuzufügen, aber die Firma Subgraph scheint das Projekt nicht weiter zu verfolgen.
- Watobo [27]: Die letzte Änderung des OpenSource Scanners stammt aus dem Jahr 2015.
- WebScarab [28]: Der Vorgänger von OWASPs Zed Attack Proxy (ZAP) ist veraltet (Latest Release 2011). OWASP empfiehlt, auf ZAP umzusteigen.
- Wfuzz [29]: Der in Python geschriebene Scanner verwendet die Bibliothek Pycurl für HTTP-Requests, diese unterstützt keine SSL/TLS Verschlüsselung.

- W3af [30]: W3af wird zwar noch sporadisch mit Bibliotheks-Aktualisierungen gepflegt, das aktuelle Release ist jedoch aus dem Jahr 2014 und es ist weder auf Kali-Linux noch auf Parrot OS gelungen, alle für den Programmstart benötigten Dependencies zu installieren (siehe Abb. 3.2). Das bei der Installation generierte Script versucht, teils veraltete Module zu installieren, manuelles Nachinstallieren der aktuellen Versionen brachte keinen Erfolg.

A screenshot of a terminal window titled 'root@kali: ~/w3af'. The terminal shows the command 'cd w3af/' and then './w3af_gui'. The output lists various Python modules needed for W3af to run, such as pybloomfilter, phply, nltk, tblib, pdfminer, OpenSSL, ndg, lxml, guess, language, cluster, ntlm, Halberd, darts, lib, utils, vulndb, markdown, psutil, ds_store, termcolor, mitmproxy, ruamel, ordereddict, Flask, yaml, tldextract, pebble, acora, esmre, diff_match_patch, bravado_core, vulners, ipaddresses, and xdot. It then provides a long command to install these modules using pip. Below that, it mentions external programs like 'retire' and provides a command to install it with npm. Finally, it states that a script has been created at '/tmp/w3af_dependency_install.sh'.

```
root@kali:~/w3af
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
root@kali:~# cd w3af/
root@kali:~/w3af# ./w3af_gui
Your python installation needs the following modules to run w3af:
    pybloomfilter phply nltk tblib pdfminer OpenSSL ndg lxml guess language cluster ntlm Halberd darts.lib
    ib.utils vulndb markdown psutil ds_store termcolor mitmproxy ruamel.orderdict Flask yaml tldextract pe
    bble acora esmre diff_match_patch bravado_core vulners ipaddresses xdot

After installing any missing operating system packages, use pip to install the remaining modules:
    sudo pip install pybloomfiltermmmap==0.3.14 phply==0.9.1 nltk==3.0.1 tblib==0.2.0 pdfminer==20140328
    pyOpenSSL==18.0.0 ndg-httpsclient==0.4.0 lxml==3.4.4 guess-language==0.2 cluster==1.1.1b3 python-ntlm==1
    .0.1 halberd==0.2.4 darts.util.lru==0.5 vulndb==0.1.1 markdown==2.6.1 psutil==5.4.8 ds-store==1.1.2 term
    color==1.1.0 mitmproxy==0.13 ruamel.orderdict==0.4.8 Flask==0.10.1 PyYAML==3.12 tldextract==1.7.2 pebb
    le==4.3.8 acora==2.1 esmre==0.3.1 diff-match-patch==20121119 bravado-core==5.0.2 vulners==1.3.0 ipadres
    ses==0.0.2 xdot==0.6

External programs used by w3af are not installed or were not found.Run these commands to install them on
your system:

    npm install -g retire

A script with these commands has been created for you at /tmp/w3af_dependency_install.sh
root@kali:~/w3af#
```

Abbildung 3.2: W3af versucht, veraltete Module zu installieren

- Wikto [31]: Wikto ist eine Windows-Portierung von Nikto und bedarf daher keiner eigenen Evaluation.
- Xenotix [32]: Xenotix wurde von OWASP für das Auffinden von XSS Schwachstellen entwickelt und ist darauf beschränkt.

3.2.3 Ausgewählte WVS

Aus der Vielzahl der ursprünglich in Betracht kommenden WVS haben sich am Ende neun herauskristallisiert, fünf mit einer Open Source-Lizenz (siehe Tab. 3.1) und vier kommerzielle Produkte (siehe Tab. 3.2). Im Abschnitt 4.3 werden sie im Zuge der Evaluation näher beschrieben.

3.2.3.1 Open Source WVS

WVS	Entwickler	Version	Verwendete Plattform
Arachni	Tasos Laskos	0.5.12 (WebUI)	Windows
Nikto	cirt.net	2.1.6	Kali
OpenVAS	Greenbone	7.0.3	Parrot
Wapiti	devloop	3.0.1	Kali
ZAP	OWASP	2.7.0	Parrot

Tabelle 3.1: Ausgewählte Free und Open Source WVS

3.2.3.2 Kommerzielle WVS

WVS	Anbieter	Version	Verwendete Plattform
Acunetix	Acunetix	12.0.190206130	Windows/Kali
Burp Suite Pro	Portswigger	2.0.15	Windows
Nessus	Tenable	8.2.2	Windows
Netsparker	Netsparker	5.2.0.22027	Windows

Tabelle 3.2: Ausgewählte kommerzielle WVS

3.3 Verwundbare Webanwendungen

Bei der Auswahl der Webanwendungen musste darauf geachtet werden, dass sie für WVS geeignet sind. Auf ursprünglich in die Auswahl aufgenommene Applikationen wie WebGoat, JuiceShop (beide von OWASP) oder Damn Vulnerable Web Application (Bestandteil von Metasploitable) wurde am Ende verzichtet, da hier beim Scannen keine hinreichenden Ergebnisse hervorgebracht wurden. Diese Anwendungen sind zwar sehr gut dokumentiert, aber hauptsächlich für das Erlernen von manuellen Angriffen entwickelt worden. Es wurde bei der Auswahl auf das OWASP Vulnerable Web Applications Directory Project zurückgegriffen, das eine Reihe von verwundbaren Web-Applikationen auflistet [33]. Die Auswahl deckt mehrere Technologien wie PHP, ASP.Net oder HTML5 ab.

Nachfolgend werden die für die Auswertung genutzten Webanwendungen kurz vorgestellt.

- **WA1: Altoro Mutual**
Altoro Mutual ist eine in C# .NET geschriebene Online-Banking Webanwendung, die von IBM entwickelt wurde, um WVS zu testen [34].
- **WA2: Webscantest**
Diese Webanwendung ist in PHP geschrieben und wurde von NTOSpider entwickelt, um WVS zu testen. Die Schwachstellen sind direkt auf der Seite dokumentiert [35].
- **WA3: Zero Bank**
Eine weitere Online-Banking Webanwendung, entwickelt von Hewlett-Packard/Micro Focus [36].
- **WA4: Bitcoin Web Site**
Diese von Netsparker entwickelte Applikation ist in ASP.NET geschrieben und simuliert eine Online-Seite für Bitcoin-Transaktionen [37].
- **WA5: Acuart**
Eine Test-Seite von Acunetix, der einen Online-Shop für Kunstwerke simuliert, geschrieben in PHP [38].
- **WA6: Crack Me Bank**
Eine in PHP geschriebene Online-Banking Seite, entwickelt von Trustwave [39].
- **WA7: Security Tweets**
Security Tweets ist eine von Twitter inspirierte Social Networks Applikation, die von Acunetix entwickelt wurde und HTML5 verwendet [40].

4 Evaluation

In diesem Kapitel wird die Evaluation samt ihren Ergebnissen dargestellt, die getesteten WVS werden beschrieben und in den einzelnen Kategorien bewertet.

4.1 Scanzeiten

In den beiden folgenden Tabellen sind die Zeiten aufgeführt, die die WVS benötigten, um die jeweiligen Webanwendungen zu scannen.

	Arachni	Nikto	OpenVAS	Wapiti	ZAP
Altoro Mutual	41	96	38	88	615
Webscantest	86	80	90	82	821
Zero Bank	42	29	85	31	786
Aspnet Testsparker	28	20	29	14	579
Acuart	39	9	43	23	660
Crack Me Bank	38	32	45	28	704
Security Tweets	28	19	33	27	523
Total	302	285	363	293	4688

Tabelle 4.1: Scanzeiten der Open Source WVS in Minuten

	Acunetix	Burp Suite Pro	Nessus	Netsparker
Altoro Mutual	15	56	44	46
Webscantest	60	102	82	241
Zero Bank	26	71	68	47
Aspnet Testsparker	11	30	27	52
Acuart	6	45	61	37
Crack Me Bank	28	39	31	71
Security Tweets	8	41	51	20
Total	154	384	364	514

Tabelle 4.2: Scanzeiten der kommerziellen WVS in Minuten

4.2 Gefundene Schwachstellen per Webanwendung

Die Buchstaben H, M, L und I stehen für die Kategorien High, Medium, Low und Informationale (siehe Abschnitt 2.4). Aus Gründen der Vergleichbarkeit wurden die Werte aus der zusätzlichen Kategorie "Critical" bei Nessus und Netsparker mit in die Kategorie High übernommen. WA1 - WA 7 stehen für die verwundbare Web-Applikationen (siehe Abschnitt 3.3).

	Arachni				Nikto	OpenVAS				Wapiti	ZAP			
	H	M	L	I		H	M	L	I		H	M	L	I
WA1	9	4	2	5	12	0	2	0	24	10	1	2	5	0
WA2	4	10	5	29	18	0	8	0	41	12	1	4	11	0
WA3	4	6	4	4	18	6	51	2	34	2	0	1	2	0
WA4	22	6	8	27	15	0	4	0	24	32	3	4	6	0
WA5	56	6	10	24	18	2	31	1	77	31	4	1	2	0
WA6	29	10	4	10	9	0	11	1	29	6	4	3	3	0
WA7	10	2	3	6	7	1	31	1	77	0	0	1	5	0
Subt.	134	44	36	105	97	9	138	5	306	93	13	16	34	0
Total	319				97	458				93	63			

Tabelle 4.3: Gefundene Schwachstellen der Open Source WVS

	Acunetix				BurpSuite Pro				Nessus				Netsparker			
	H	M	L	I	H	M	L	I	H	M	L	I	H	M	L	I
WA1	4	10	2	34	10	0	7	18	0	3	2	21	4	6	10	15
WA2	25	41	6	14	5	2	4	160	1	7	1	25	37	18	24	20
WA3	19	23	20	24	0	0	1	13	14	31	1	23	7	6	16	14
WA4	73	26	6	7	17	1	4	119	1	6	1	20	21	8	16	28
WA5	39	34	9	19	28	0	4	49	21	18	1	21	24	18	12	12
WA6	6	14	27	5	11	0	1	74	0	5	1	22	14	4	11	13
WA7	14	4	9	3	8	2	2	11	0	1	2	16	8	2	10	11
Subt.	180	152	79	106	79	5	23	444	37	71	9	148	115	62	99	113
Total	517				551				265				389			

Tabelle 4.4: Gefundene Schwachstellen der kommerziellen WVS

4.3 Bedienung, Reporting und Geschwindigkeit

Nachfolgend werden die einzelnen WVS in den Kategorien Bedienung, Reporting und Geschwindigkeit beurteilt. Die Screenshots der Benutzeroberflächen wurden während des Testens selbst erstellt. Im Anhang A befindet sich zudem jeweils ein exemplarischer Screenshot eines generierten Berichtes von jedem WVS, die vollständigen Berichte aller Scans sind auf der beiliegenden CD-ROM zu finden.

4.3.1 Open Source

- **Nikto** [41]:
Nikto ist ein gut dokumentiertes Terminal-Programm, nach kurzer Einarbeitung hat ein ungeübter User die benötigten Befehle und Optionen gefunden, um einen Scan zu starten. Der generierte Report (siehe Abb. A.7) listet alle gefundenen Schwachstellen auf, unterscheidet diese jedoch im Gegensatz zu den meisten anderen WVS nicht zwischen High, Medium, Low und Informational. Die Scan-Geschwindigkeit ist überdurchschnittlich.

Bewertung: Reporting 1, Bedienung 2, Geschwindigkeit 3

- **Wapiti** [42]:
In der Handhabung und im Reporting (siehe Abb. A.8) ähnelt Wapiti dem anderen reinen Terminal-Programm Nikto. Die auswählbaren Optionen sind ähnlich, und die gefundenen Schwachstellen werden auch hier nicht in Kategorien eingeteilt. Die Dokumentation fällt etwas spartanischer aus, ist aber ausreichend, um sich schnell zurechtzufinden. Wapiti scannt fast so schnell wie Nikto und reiht sich hier auf dem dritten Platz ein.

Bewertung: Reporting 1, Bedienung 2, Geschwindigkeit 3

- **Arachni** [43]:

Arachni gibt es als reine Terminal-Anwendung oder als Ruby on Rails Framework mit Web-Interface. Die Web-Oberfläche ist übersichtlich und verständlich aufgebaut (siehe Abb. 4.1), der User findet sich schnell zurecht und kann sofort mit dem Scannen einer Seite beginnen, die Scangeschwindigkeit liegt über dem Durchschnitt. Als Hilfestellung gibt es ein umfangreiches Wiki mit Erklärungen und Screenshots. Der Report (siehe Abb. A.5) ist sehr umfangreich, verschiedene Balken- und Kuchendiagramme geben Statistiken über Art und Schweregrad der Funde wieder, zudem gibt es Verlinkungen zu den OWASP Top 10 und detaillierte Ausführungen über die Schwachstellen. Arachni unterscheidet bei den Funden außerdem zwischen gesicherten (“Trusted”) und noch zu überprüfenden Ergebnissen (“Untrusted”).

Bewertung: Reporting 4, Bedienung 3, Geschwindigkeit 3

Arachni v1.5.1 - WebUI v0.5.12 Scans Profiles Dispatchers Users Administrator

http://testhtml5.vulnweb.com/

Currently auditing:
• http://testhtml5.vulnweb.com/like?id=696a3680438a7af53a0a54d3d26469bf

Pages discovered	20	Requests performed	10024	Requests per second	33.44	Request concurrency	20
Running for	00:04:58	Responses received	10013	Timed out requests	0	Response times	0.525 s

Issues [15]

Issues may be missing some context while the scan is running.
You better wait until the scan is over to review them as the meta-analysis phase will flag probable false-positives and other untrusted issues accordingly.

All [15] Fixed [0] Verified [0] Pending verification [0] False positives [0] Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY	URL	Input	Elem
High 7	Cross-Site Scripting (XSS) 4		
Medium 2			
Low 3			
Informational 3			
Cross-Site Scripting (XSS) 4			
Unvalidated DOM redirect 1			
DOM based Cross-Site Scripting (XSS) in script c 1			

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.

If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).

Arachni has discovered that it is possible to insert script content directly into HTML element content.

(CWE)

Abbildung 4.1: Arachni WebUI 0.5.12

- **OpenVAS** [44]:

OpenVAS ist aus der Software Nessus hervorgegangen, als diese im Jahr 2005 von Open Soucre zu einer kommerziellen Lizenz wechselte, und wird seitdem auf Basis der letzten freien Nessus-Version 2.2 von Greenbone Networks weiterentwickelt. Der Scanner ist eingebettet in den Greenbone Security Assistant, der über ein Web-Interface bedient wird (siehe Abb. 4.2). Die Oberfläche ist nicht selbsterklärend. Es bedarf etwas an Recherche, bis sich dem User der logische Aufbau des Programms erschließt. Hier ist das “Tech Doc-Portal” von Greenbone sehr hilfreich. Zuerst muss unter Configuration/Targets ein Ziel definiert werden, dann kann der User für dieses Ziel unter dem Punkt “Scans” einen Task erstellen und diesen entweder sofort oder per Schedule starten. Die umständliche Handhabung hat jedoch den Vorteil, dass sich leicht mehrere Tasks automatisieren lassen. Der Bericht (siehe Abb. A.6) präsentiert sich etwas sparsam, die gefundenen Schwachstellen der Kategorie “Informational” werden nicht aufgelistet. Die Scangeschwindigkeit ist durchschnittlich.

Bewertung: Reporting 2, Bedienung 1, Geschwindigkeit 2

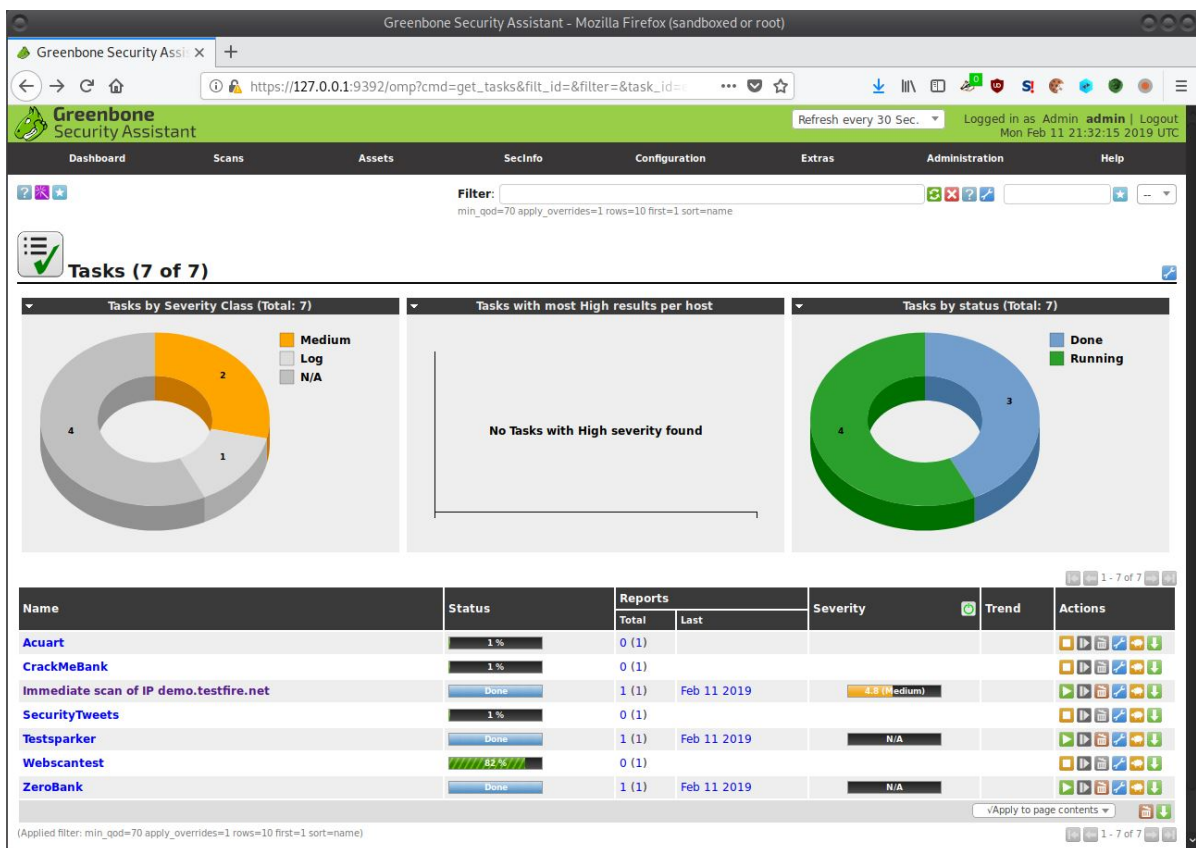


Abbildung 4.2: OpenVAS im Greenbone Security Assistant

- **ZAP** [45]:

Der von OWASP entwickelte Scanner hat eine übersichtliche Benutzeroberfläche (siehe Abb. 4.3) und lässt sich intuitiv bedienen. Auf der Startseite lässt sich direkt die anzugreifende URL eingeben und ohne weitere Konfiguration angreifen. Es gibt umfangreiche Hilfestellung in Form eines Handbuchs und einem Online-Wiki, zudem gibt es mit der OWASP ZAP User Group ein gut frequentiertes Benutzerforum, auf dem ein reger Austausch zwischen den Benutzern stattfindet. Auffällig sind die langen Scan-Zeiten von mehreren Stunden, die sich jedoch nicht in einer höheren Anzahl an gefundenen Schwachstellen widerspiegeln. Die wenigen Funde werden im Report ausführlich beschrieben einschließlich umfangreicher Empfehlungen zur Behebung (siehe Abb. A.9).

Bewertung: Reporting 3, Bedienung 3, Geschwindigkeit 0

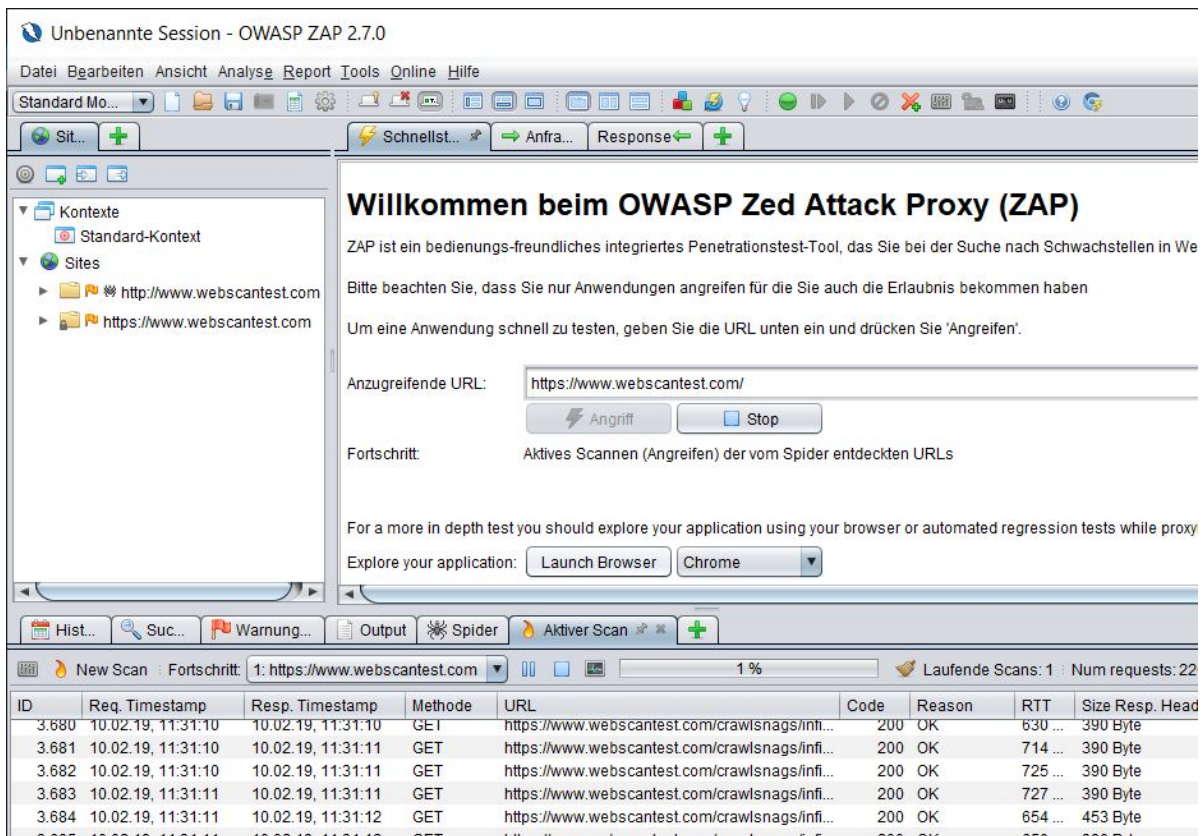


Abbildung 4.3: Grafische Benutzeroberfläche von ZAP

4.3.2 Kommerziell

- **Netsparker** [46]:

Netsparker stellte nach Rücksprache eine 14-tägige Testversion zur Verfügung, die auf acht zu scannende Web-Applikationen begrenzt ist. Die grafische Benutzeroberfläche ist etwas unruhig und überladen (siehe Abb. 4.4), der User kann aber direkt über den Button “New” eine Web-Seite scannen. Die Scangeschwindigkeit ist im unteren Mittelfeld angesiedelt. Der Report ist äußerst umfangreich, aber etwas unübersichtlich (siehe Abb. A.4). Netsparker hat neben High, Medium, Low und Informationale eine fünfte Kategorie “Critical” eingeführt, die auf besonders kritische Schwachstellen hinweist. Wie bei Arachni und BurpSuite werden gesicherte Ergebnisse gesondert gekennzeichnet, hier als “Confirmed”.

Bewertung: Reporting 3, Bedienung 2, Geschwindigkeit 1

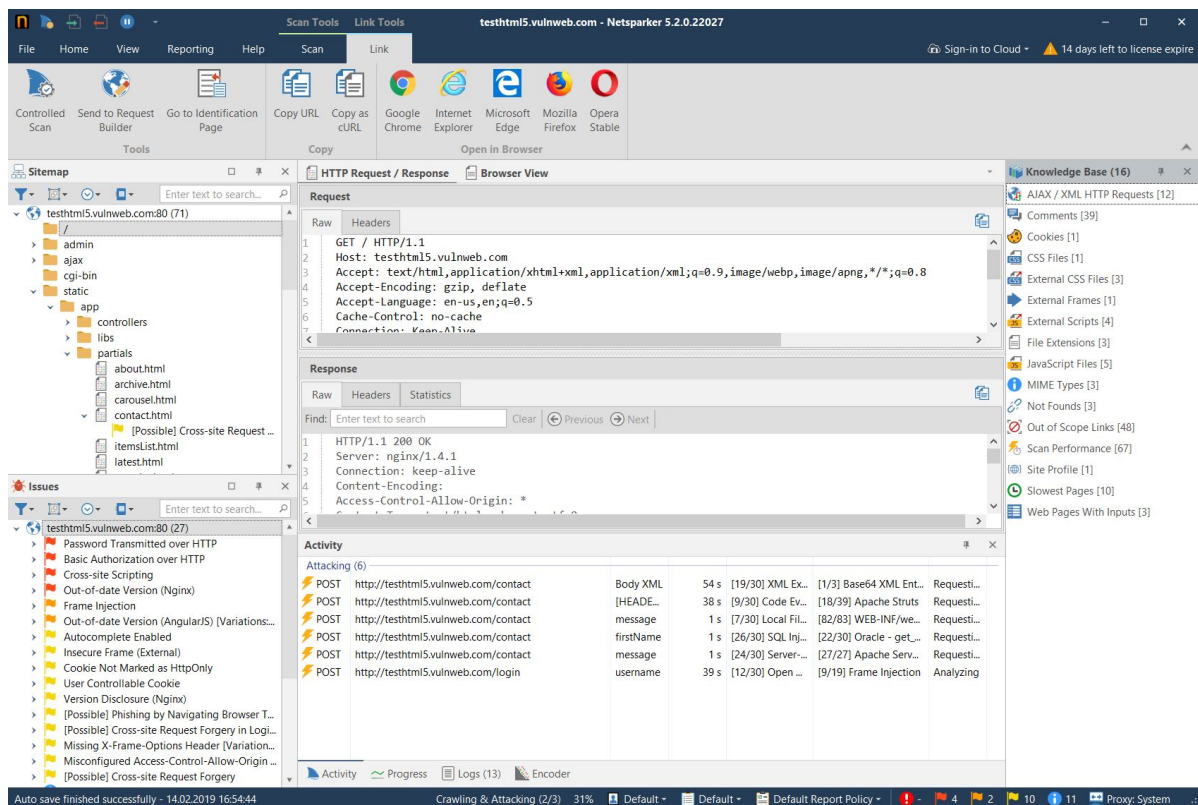


Abbildung 4.4: Grafische Benutzeroberfläche von Netsparker

- **Acunetix** [47]:

Acunetix stellte eine 14-tägige Vollversion zur Verfügung. Die graphische Oberfläche ist sehr übersichtlich (siehe Abb. 4.5) und lässt sich intuitiv bedienen. Online gibt es ein Support-Portal mit ausführlicher Dokumentation und Hilfestellung. Auffällig ist die im Vergleich zu allen anderen WVS ungewöhnlich hohe Scan-Geschwindigkeit, die sich im Minutenbereich einordnet. Unter Windows brachte Acunetix das System mehrmals zum Absturz (BSoD¹), so dass auf die Linux-Version ausgewichen wurde. Hier lief das Programm stabil und scannte von den kommerziellen WVS am schnellsten, von allen WVS muss sich Acunetix hier nur den Terminalprogrammen Wapiti und Nikto geschlagen geben. Der Report (siehe Abb. A.1) listet zu jeder gefundenen Schwachstelle sehr detailliert die vollständigen GET- und POST-Requests sowie teilweise seitenlange Code-Passagen auf. Die Empfehlungen zur Behebung der Funde könnten hingegen ausführlicher sein. Aufgrund der Abstürze wurden bei der Gesamtpunktzahl 3 Punkte abgezogen.

Bewertung: Reporting 3, Bedienung 3, Geschwindigkeit 4

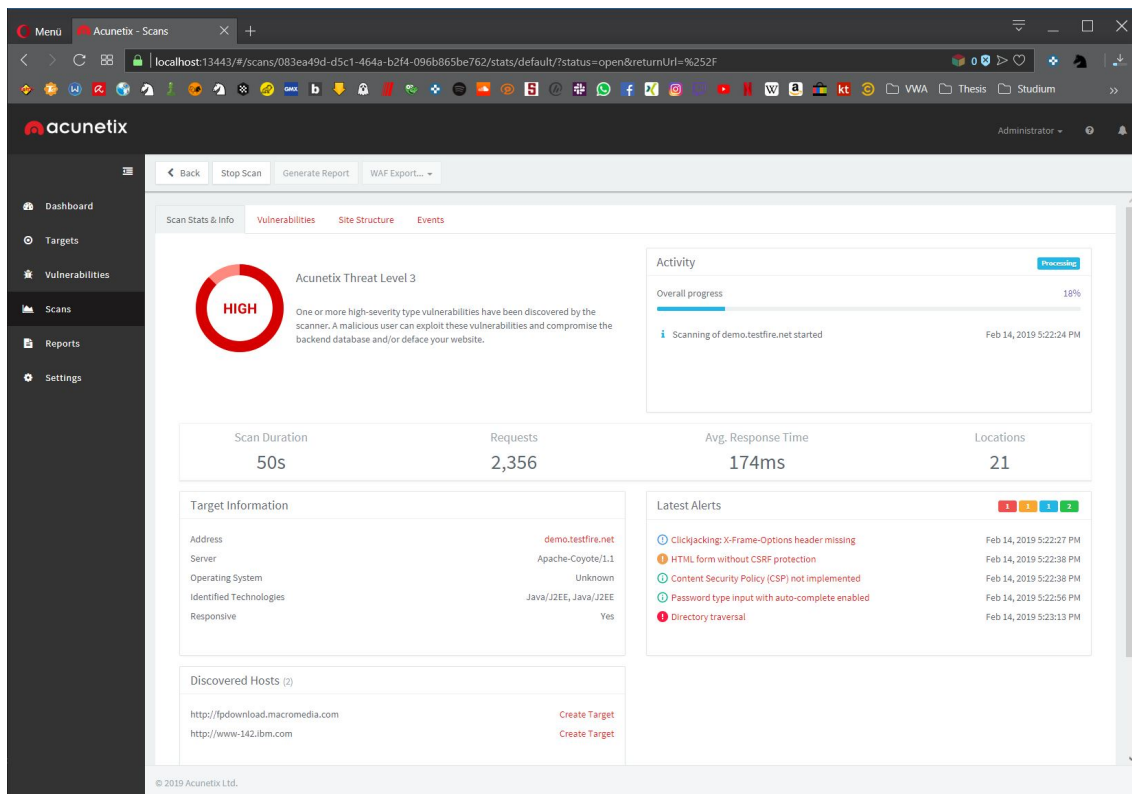


Abbildung 4.5: Weboberfläche von Acunetix

¹BSoD: Der “Blue Screen of Death” erscheint nach einem kritischen Systemfehler unter Microsoft Windows. Das System wird angehalten und die Benutzeroberfläche des Betriebssystems vollständig durch einen blauen Bildschirm ersetzt. Das System startet schließlich nach Sammlung aller Fehlerinformationen neu.

- **Nessus** [48]:

Die Firma Tenable bietet zwei Testversionen an: Nessus Home für das Testen des heimischen Netzwerks, gültig für ein Jahr, sowie eine unbeschränkte Version von Nessus Pro, gültig für sieben Tage. Nessus präsentiert sich auf einer übersichtlich gestalteten Web-Schnittstelle (siehe Abb. 4.6) und ist selbsterklärend zu bedienen. Einen Hilfe-Button sucht man vergeblich, die umfangreiche Dokumentation mit Anleitungen findet man online durch Recherchieren. Die Scangeschwindigkeit ist durchschnittlich, der Report übersichtlich, aber eher spartanisch (siehe Abb. A.3). Nur durch Anklicken der Funde gibt es online Beschreibungen und Lösungsvorschläge. Wie bei Netsparker gibt es auch bei Nessus neben High, Medium, Low und Informationale die zusätzliche Kategorie “Critical”.

Bewertung: Reporting 2, Bedienung 3, Geschwindigkeit 2

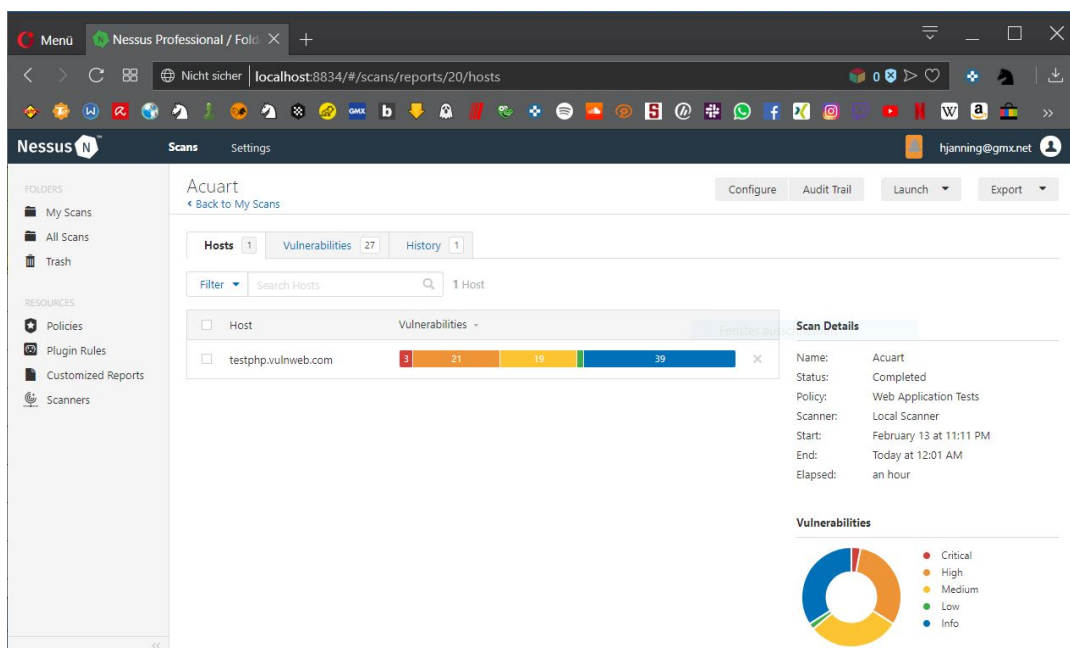


Abbildung 4.6: Grafische Benutzeroberfläche von Nessus

- **BurpSuite Pro** [49]:

Die Firma Portswigger stellte auf Anfrage eine 30-tägige unbeschränkte Testversion zur Verfügung. BurpSuite Pro enthält eine umfangreiche Dokumentation mit zahlreichen Hilfestellungen für verschiedene Anwendungsszenarien. Das Dashboard ist sehr übersichtlich und intuitiv zu bedienen (siehe Abb. 4.7). Mit Hilfe des Buttons “New Scan” lässt sich direkt ohne größeren Konfigurationsaufwand eine Website erfolgreich und in durchschnittlicher Geschwindigkeit scannen. Der von BurpSuite generierte Report ist von allen getesteten WVS der umfangreichste und ist trotzdem sehr übersichtlich (siehe Abb. A.2).

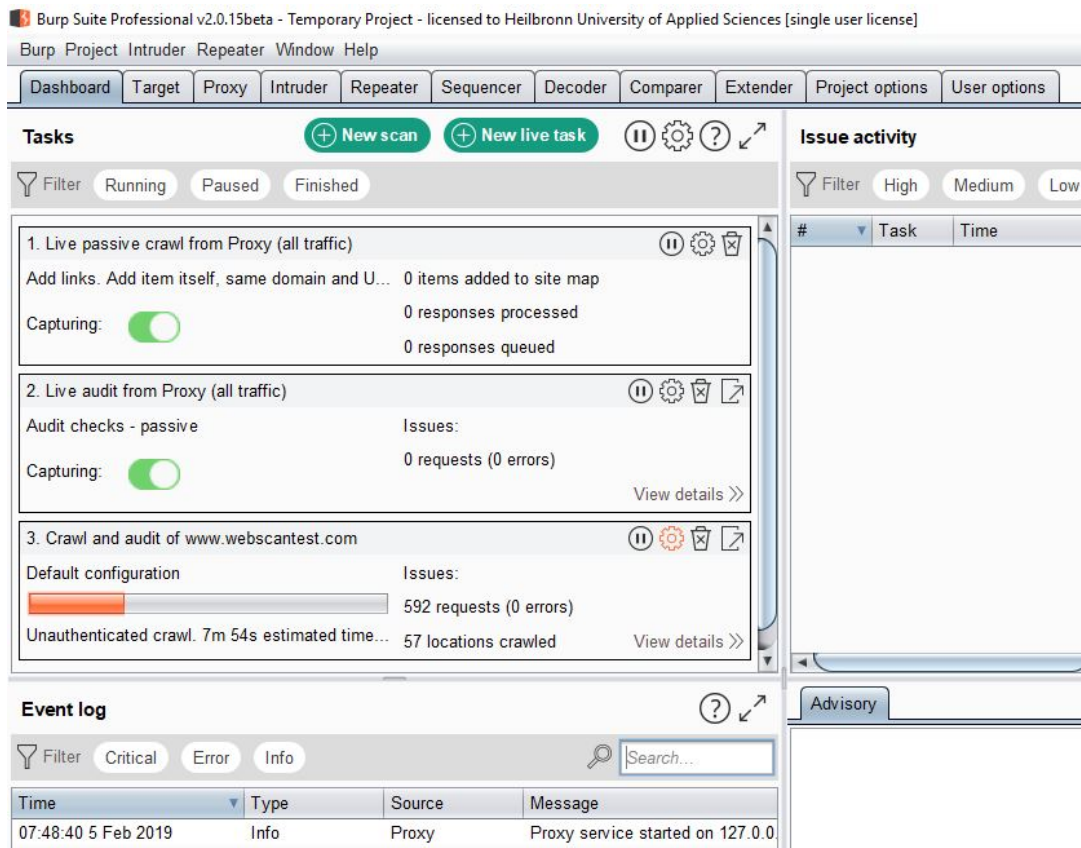


Abbildung 4.7: Dashboard von BurpSuite Pro

Ähnlich wie Arachni unterscheidet BurpSuite zwischen gesicherten und ungesicherten Ergebnissen, allerdings noch genauer: in einer “Confidence”-Tabelle wird zwischen gesicherten (Certain), wahrscheinlichen (Firm) und möglichen (Tentative) Schwachstellen unterschieden (siehe Abb. 4.8).

Bewertung: Reporting 4, Bedienung 3, Geschwindigkeit 2

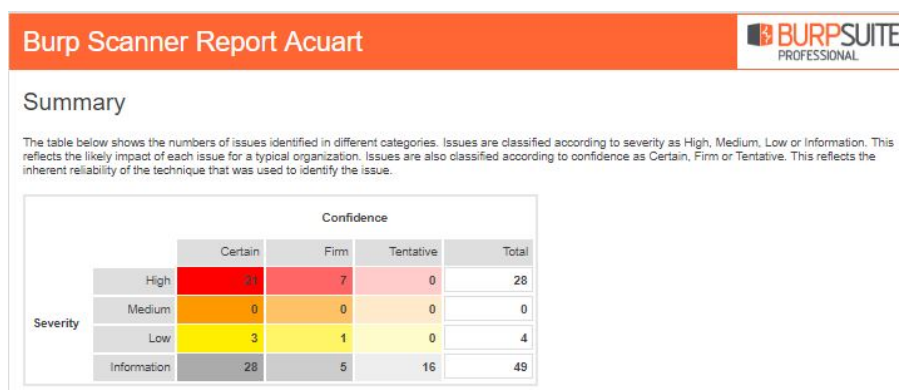


Abbildung 4.8: Confidence-Tabelle im Report von BurpSuite Pro

4.3.3 Gesamtbewertung und Ranking

Open Source WVS

	Arachni	Nikto	OpenVAS	Wapiti	ZAP
Scanergebnis (50%) *5	3	1	4	1	0
Reporting (20%) *2	4	1	2	1	3
Bedienung (20%) *2	3	2	1	2	3
Geschwindigkeit (10%)	3	3	2	3	0
Total	32	14	28	14	12

Tabelle 4.5: Bewertung der Open Source WVS

Kommerzielle WVS

	Acunetix	BurpSuite Pro	Nessus	Netsparker
Scanergebnis (50%) *5	4	4	2	3
Reporting (20%) *2	3	4	2	3
Bedienung (20%) *2	3	3	3	2
Geschwindigkeit (10%)	4	2	2	1
Total	36	36	22	26

Tabelle 4.6: Bewertung der kommerziellen WVS

Ranking aller WVS

	WVS	Total	Scanergebnis	Reporting	Bedienung	Geschwindigkeit
1	BurpSuite Pro	36	4	4	3	2
2	Acunetix	33 ²	4	3	3	4
3	Arachni	32	3	4	3	3
4	OpenVAS	28	4	2	1	2
5	Netsparker	26	3	3	2	1
6	Nessus	22	2	2	3	2
7	Nikto	14	1	1	2	3
7	Wapiti	14	1	1	2	3
9	ZAP	12	0	3	3	0

Tabelle 4.7: Ranking aller WVS

¹Ergebnis nach Abzug von 3 Punkten, siehe Abschnitt 4.3.2

5 Diskussion

In der nachfolgenden Diskussion sollen die Ergebnisse der Evaluation im Hinblick auf die in der Einleitung thematisierten Fragestellungen analysiert und erörtert werden.

5.1 Anzahl der gefundenen Schwachstellen

Die Tabellen 4.3 und 4.4 zeigen eine große Bandbreite an unterschiedlichen Ergebnissen. Während ZAP insgesamt nur 63 Schwachstellen findet, sind es bei BurpSuite Pro mit 551 Funden ungefähr neun Mal so viele. Die beiden Terminalprogramme Nikto und Wapiti liegen fast gleichauf mit 97 und 93 Funden und sind damit nur geringfügig besser als das Schlusslicht ZAP. Mit 265 Funden hat Nessus bei den kommerziellen Scannern das schlechteste Ergebnis, überraschend ist hier vor allem, dass die Open Source Software und Nessus-Abspaltung OpenVAS fast 200 Schwachstellen mehr findet. OpenVAS lässt mit diesem Ergebnis auch noch den kommerziellen WVS Netsparker (389 Funde) hinter sich und belegt insgesamt den dritten Platz. Arachni findet 319 Schwachstellen und reiht sich damit zwischen Nessus und Netsparker ein. Acunetix muss sich mit 517 Funden nur BurpSuite Pro geschlagen geben und belegt hier den zweiten Platz.

Auch wenn die Werte in die Kategorien High, Medium, Low und Informational aufgesplittet werden, gibt es eine breite Palette an Ergebnissen, es gibt fast keinerlei Übereinstimmungen oder erkennbare Muster. Bei den WVS, die bei den insgesamt gefundenen Schwachstellen ungefähr gleichauf liegen, lässt sich dies veranschaulichen: Acunetix hat zum Beispiel mehr als 330 Funde in High und Medium eingeteilt und ca. 180 in Low und Informational, BurpSuite Pro stuft die Schwachstellen als nicht so schwerwiegend ein, gerade einmal 84 Funde finden sich in High und Medium, aber 467 in Low und Informational. Arachni hat 134 Funde in die Kategorie High eingestuft, Nessus nur 37 und OpenVAS gar nur neun.

Selbst wenn man die Ergebnisse nach den verwundbaren Webanwendungen aufteilt, gibt es keine Wiedererkennungswerte. Weder gibt es eine Webseite, bei der von allen WVS besonders viele Schwachstellen gefunden wurden, noch sticht eine mit besonders wenigen Funden heraus. Auch die Anzahl der Funde pro Webanwendung ist von WVS zu WVS sehr verschieden. So findet zum Beispiel Acunetix auf der Seite Zero Bank (WA3)

68 Schwachstellen, BurpSuite Pro nur 14, andererseits findet BurpSuite Pro auf Webscantest (WA2) 169 Schwachstellen und Acunetix nur 86. OpenVAS findet auf Security Tweets (WA7) 110 Schwachstellen, Netsparker nur 31. Auf Webscantest (WA2) hingegen findet Netsparker doppelt so viele (99) Schwachstellen wie OpenVAS (49).

Bezüglich der Webanwendungen gibt es eine interessante Beobachtung: Acunetix (WA5) und Security Tweets (WA7) wurden beide von Acunetix entwickelt, die naheliegende Vermutung, dass der WVS von Acunetix hier besonders viele Schwachstellen finden müsste, hat sich nicht bestätigt. Ebenso wenig findet auch Netsparker auf der selbst entwickelten Bitcoin Web Site (WA4) relevant mehr Schwachstellen als die anderen WVS, Acunetix und BurpSuite Pro finden sogar deutlich mehr.

Zusammenfassend muss festgehalten werden, dass bei der Anzahl der gefundenen Schwachstellen keinerlei Regelmäßigkeiten erkennbar sind. Die Ergebnisse der einzelnen WVS weisen erhebliche Unterschiede auf und so lässt sich die erste Forschungsfrage **Wie viele Schwachstellen werden von den WVS gefunden?** nur für jeden WVS individuell beantworten - mit Blick auf die Tabellen 4.1 und 4.2.

5.2 Bedienung, Reporting und Scan-Geschwindigkeit

Die nachfolgenden Abschnitte widmen sich der Fragestellung **Wie unterscheiden sich die WVS in den Kategorien Bedienung, Reporting und Scan-Geschwindigkeit?**

5.2.1 Bedienung

In dieser Kategorie gibt es keinen WVS, der die volle Punktzahl erreicht, es gibt aber auch keinen mit null Punkten (siehe Tabellen 4.5 und 4.6). Den beiden Terminalprogrammen Nikto und Wapiti fehlt es naturgemäß am Komfort, den eine grafische Benutzeroberfläche bietet, trotzdem schneiden sie noch besser ab als OpenVAS, das erst nach umfangreicher Einarbeitungszeit sinnvoll genutzt werden kann. Das Streben nach Automatisierung geht hier zu Lasten der Bedienbarkeit. Netsparker befindet sich mit seiner überladenen Benutzeroberfläche ebenfalls nur im Mittelfeld, Acunetix, BurpSuite Pro und Nessus sind - erwartungsgemäß für kommerzielle WVS - sehr übersichtlich und benutzerfreundlich. Die Open Source Programme Arachni und ZAP stehen dem jedoch in nichts nach und sind ebenfalls leicht verständlich und intuitiv zu bedienen.

Insgesamt gibt es in dieser Kategorie keinen klaren Sieger, mit Ausnahme von OpenVAS sind alle WVS mühelos und unproblematisch zu bedienen.

5.2.2 Reporting

Nikto und Wapiti schneiden in dieser Kategorie unterdurchschnittlich ab, da sie die gefundenen Schwachstellen nicht nach Schweregrad unterteilen (siehe Tabellen 4.5 und 4.6). Das Reporting von Nessus und OpenVAS könnte ausführlicher sein, OpenVAS verzichtet auf die Nennung von gefundenen Schwachstellen der Kategorie “Informational”, bei Nessus sind die Beschreibungen der Schwachstellen und Lösungsvorschläge nur online abzurufen, das bedeutet zusätzlichen Aufwand, wenn der Auftraggeber einen gedruckten Bericht wünscht. Überdurchschnittlich schneiden ZAP, Acunetix und Netsparker ab, die alle sehr umfangreiche Beschreibungen der Schwachstellen liefern. Netsparker ist hier hervorzuheben für die zusätzliche Kategorie “Critical” und die besondere Kennzeichnung gesicherter Ergebnisse als “Confirmed”. Überraschende Ergebnisse liefern Arachni und BurpSuite Pro, Arachni sticht neben der Unterscheidung zwischen gesicherten und noch zu überprüfenden Ergebnissen mit seinen ausführlichen Statistikfunktionen heraus, BurpSuite Pro mit seiner “Confidence”-Tabelle, die die Schwachstellen noch genauer zwischen gesichert, wahrscheinlich und tentativ differenziert. Zudem bieten beide äußerst detaillierte Beschreibungen der Schwachstellen und sind trotzdem sehr übersichtlich gestaltet.

5.2.3 Scan-Geschwindigkeit

Mit einer Ausnahme liegen die Scan-Geschwindigkeiten alle im vertretbaren Bereich, lediglich ZAP weicht hier mit Scanzeiten von 10 bis 14 Stunden pro Webanwendung ungewöhnlich weit von der Norm ab (siehe Tabellen 4.1 und 4.2). Selbst die Werte von Netsparker, der auf dem vorletzten Platz landet, sind bis auf einen Ausreißer bei Webscantest (WA2) akzeptabel. Die Zeiten von OpenVAS, BurpSuite Pro und Nessus liegen alle nah beieinander und ordnen sich im Mittelfeld ein. Arachni sowie die beiden Terminalprogramme Nikto und Wapiti scannen überdurchschnittlich schnell, der beste WVS in dieser Kategorie ist mit großem Vorsprung Acunetix, der teilweise keine zehn Minuten für einen Scan benötigt.

5.3 Ranking

Tabelle 4.7 zeigt einen klaren Verlierer dieser Evaluation: ZAP ist der einzige WVS, der mit null Punkten bewertet werden musste, und das gleich zweimal, in den Kategorien Scanergebnis und Geschwindigkeit. ZAP ist damit als unbrauchbar zu bezeichnen, zumindest in der Funktion als WVS; die jeweils drei Punkte in den Kategorien Reporting und Bedienung sind wertlos, da kaum Schwachstellen gefunden werden. Nikto und Wapiti liegen mit jeweils 14 Punkten auf dem vorletzten Platz, mit den dürftigen

Scanergebnissen und den Mängeln im Reporting sind diese Tools für professionelles Penetration Testing nur sehr bedingt tauglich. Nessus befindet sich mit 22 Punkten im unteren Mittelfeld und kann nur in der Kategorie Bedienung überzeugen, erfüllt aber insgesamt seinen Zweck. Netsparker hat gute Werte im Scanergebnis und im Reporting und belegt mit 26 Punkten den 5. Platz. OpenVAS erreicht 28 Punkte und lässt damit den kommerziellen WVS Nessus, aus dem OpenVAS hervorgegangen ist, hinter sich. Auf den ersten drei Plätzen befinden sich mit Arachni, Acunetix und BurpSuite Pro diejenigen WVS, die durchweg überdurchschnittliche und überragende Werte erreicht haben und somit fast uneingeschränkt empfehlenswert sind. Arachni belegt mit 32 Punkten den 3. Platz und ist damit der beste Open Source WVS. Acunetix belegt mit 33 Punkten den 2. Platz, allerdings nur durch den Punktabzug aufgrund der Abstürze beim Testen unter Windows. Ohne Abstürze hätte Acunetix sich den ersten Platz mit BurpSuite Pro geteilt.

Testsieger und damit die Antwort auf die Frage **Welcher WVS schneidet insgesamt am besten ab?** ist BurpSuite Pro mit 36 Punkten. Ausschlaggebend für das Ergebnis sind in erster Linie das Scanergebnis und das Reporting, in beiden Kategorien hat BurpSuite Pro am besten von allen WVS abgeschnitten.

5.4 Open Source im Vergleich mit kommerziellen WVS

Nachfolgend wird die Frage **Wie schneiden die Open Source WVS im Vergleich mit kommerziellen WVS ab?** erörtert.

Von den fünf getesteten Open Source WVS finden sich im Ranking drei auf den letzten Plätzen wieder (siehe Tabelle 4.7). Nikto und Wapiti haben als Terminalprogramme naturgemäß Nachteile in der Handhabung, sie schneiden aber auch beim Scanergebnis und im Reporting unterdurchschnittlich ab. ZAP auf dem letzten Platz ist zwar als WVS ungeeignet, wird in der Regel aber auch als "Intercepting Proxy" verwendet, der den Browsertraffic abfangen, überprüfen und verändern kann. Der Name deutet darauf hin, dass dies die Hauptfunktion von ZAP ist, vom schlechten Abschneiden als WVS sollte hier also nicht auf die übrigen Funktionen geschlossen werden.

Arachni und OpenVAS auf dem 3. und 4. Platz im Gesamtranking schneiden besser ab, als die kommerziellen WVS Netsparker und Nessus und stellen damit zwei kostengünstige Alternativen dar. Nach Bewältigung der Einarbeitungszeit lassen sich mit OpenVAS gute Ergebnisse erzielen, insbesondere wenn man einen hohen Automatisierungsgrad anstrebt. Arachni überzeugt mit leichter Handhabung, sehr gutem Reporting und überdurchschnittlicher Geschwindigkeit, bei der Anzahl der gefundenen Schwachstellen setzen sich jedoch die kommerziellen WVS BurpSuite Pro und Acunetix durch.

6 Fazit und Ausblick

Das Ziel dieser Arbeit war es, aus der großen Anzahl von WVS die für eine Evaluation geeigneten herauszufiltern und auf ihre Tauglichkeit und Qualität zu testen. Nach eingehender Prüfung der in Frage kommenden Kandidaten wurden schließlich neun in die Evaluation aufgenommen, fünf Open Source- und vier kommerzielle WVS. Zum Testen wurden sieben verwundbare Webanwendungen mit verschiedenen Technologien ausgewählt, die von den WVS gescannt und auf Schwachstellen überprüft wurden. Anhand eines Punktesystems wurden die WVS in den Kategorien Scannergebnis, Reporting, Bedienung und Geschwindigkeit verglichen. Neben dem Aufzeigen der Unterschiede in den einzelnen Kategorien sollten die Fragen beantwortet werden, welcher WVS das beste Resultat erzielt und wie die Open Source WVS im Vergleich zu den kommerziellen Scannern abschneiden.

Durch die Evaluation ist es gelungen, für jede Fragestellung Antworten zu finden:

Anzahl gefundener Schwachstellen: Mit Hilfe der Tabellen 4.3 und 4.4 werden die Unterschiede bei der Anzahl gefundener Schwachstellen sichtbar gemacht. BurpSuitePro und Acunetix schneiden in dieser Kategorie mit über 500 Funden am besten ab. Auffällig ist, dass sich insgesamt keine Übereinstimmungen zwischen den WVS feststellen lassen, weder bei Aufsplittung der Ergebnisse in High, Low, Medium und Informationale, noch bei den Resultaten für die einzelnen Webanwendungen. Erwartungen bezüglich anzu-treffender Muster oder Regelmäßigkeiten können nicht bestätigt werden.

Bedienung, Reporting und Geschwindigkeit: Die Scan-Geschwindigkeit wurde den Berichten entnommen oder manuell ermittelt. Die subjektiven Eindrücke für die Bedienung und das Reporting wurden für jeden WVS einzeln beschrieben und mit Hilfe des Punktesystems bewertet. Die Ergebnisse werden in den Tabellen 4.5 und 4.6 dargestellt. Die Bewertung resultiert in einem Gesamtranking (siehe Tabelle 4.7).

Ranking: Aus dem Gesamtranking (siehe Tabelle 4.7) lässt sich der WVS ermitteln, der am besten abgeschnitten hat, es ist BurpSuite Pro mit 36 Punkten. Hieraus sollte jedoch keine Allgemeingültigkeit abgeleitet werden, es ist das Ergebnis des für diese Thesis

angewandten Testverfahrens mit seinem individuellen Testaufbau und seinen spezifischen Gewichtungen der Kategorien.

Open Source im Vergleich mit kommerziellen WVS: Anhand des Rankings wurde auch das Abschneiden der Open Source WVS aufgezeigt, mit Arachni und OpenVAS an dritter und vierter Stelle der Rangliste gibt es vollwertige, kostenlose Alternativen zu den kommerziellen WVS.

Ungeachtet der Resultate soll hier durch Reflexion der gewählten Methodik auch auf die Grenzen der Evaluation eingegangen werden.

So hat die Gesamtanzahl der gefundenen Schwachstellen zum Beispiel nur eingeschränkte Aussagekraft; zum einen müsste jeder Fund noch durch manuelles Testen verifiziert werden, um False-Positives auszuschließen, zum anderen ist die durch die WVS vorgenommene Einteilung in die Kategorien “High”, “Medium”, “Low” und “Informational” problematisch, da die “Informational”-Funde, wie der Name schon sagt, nur der Information dienen und gar kein Eingreifen erfordern. Würde man diese Werte ausblenden, ergäbe sich im Ranking ein komplett anderes Bild, der Testsieger BurpSuite Pro käme zum Beispiel nur noch auf 107 gefundene Schwachstellen und würde damit in dieser Kategorie den vorletzten Rang belegen. In diesem Zusammenhang muss rückblickend auch die Gewichtung der einzelnen Kategorien hinterfragt werden, angesichts der zweifelhaften Aussagekraft des Scannergebnisses ist die Gewichtung von 50% vielleicht zu hoch angesetzt.

Die Ergebnisse dieser Thesis sind somit als Grundlage für weitergehende Evaluationen einzuordnen.

Für künftige Studien sind mehrere Ansätze möglich:

- Durch Verifizierung der False-Positives werden die Scan-Ergebnisse genauer, hier müsste allerdings aufgrund des hohen Aufwands die Anzahl der WVS und der Webanwendungen reduziert werden.
- Durch Weglassen der “Informational”-Funde werden nur relevante Schwachstellen erfasst, die auch tatsächlich ein Eingreifen erfordern.
- Bei Auswahl und Gewichtung der Bewertungskategorien können andere Prioritäten gesetzt werden, indem etwa die Scan-Geschwindigkeit vernachlässigt oder bei den kommerziellen WVS der Preis miteinbezogen wird.

Des Weiteren sei hier für tiefergehende Analysen auf das Projekt OWASP-Benchmark [50] verwiesen, eine von OWASP entwickelte, kostenlose Testsuite, mit der WVS in mehrtägigen Scans anhand von Tausenden von Testfällen untersucht werden können.

Quellenverzeichnis

- [1] Dafydd Stuttard und Marcus Pinto. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition*. John Wiley & Sons, Inc., 2011.
- [2] CVE Details. *Vulnerabilities by Year*. 2019. URL: <https://www.cvedetails.com/browse-by-date.php> (besucht am 26.03.2019).
- [3] Bitkom. *Wirtschaftsschutz in der Industrie*. 2018. URL: <https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf> (besucht am 02.03.2019).
- [4] Bundesamt für Sicherheit in der Informationstechnik. *Leitfaden zur Entwicklung sicherer Webanwendungen*. BSI, 2013.
- [5] Hannes Holm. *A quantitative evaluation of vulnerability scanning*. Royal Institute of Technology, Stockholm, 2011.
- [6] Martin Wundram. „Die schwächste Stelle, Drei Webapplikations-Scanner im Vergleich“. In: *iX* (2011), 72–77.
- [7] Martin Wundram. „Gut Gesucht, Werkzeuge für das Aufspüren von Schwachstellen“. In: *iX* (2012), 92–98.
- [8] OWASP. *Category: Vulnerability Scanning Tools*. 2019. URL: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools (besucht am 26.01.2019).
- [9] Matthias Rohr. *Sicherheit von Webanwendungen in der Praxis, 2. Auflage*. Springer Fachmedien Wiesbaden GmbH, 2018.
- [10] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschrutzkatalog*. BSI, 2016.
- [11] Bundesamt für Sicherheit in der Informationstechnik. *Lebenszyklus einer Schwachstelle*. 2018. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_027.pdf?__blob=publicationFile&v=4 (besucht am 16.03.2019).
- [12] Web Application Security Consortium. *The WASC Threat Classification v2.0*. 2010. URL: <http://projects.webappsec.org/w/page/13246978/Threat%20Classification> (besucht am 16.03.2019).
- [13] OWASP. *OWASP Top 10 Application Security Risks*. 2017. URL: https://www.owasp.org/index.php/Top_10-2017_Top_10 (besucht am 28.12.2018).

- [14] Patrick Engebretson. *The Basics of Hacking and Penetration Testing*. Elsevier Inc., 2013.
- [15] Vogel Communications Group. *Was ist eine Web Application Firewall?* 2017. URL: <https://www.security-insider.de/was-ist-eine-web-application-firewall-a-627220/> (besucht am 13.03.2019).
- [16] Bundesamt für Sicherheit in der Informationstechnik. *Sicherheit von Webanwendungen, Maßnahmenkatalog und Best Practices*. BSI, 2006.
- [17] Ron Lepofsky. *The Manager's Guide to Web Application Security*. Apress, Berkeley, CA, 2014.
- [18] nstalker.com. *N-Stalker*. 2019. URL: <http://www.nstalker.com> (besucht am 20.02.2019).
- [19] Golismero Project. *Golismero*. 2019. URL: <http://www.golismero.com> (besucht am 19.02.2019).
- [20] Romain Gaucher. *Grabber*. 2006. URL: <http://rgaucher.info/beta/grabber/> (besucht am 19.02.2019).
- [21] David Byrne. *Grendel-Scan*. 2015. URL: <https://sourceforge.net/projects/grendel/> (besucht am 19.02.2019).
- [22] Lavakumar Kuppan. *IronWasp*. 2014. URL: <https://ironwasp.org> (besucht am 19.02.2019).
- [23] Google.com. *ratproxy*. 2009. URL: <https://code.google.com/archive/p/ratproxy/> (besucht am 19.02.2019).
- [24] Google.com. *skipfish*. 2012. URL: <https://code.google.com/archive/p/skipfish/> (besucht am 19.02.2019).
- [25] Bernardo Damele. *sqlmap*. 2019. URL: <http://sqlmap.org> (besucht am 19.02.2019).
- [26] Subgraph. *Vega*. 2014. URL: <https://subgraph.com/vega/> (besucht am 19.02.2019).
- [27] siberas. *Watobo*. 2015. URL: <https://sourceforge.net/projects/watobo/> (besucht am 19.02.2019).
- [28] OWASP. *OWASP WebScarab Project*. 2014. URL: https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project (besucht am 19.02.2019).
- [29] sectools.org. *Wfuzz*. 2019. URL: <http://www.edge-security.com/wfuzz.php> (besucht am 19.02.2019).
- [30] w3af.sourceforge. *w3af*. 2013. URL: <http://w3af.org> (besucht am 19.02.2019).
- [31] sensepost. *Wikto*. 2015. URL: <https://github.com/sensepost/wikto> (besucht am 19.02.2019).
- [32] OWASP. *OWASP Xenotix XSS Exploit Framework*. 2019. URL: <https://xenotix.in> (besucht am 19.02.2019).

- [33] OWASP. *OWASP Vulnerable Web Applications Directory Project*. 2018. URL: https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=On-Line_apps (besucht am 26.02.2019).
- [34] IBM. *Altoro Mutual*. 2019. URL: <https://demo.testfire.net> (besucht am 21.02.2019).
- [35] NTOSpider. *Web Scanner Test Site*. 2019. URL: <https://www.webscantest.com> (besucht am 21.02.2019).
- [36] Micro Focus Development Company. *Zero Bank*. 2018. URL: <http://zero.webappsecurity.com> (besucht am 21.02.2019).
- [37] Netsparker. *Bitcoin Web Site*. 2018. URL: <http://aspnet.testsparker.com> (besucht am 21.02.2019).
- [38] Acunetix. *Acunetix Acuart*. 2018. URL: <http://testphp.vulnweb.com> (besucht am 21.02.2019).
- [39] Micro Focus Development Company. *Crack Me Bank*. 2018. URL: <http://crackme.cenzic.com/kelev/view/home.php> (besucht am 21.02.2019).
- [40] Acunetix. *Security Tweets*. 2013. URL: <http://testhtml5.vulnweb.com> (besucht am 21.02.2019).
- [41] cirt.net. *Nikto2*. 2019. URL: <https://cirt.net/Nikto2> (besucht am 19.02.2019).
- [42] Nicolas Surribas. *Wapiti - The web-application vulnerability scanner*. 2018. URL: <http://wapiti.sourceforge.net> (besucht am 20.02.2019).
- [43] arachni scanner.com. *arachni web application security scanner framework*. 2017. URL: <http://www.arachni-scanner.com> (besucht am 19.02.2019).
- [44] Greenbone. *OpenVAS - Open Vulnerability Assessment System*. 2019. URL: <http://www.openvas.org/index-de.html> (besucht am 19.02.2019).
- [45] OWASP. *The OWASP Zed Attack Proxy*. 2019. URL: <https://www.zaproxy.org> (besucht am 20.02.2019).
- [46] Netsparker. *netsparker*. 2019. URL: <https://www.netsparker.com> (besucht am 20.02.2019).
- [47] Acunetix. *acunetix*. 2019. URL: <https://www.acunetix.com> (besucht am 20.02.2019).
- [48] Tenable. *nessus Professional*. 2019. URL: <https://www.tenable.com/products/nessus/nessus-professional> (besucht am 20.02.2019).
- [49] Portswigger. *Burp Suite Editions*. 2019. URL: <https://portswigger.net/burp> (besucht am 20.02.2019).
- [50] OWASP. *Benchmark*. 2018. URL: <https://www.owasp.org/index.php/Benchmark#tab=Main> (besucht am 25.03.2019).

A Screenshots der Berichte

Generated by Acunetix

Scan of testphp.vulnweb.com

Scan details

Scan information	
Start time	14/02/2019, 16:50:27
Start url	http://testphp.vulnweb.com/
Host	testphp.vulnweb.com
Scan time	5 minutes, 35 seconds
Profile	Full Scan
Server information	nginx/1.4.1
Responsive	True
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	101
 High	39
 Medium	34
 Low	9
 Informational	19

Affected items

/search.php	
Alert group	Blind SQL Injection
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

Abbildung A.1: Bericht Acunetix

Burp Scanner Report Acuart

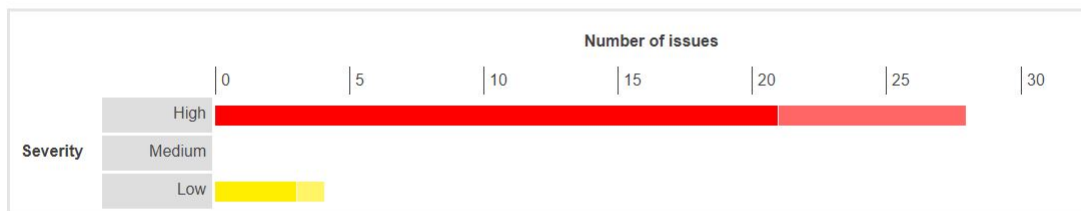


Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	21	7	0	28
	Medium	0	0	0	0
	Low	3	1	0	4
	Information	28	5	16	49

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. SQL injection

- 1.1. <http://testphp.vulnweb.com/artists.php> [artist parameter]
- 1.2. <http://testphp.vulnweb.com/listproducts.php> [artist parameter]
- 1.3. <http://testphp.vulnweb.com/listproducts.php> [cat parameter]
- 1.4. <http://testphp.vulnweb.com/product.php> [pic parameter]
- 1.5. <http://testphp.vulnweb.com/search.php> [test parameter]
- 1.6. <http://testphp.vulnweb.com/secured/newuser.php> [uname parameter]
- 1.7. <http://testphp.vulnweb.com/userinfo.php> [pass parameter]
- 1.8. <http://testphp.vulnweb.com/userinfo.php> [uname parameter]

2. Out-of-band resource load (HTTP)

3. Cross-site scripting (reflected)

- 3.1. <http://testphp.vulnweb.com/guestbook.php> [name parameter]

Abbildung A.2: Bericht BurpSuite Pro

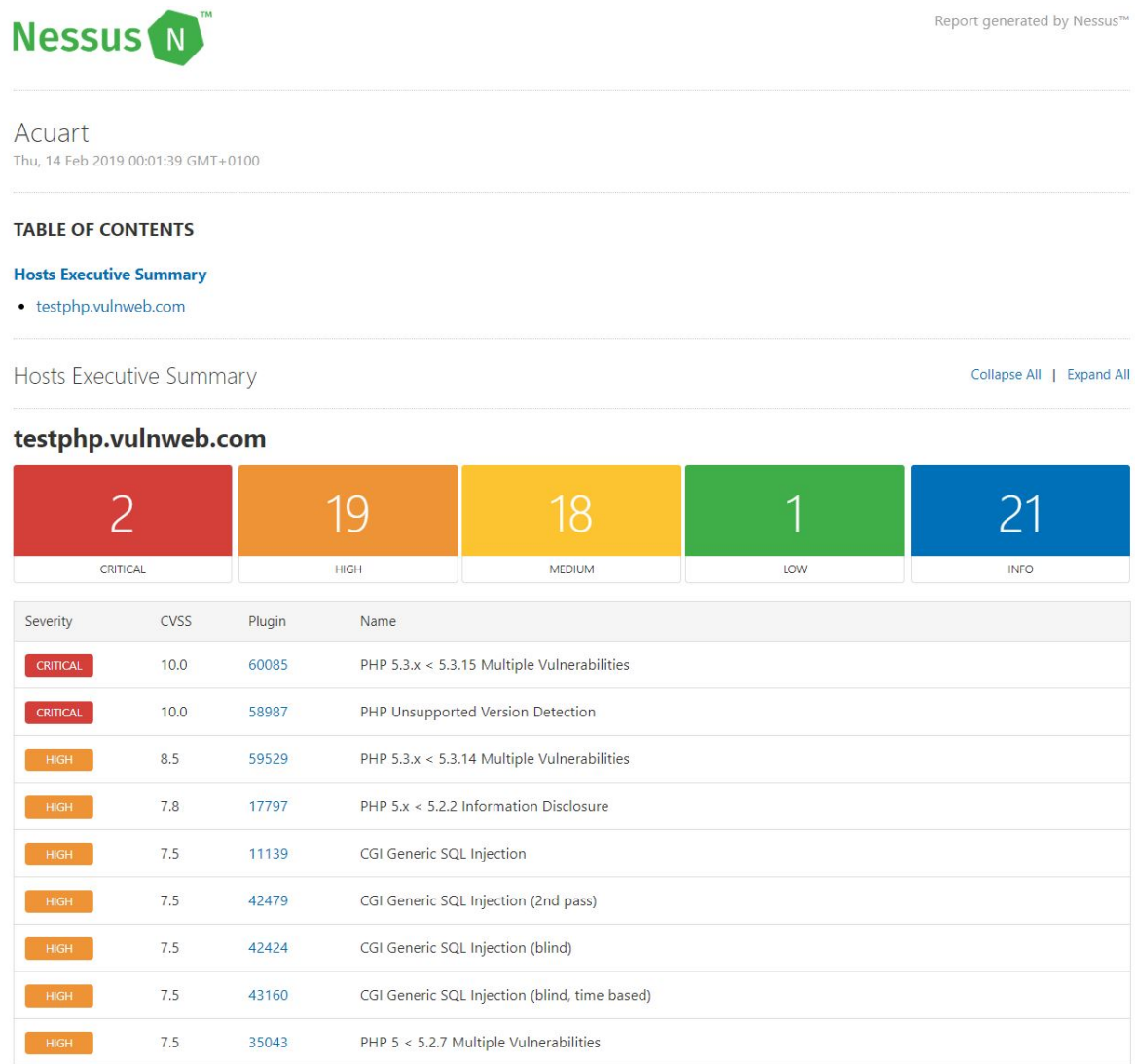


Abbildung A.3: Bericht Nessus

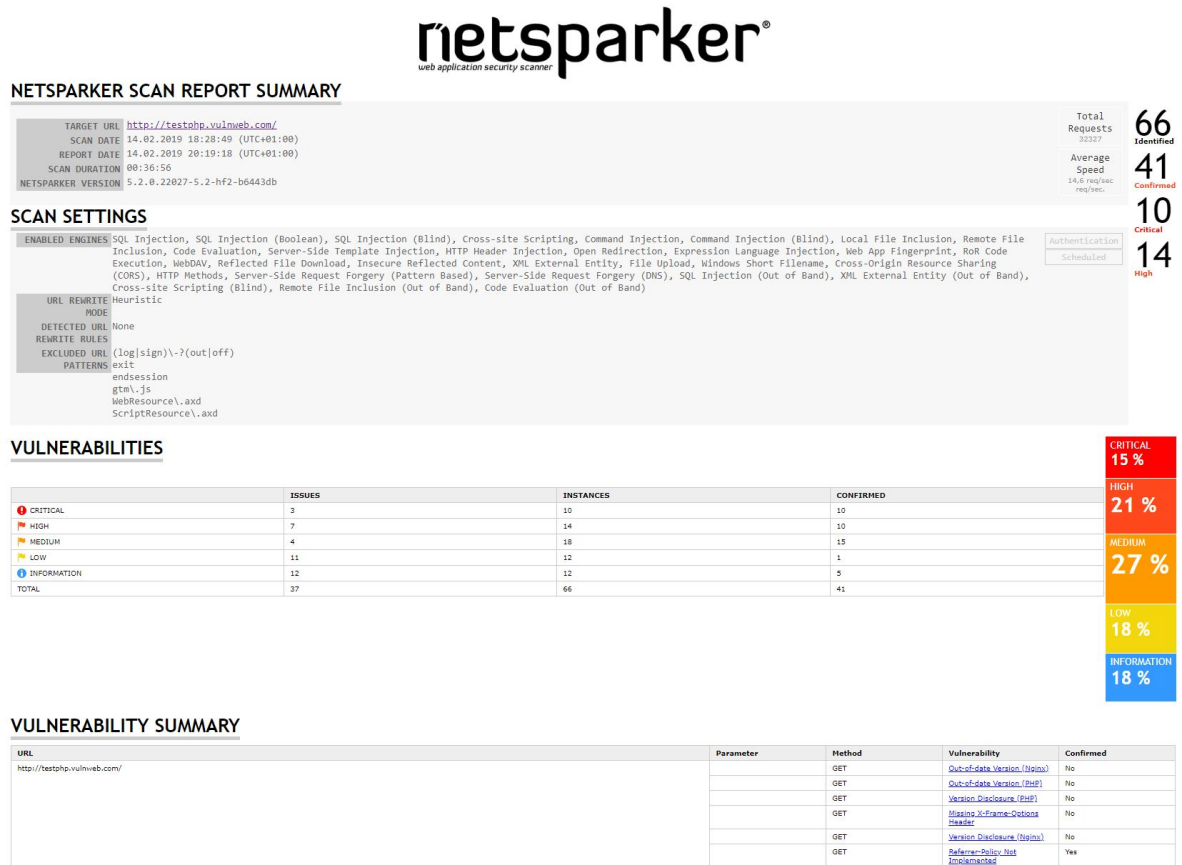


Abbildung A.4: Bericht Netsparker

A Screenshots der Berichte

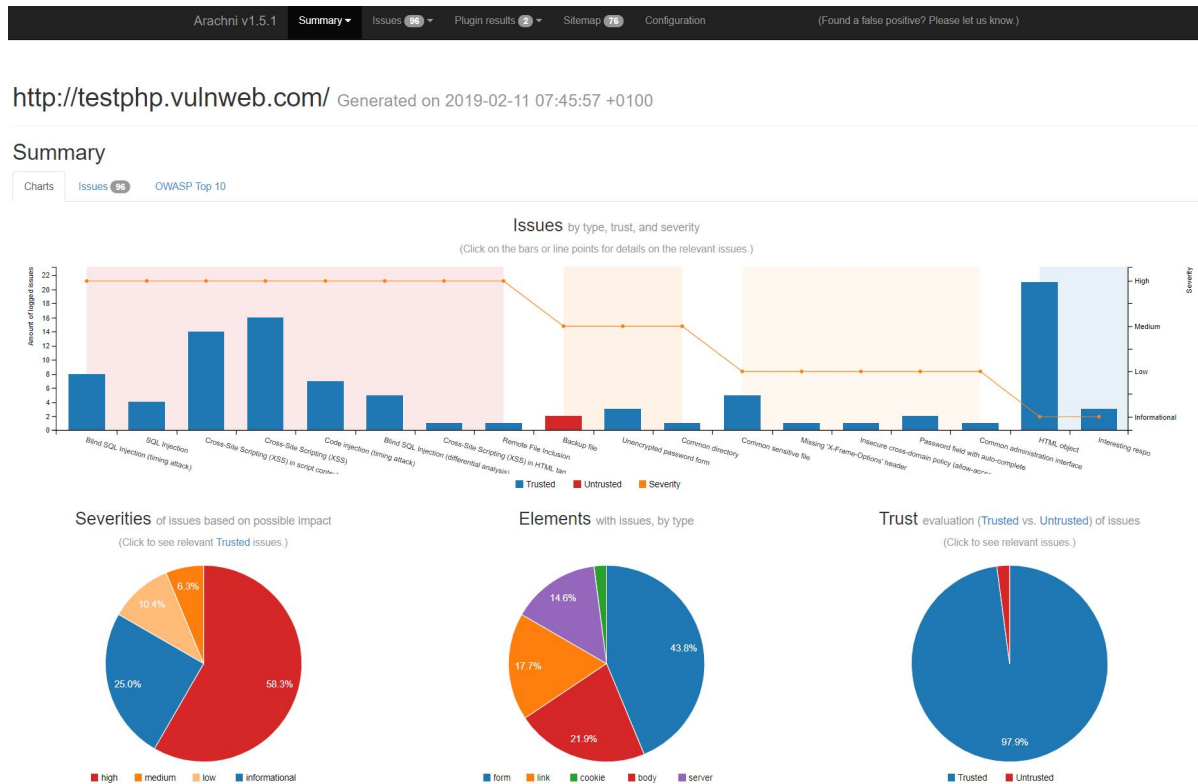


Abbildung A.5: Bericht Arachni

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Log" are not shown. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

This report contains all 34 results selected by the filtering described above. Before filtering there were 199 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started: **Mon Feb 11 21:27:17 2019 UTC**
Scan ended: **Mon Feb 11 22:09:42 2019 UTC**
Task: **Acuort**

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
176.28.50.165 (testphp.vulnweb.com)	Feb 11, 21:27:47	Feb 11, 22:09:42	2	31	1	0	0
Total: 1			2	31	1	0	0

Results per Host

Host 176.28.50.165

Scanning of this host started at: Mon Feb 11 21:27:47 2019 UTC
Number of results: 34

Port Summary for Host 176.28.50.165

Service (port)	Threat Level
general/tcp	High
143/tcp	Medium
995/tcp	Medium
80/tcp	High
25/tcp	Medium
22/tcp	Medium
993/tcp	Medium
465/tcp	Medium

Security Issues for Host 176.28.50.165

High (CVSS: 10.0) OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)	general/tcp
Product detection result: cpe:/o:canonical:ubuntu_jiruk:10.04 by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)	
Summary OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore.	
Vulnerability Detection Result The "ubuntu" Operating System on the remote host has reached the end of life.	

Abbildung A.6: Bericht OpenVAS

testhtml5.vulnweb.com / 176.28.50.165 port 80	
Target IP	176.28.50.165
Target hostname	testhtml5.vulnweb.com
Target Port	80
HTTP Server	nginx/1.4.1
Site Link (Name)	http://testhtml5.vulnweb.com:80/
Site Link (IP)	http://176.28.50.165:80/
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://testhtml5.vulnweb.com:80/ http://176.28.50.165:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://testhtml5.vulnweb.com:80/ http://176.28.50.165:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://testhtml5.vulnweb.com:80/ http://176.28.50.165:80/
OSVDB Entries	OSVDB-0
URI	/favicon.ico
HTTP Method	GET
Description	Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x51e79f63 0x37e
Test Links	http://testhtml5.vulnweb.com:80/favicon.ico http://176.28.50.165:80/favicon.ico
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.3.10-1~lucid+2uwsgi2
Test Links	http://testhtml5.vulnweb.com:80/ http://176.28.50.165:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	OPTIONS
Description	Allowed HTTP Methods: HEAD, OPTIONS, GET
Test Links	http://testhtml5.vulnweb.com:80/ http://176.28.50.165:80/
OSVDB Entries	OSVDB-0
URI	/samples/
HTTP Method	GET
Description	/samples/: This might be interesting...
Test Links	http://testhtml5.vulnweb.com:80/samples/ http://176.28.50.165:80/samples/
OSVDB Entries	OSVDB-3092
Host Summary	
Start Time	2019-02-14 17:15:35
End Time	2019-02-14 17:34:20
Elapsed Time	1125 seconds
Statistics	8354 requests, 20 errors, 7 findings
Scan Summary	
Software Details	Nikto 2.1.6
CLI Options	-h http://testhtml5.vulnweb.com/ -o /root/SecurityTweets_nikto.html -Format HTM
Hosts Tested	1
Start Time	Thu Feb 14 17:15:35 2019
End Time	Thu Feb 14 17:34:20 2019
Elapsed Time	1125 seconds

Abbildung A.7: Bericht Nikto

Wapiti vulnerability report

Target: <http://testphp.vulnweb.com/>

Date of the scan: Wed, 13 Feb 2019 21:59:38 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
SQL Injection	8
Blind SQL Injection	7
File Handling	2
Cross Site Scripting	13
CRLF Injection	0
Commands execution	0
Htaccess Bypass	0
Backup file	0
Potentially dangerous file	0
Server Side Request Forgery	1
Internal Server Error	0
Resource consumption	0

SQL Injection

Description

SQL injection vulnerabilities allow an attacker to alter the queries executed on the backend database. An attacker may then be able to extract or modify informations stored in the database or even escalate his privileges on the system.

Vulnerability found in /artists.php

- [Description](#)
- [HTTP Request](#)
- [cURL command line](#)

MySQL Injection via injection in the parameter artist

Abbildung A.8: Bericht Wapiti

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	1
Low	2
Informational	0

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	uname
Attack	ZAP' OR '1'='1' --
URL	http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
Method	GET
Parameter	cat
Attack	4 OR 1=1 --
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	uname
Attack	ZAP' OR '1'='1' --
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Parameter	pass
Attack	ZAP' OR '1'='1' --
URL	http://testphp.vulnweb.com/artists.php?artist=5-2
Method	GET

Abbildung A.9: Bericht ZAP

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die vorgelegte Bachelorarbeit selbstständig verfasst und noch nicht anderweitig zu Prüfungszwecken vorgelegt habe. Alle benutzten Quellen und Hilfsmittel sind angegeben, wörtliche und sinngemäße Zitate wurden als solche gekennzeichnet.

Löwenstein, den 04.04.2019

Henning Janning