audatis®
Datenschutz und Informationssicherheit | CERT

WEB-SCHWACHSTELLENANALYSE

Überprüfung von Webseiten und Webanwendungen aus Sicht eines Hackers zur Aufdeckung von Sicherheitslücken

Lieber Webseiten-Betreiber,

wer heute eine webbasierte Anwendung im Internet bereitstellt, muss mit zahlreichen Gefahren rechnen, die dort lauern.

Durch die weltweite Verfügbarkeit der Inhalte, können Angriffe auf die Systeme von überall auf der Welt her erfolgen. Dabei gibt es mehrere Ziele, die von Angreifern anvisiert werden:

- Ihre Geschäftsdaten.
- Die Daten Ihrer Kunden.
- Die Ressourcen Ihres Webservers für:
  - die Verbreitung von Spam-Mails,
  - Zwischenlager von Schadsoftware oder
  - das Ausführen von Angriffen auf weitere Webseiten.
- Ausfall Ihrer Seite für:
  - digitale Schutzgelderpressung oder
  - Imageschädigung.

Die wichtigste Erkenntnis sollte für Sie jedoch sein, dass egal welche Angriffsmotive vorliegen und welche Ziele man bei Ihnen verwirklichen kann, die Tatsache entscheidend ist, dass es nur eine Frage der Zeit ist, wann Ihre Webseite angegriffen wird. Selbst der noch so kleine Online-Shop möchte bei Google gefunden werden und so kommen Hacker auch auf Ihre Seite, die nach ungeschützten Systemen die Augen offen halten. Auf ungeschützten oder verwundbaren Seiten bringt der Angriff mehr Erfolg, weil in kürzester Zeit ein großer Nutzen realisiert wird.

Auch der Einsatz von Standardsoftware wie z.B. Homepage-Baukästen, Content-Management- oder Shop-Systemen hilft hier nicht weiter, denn diese sind oftmals fehlerhaft oder enthalten Sicherheitslücken. Vom Betriebssystem des Servers bis zu Ihrer Anwendung, sind es mehrere Millionen Zeilen Quellcode und dort stecken garantiert noch tausende von Fehlern und Schwachstellen, die evtl. bisher niemand gefunden hat. Was aber passiert, wenn diese Schwachstellen gegen Ihr Unternehmen ausgenutzt werden?

Darum sollten Sie sich genau überlegen, welche Sicherheitslücken Ihre Web-Anwendung enthalten könnte, wie Sie diese schließen und es den Angreifern möglichst schwer machen.

Wir bieten Ihnen daher eine professionelle Web-Schwachstellenanalyse an, um Ihnen die notwendigen Gegenmaßnahmen aufzuzeigen und den Angreifern zuvorzukommen.

Carsten Knoop
Geschäftsführer

Welche Risiken hat Ihre Webseite?

Es gibt viele Möglichkeiten Webseiten, Online-Shops oder andere Web-Anwendungen auf mögliche Risikofaktoren zu überprüfen. Die eine Form ist ein manuelles Prüfverfahren, die andere ein (halb) automatisiertes Verfahren. Die beste Variante ist sicherlich beides zu machen, allerdings stellt sich als Unternehmer die Frage, wie man kostengünstig möglichst viele Bedrohungen aus dem Weg räumen kann.

Nicht die Frage der Firmengröße soll entscheiden, welches Verfahren Sie nutzen, sondern die Frage der wirtschaftlichsten Schutzfunktion.

Nach der neuen Datenschutz-Grundverordnung, welche in ganz Europa ab dem 25.05.2018 gilt müssen Sie gem. Art. 32 DS-GVO zukünftig einen Nachweis der Sicherheit liefern. Dieser Nachweis kann für Ihre Internetanwendungen in einer regelmäßigen Web-Schwachstellenanalyse bestehen, was Sie bei allen Bußgeld- oder Haftungsrisiken zukünftig deutlich besser stellt. Diese werden dadurch deutlich minimiert, evtl. sogar komplett vermieden.

Die zwei wichtigsten Entscheidungsfragen:

Ist Ihre Webseite oder Ihr Online-Shop, Blog, CMS, etc. eine Standard-Anwendung oder handelt es sich um eine individuelle, auf Ihre eigenen Bedürfnisse entwickelte Software?

Dort wo sehr viele Standardkomponenten zum Einsatz kommen, sind automatisierte und halb-automatisierte Testverfahren die erste Wahl, um die wichtigsten Sicherheitslücken zu finden. Hierzu eignet sich unsere BASIC Schwachstellenanalyse am besten. Eine automatisierte Überprüfung auf bekannte Schadsoftware kann hier ergänzend eingebunden werden. Je nach Komplexität und Sicherheitsanforderungen der Webseite, ist eine zusätzliche manuelle Überprüfung von Sicherheitslücken oder sogar des gesamten Quellcodes ratsam. Hierbei kommt unsere PREMIUM Schwachstellenanalyse zum Einsatz.

Hat Ihre Website wenig dynamische Inhalte oder ist sie vielmehr eine interaktive Website mit Kontaktformularen, Eingabefeldern für interne Suchen oder sogar mit einem Login-System für Kunden oder Lieferanten?

Wo individualisierte Software und Online-Shops sowie interaktive Webseiten genutzt werden, ist eine manuelle Prüfung als Ergänzung zu empfehlen. Je mehr Daten im Shop und den angebundenen Datenbanken gespeichert werden, desto regelmäßiger sollten die Schwachstellenüberprüfungen durchgeführt werden. Hierzu eignet sich unsere PREMIUM Schwachstellenanalyse.

Wenn Sie unsicher sind, welches Verfahren für Sie am besten geeignet ist oder Sie noch Fragen zur Sicherheit Ihrer Web-Applikationen haben, beraten wir Sie gerne.

Kontaktieren Sie uns per:
Tel.: 05221 87292-0,
E-Mail: info@audatis-cert.de
oder nutzen Sie unser Kontaktformular auf Seite 5.

Unsere Web-Schwachstellenanalysen im Schnellüberblick

	BASIC	PREMIUM
Statische Web-Seite	+++	+++
Interaktive Web-Seite	+	+++
Online-Shop, Standard-Anwendung (z.B. 1&1 Shop, Magento, usw.)	++	+++
Online-Shop, individualisiert	+	+++
Web-Anwendung, Standard (z.B. Blog, CMS, usw.)	++	+++
Web-Anwendung, individualisiert	+	+++
Anzahl URLs	1 Domain / Webanwendung	Beliebig viele Domains und Subdomains
Beschränkung	Ohne Anmeldung (als externer Besucher)	Zusätzlich mit Anmeldung (registrierter Besucher/ Mitglied)
Beschreibung des Testverfahren	Halbautomatisiertes Testverfahren zum Überprüfen der Seite auf die wichtigsten Schwachstellen und Sicherheitslücken durch gängige Hackermethoden	Individuelle und manuelle Testverfahren zum Überprüfen der Schwachstellen und Sicherheitslücken sowie Hackermethoden durch einen Web-Security Experten
Abdeckung	Bietet eine gute Überprüfung mit den wichtigsten Angriffsmöglichkeiten (z.B. nach OWASP)	Bietet eine sehr gute Überprüfung, die fast alle Angriffsmöglichkeiten einbezieht
Berichte	Management Summary der gefundenen Schwachstellen (in deutscher Sprache) sowie ausführlicher Bericht inkl. Beschreibung der Gegenmaßnahmen (auf Englisch)	Optional können alle Berichte auch in deutscher Sprache zur Verfügung gestellt werden
Zertifikat	WEB-SICHERHEIT GEPRÜFT 2020 audatis® Cert GmbH	WEB-SICHERHEIT GEPRÜFT 2020 audatis® Cert GmbH
Preis	Einmalig 649,- € * je Webanwendung	nach individuellem Angebot
Erneute/regelmäßige Prüfung	Bei gleichem Inhalt je 249,- € *	nach individuellem Angebot

* Alle Preise zzgl. gesetzliche USt.

+ nur als Einstieg geeignet

++ gut geeignet (Schwerpunkt: Preis-/Leistung)

+++ sehr gut geeignet (Schwerpunkt: Höchste Sicherheit)

An

audatis® Cert GmbH
Luisenstr. 1

32052 Herford

per Fax: 05221 87292-49
oder E-Mail: info@audatis-cert.de

Web-Schwachstellenanalyse

☐ Hiermit beauftragen wir audatis Consulting mit der Durchführung der BASIC Web- Schwachstellenanalyse und akzeptieren die AGB der audatis Cert GmbH (https://www.audatis.de/ueber-uns/agb).

☐ Wir möchten ein Angebot für die Premium Web-Schwachstellenanalyse bekommen.

☐ Wir benötigen eine unverbindliche Beratung zur Auswahl der für uns passenden Analyse-Methode.

Domain(s)	
Gewünschter Auftragsbeginn	

Auftraggeber

_____
Firma

_____
Straße und Hausnr.

_____
PLZ und Ort

_____
Telefon

_____
Name des Vertretungsberechtigten

_____ _____
Datum *Unterschrift und Stempel Auftraggeber*

audatis®
Datenschutz und Informationssicherheit | CERT

Hauptsitz/Büro Ostwestfalen
Luisenstr. 1 | 32052 Herford
Fon: 05221 87292-0
Fax: 05221 87292-49
E-Mail: info@audatis-cert.de
Internet: www.audatis.de/cert