

# Titel

## ARBEIT

255979

08. Juni, 2009

---

## Vorwort

blaaa

## Inhaltsverzeichnis

<b>1 Sicherheit von Web-Applikationen</b>	<b>A</b>
1.1 Allgemeines . . . . .	A
1.2 Herausforderungen bei der Klassifikation . . . . .	A
<b>Listings</b>	<b>A</b>
<b>Literatur</b>	<b>B</b>

## Abbildungsverzeichnis

## Tabellenverzeichnis

## Listings

# 1 Sicherheit von Web-Applikationen

## 1.1 Allgemeines

Zum Verständnis verschiedener Aspekte von Web Application Firewalls muss ein grundlegendes Verständnis von aktuellen Bedrohungen vorhanden sein, denen Web-Anwendungen gegenüberstehen. Die folgenden Abschnitte sollen den Leser nicht nur sensibilisieren, indem aufgezeigt wird, wie hoch der Grad einer Bedrohung ist. Es soll auch ein prinzipielles, technisches Verständnis vermittelt werden, um in späteren Abschnitten der Arbeit Gegenmaßnahmen sinnvoll bewerten zu können. Trotzdem ist die folgende Auflistung von möglichen Angriffen nicht als technische Referenz zu betrachten. Falls tiefergehendes Interesse an Sicherheitslücken in Web-Anwendungen besteht, wird auf die jeweiligen Quellen verwiesen.

## 1.2 Herausforderungen bei der Klassifikation

Gruppen wie das „Web Application Security Consortium“ [11] haben mit dem „Security Threat Classification Project“ bereits erste Bemühungen zur Etablierung eines offiziellen Standards vollzogen. Die Ausarbeitung unterliegt jedoch ständigen Änderungen und erhielt bisher keine offizielle Zertifizierung. Ähnliche Ambitionen verfolgt das „Open Web Application Security Project“ mit dem „OWASP Top Ten“ Projekt [2]. Dessen Hauptaugenmerk liegt jedoch auf der Einordnung aktueller Bedrohungen nach deren Häufigkeit ihres Auftretens. Das wohl umfangreichste und Projekt ist das „MITRE Common Weakness Enumeration“ (MITRE CWE) Projekt [9], welches Beziehungen zwischen Bedrohungen bzw. Sicherheitslücken auf verschiedenen Ebenen herstellt und diese erläutert. Um eine sinnvolle Einteilung vorzunehmen, muss daher die Problematik dieses Unterfangens analysiert werden. Danach werden verschiedene Möglichkeiten zur Kategorisierung gegeben und die aus Sicht des Autors sinnvollste auf aktuelle Bedrohungen für Web-Anwendungen angewandt.

## Listings

## Literatur

- [1] *AWStats - Free log file analyzer for advanced statistics*,  
<http://awstats.sourceforge.net/>, . – Online, Stand 18. Mai 2009
- [2] AL., Andrew van der Stock e.: *OWASP Top 10 2007*.  
[http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007), 2007. – Online, Stand 11. Mai 2009
- [3] ANLEY, Chris: *Advanced SQL Injection in SQL Server Applications*.  
[http://www.nextgenss.com/papers/advanced\\_sql\\_injection.pdf/](http://www.nextgenss.com/papers/advanced_sql_injection.pdf/), 2002. – On-  
line, Stand 18. Mai 2009
- [4] AUGER, Robert: *The Cross-Site Request Forgery (CSRF/XSRF) FAQ*.  
<http://www.cgisecurity.com/csrf-faq.html/>, 2008. – Online, Stand 18. Mai  
2009
- [5] BECHER, Michael: *Web Application Firewalls - Applied Web application security*.  
VDM Verlag Dr. Müller, 2007
- [6] BELANI, Rohyt: *Basic Web Session Impersonation*.  
<http://www.securityfocus.com/infocus/1774>, 2004. – Online, Stand 18.  
Mai 2009
- [7] BERNES-LEE, et a.: *Uniform Resource Identifier (URI): Generix Syntax*.  
<http://www.ietf.org/rfc/rfc3986.txt>, 2005. – Absatz 3.5 Fragments. Online,  
Stand 18. Mai 2009
- [8] CHAPTER, OWASP G.: *Einsatz von Web Application Firewalls*.  
[http://www.owasp.org/index.php/Category:OWASP\\_Best\\_Practices:\\_Use\\_of\\_Web\\_Application\\_Firewal](http://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewal).  
2008. – Online, Stand 14. Mai 2009
- [9] CHRISTEY, Steve: *2009 CWE/SANSA Top 25 Most Dangerous Programming Errors*.  
<http://cwe.mitre.org/top25/index.html>, 2009. – Online, Stand 11. Mai 2009
- [10] CHRISTOPHER KRUEGEL, Giovanni V.: *Anomaly Detection of Web-Based Attacks*.  
[http://www.cs.ucsb.edu/~vigna/publications/2003\\_kruegel\\_vigna\\_ccs03.pdf](http://www.cs.ucsb.edu/~vigna/publications/2003_kruegel_vigna_ccs03.pdf),  
2003. – Online, Stand 20. Mai 2009
- [11] CONSORTIUM, Web Application S.: *Web Application Security Consortium: Threat Classi-  
fication*. <http://www.webappsec.org/projects/threat/>, 2005. – Online, Stand 11. Mai  
2009
- [12] CONSORTIUM, Web Application S.: *Web Application Security Statistics*.  
<http://www.webappsec.org/projects/statistics/>, 2007. – Online, Stand 11.  
Mai 2009
- [13] COUNCIL, PCI Security S.: *Payment Card Industry (PCI) - Datensicherheit. Seite 36*.  
[http://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_german.pdf](http://www.pcisecuritystandards.org/pdfs/pci_dss_german.pdf), 2008. – Online,  
Stand 20. Mai 2009
- [14] CRAB, Diabolic: *HTTP Response Splitting*. [http://www.infosecwriters.com/text\\_resources/pdf/HTTP\\_Res](http://www.infosecwriters.com/text_resources/pdf/HTTP_Res)  
2005. – Online, Stand 18. Mai 2009
- [15] FERNANDEZ, Kevin: *FBI.gov xssed!* [http://www.xssed.com/news/82/FBI.gov\\_xssed/](http://www.xssed.com/news/82/FBI.gov_xssed/),  
2009. – Online, Stand 11. Mai 2009

- 
- [16] GROSSMAN, Jeremiah: *Vulnerability Assessment Plus Web Application Firewall (VA+WAF)*. [http://www.whitehatsec.com/home/assets/WP\\_WAF061708.pdf](http://www.whitehatsec.com/home/assets/WP_WAF061708.pdf), 2008. – Online, Stand 20. Mai 2009
  - [17] HIGGINS, Kelly J.: *CSRF Vulnerability: A 'Sleeping Giant'*. <http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=208804131/>, 2006. – Online, Stand 18. Mai 2009
  - [18] IVAN RISTIC, et a.: *Web Application Firewall Evaluation Criteria*. <http://www.webappsec.org/projects/wafec>, 2006. – Online, Stand 18. Mai 2009
  - [19] IVAN RISTIC, Ofer S.: *Enough with Default Allow in Web Applications!* [http://blog.modsecurity.org/files/Breach\\_Security\\_Labs-Enough\\_with\\_Default\\_Allow.pdf](http://blog.modsecurity.org/files/Breach_Security_Labs-Enough_with_Default_Allow.pdf), 2006. – Online, Stand 20. Mai 2009
  - [20] JOEL SCAMBRAY, Caleb S. Mike Shema S. Mike Shema: *Hacking Exposed: Web Applications security - Web Security & Solutions*. 2. McGraw-Hill Osborne Media, 2006
  - [21] KACHEL, Erich: *Session-Angriffe - eine Analyse an PHP*. <http://erich-kachel.de/?p=368>, 2008. – Online, Stand 20. Mai 2009
  - [22] KLEIN, Amit: *DOM Based Cross Site Scripting or XSS of the Third Kind*. <http://www.webappsec.org/projects/articles/071105.shtml>, 2005. – Online, Stand 11. Mai 2009
  - [23] KOLOKYTHAS, Panagiotis: *CSRF-Attacke aus dem Web*. [http://www.pcwelt.de/start/sicherheit/firewall/news/196381/csrf\\_attack\\_e\\_aus\\_dem\\_web/](http://www.pcwelt.de/start/sicherheit/firewall/news/196381/csrf_attack_e_aus_dem_web/), 2009. – Online, Stand 18. Mai 2009
  - [24] LUCA CARETTONI, Stefano di P.: *HTTP Parameter Pollution*. [http://www.owasp.org/images/b/ba/AppsecEU09\\_CarettoniDiPaola\\_v0.8.pdf](http://www.owasp.org/images/b/ba/AppsecEU09_CarettoniDiPaola_v0.8.pdf), 2000. – Online, Stand 22. Mai 2009
  - [25] MICROSOFT: *Microsoft Security Bulletin (MS00-078)*. <http://www.microsoft.com/technet/security/bulletin/MS01-026.msp>, 2000. – Online, Stand 20. Mai 2009
  - [26] MICROSOFT: *Microsoft Security Bulletin (MS01-026)*. <http://www.microsoft.com/technet/security/bulletin/MS01-026.msp>, 2001. – Online, Stand 20. Mai 2009
  - [27] NEERUMALLA, Bala: *New SQL Truncation Attacks And How To Avoid Them*. <http://msdn.microsoft.com/en-us/magazine/cc163523.aspx>, 2003. – Online, Stand 20. Mai 2009
  - [28] OFER MAOR, Amichai S.: *Blind SQL Injection*. [http://www.imperva.com/resources/adc/blind\\_sql\\_server\\_injection.html/](http://www.imperva.com/resources/adc/blind_sql_server_injection.html/), 2002. – Online, Stand 18. Mai 2009
  - [29] PAGKALOS, Dimitris: *Verisign, McAfee and Symantec sites can be used for phishing due to XSS*. [http://www.xssed.com/news/72/Verisign\\_McAfee\\_and\\_Symantec\\_sites\\_can\\_be\\_used\\_for\\_phishing\\_due](http://www.xssed.com/news/72/Verisign_McAfee_and_Symantec_sites_can_be_used_for_phishing_due), 2008. – Online, Stand 11. Mai 2009
  - [30] PETKOV, Petko D.: *Google Gmail E-Mail Hijack Technique*. <http://www.gnucitizen.org/blog/google-gmail-e-mail-hijack-technique>, 2007. – Online, Stand 18. Mai 2009



- [31] POESSNECK, Lutz: *Cross-Site Scripting-Lücke in Google-Services*.  
[http://www.silicon.de/sicherheit/management/0,39039020,39189657,00/cross\\_site+scripting\\_luec](http://www.silicon.de/sicherheit/management/0,39039020,39189657,00/cross_site+scripting_luec)  
2008. – Online, Stand 11. Mai 2009
- [32] RANUM, Marcus J.: *The Six Dumbest Ideas in Computer Security*.  
[http://ranum.com/security/computer\\_security/editorials/dumb/index.html](http://ranum.com/security/computer_security/editorials/dumb/index.html),  
2005. – Online, Stand 20. Mai 2009
- [33] RISTIC, Ivan: Web application firewalls primer. In: *(IN)SECURE Magazine* 5 (2006), S.  
6–12. – Beziehbar von <http://www.net-security.org>
- [34] SAMUEL PATTON, David D. William Yurcik Y. William Yurcik: *An Achilles' Heel in Signature-Based IDS: Squealing False Positives in Snort*.  
[http://www.raid-symposium.org/raid2001/papers/patton\\_yurcik\\_doss\\_raid2001.pdf](http://www.raid-symposium.org/raid2001/papers/patton_yurcik_doss_raid2001.pdf),  
2001. – Online, Stand 20. Mai 2009
- [35] SECURENET: *Sicherheit von Webanwendungen - Maßnahmen und Best Practices*.  
<http://www.bsi.bund.de/literat/studien/websec/WebSec.pdf>, 2005. – Seite 51. On-  
line, Stand 18. Mai 2009
- [36] SEGAL, Ory: *Threat Classification*. [http://blog.watchfire.com/wfblog/2007/05/threat\\_classification.html#m](http://blog.watchfire.com/wfblog/2007/05/threat_classification.html#m)  
2007. – Online, Stand 11. Mai 2009
- [37] SK: *SQL Injection Walkthrough*. <http://www.securiteam.com/securityreviews/5DP0N1P76E.html/>,  
2002. – Online, Stand 18. Mai 2009
- [38] SOMMERLAD, Peter: *Reverse Proxy Patterns*. <http://modsecurity.org/archive/ReverseProxy-book-1.pdf>,  
2003. – Online, Stand 13. Mai 2009
- [39] SUBY, Michael: *Web Applications Firewalls Poised to Become Mainstream. Seite 4*.  
[http://blog.modsecurity.org/files/Breach\\_Security\\_Labs-Enough\\_with\\_Default\\_Allow.pdf](http://blog.modsecurity.org/files/Breach_Security_Labs-Enough_with_Default_Allow.pdf),  
2009. – Online, Stand 20. Mai 2009
- [40] WIKIPEDIA: *Cross-Site Request Forgery* — *Wikipedia, Die freie Enzyklopädie*.  
[http://de.wikipedia.org/w/index.php?title=Cross-Site\\_Request\\_Forgery&oldid=59264093/](http://de.wikipedia.org/w/index.php?title=Cross-Site_Request_Forgery&oldid=59264093/),  
2009. – Online, Stand 18. Mai 2009
- [41] WIKIPEDIA: *OSI-Modell* — *Wikipedia, Die freie Enzyklopädie*.  
<http://de.wikipedia.org/w/index.php?title=OSI-Modell&oldid=59723915>, 2009. –  
Online, Stand 13. Mai 2009
- [42] WIKIPEDIA: *Same Origin Policy* — *Wikipedia, Die freie Enzyklopädie*.  
[http://de.wikipedia.org/w/index.php?title=Same\\_Origin\\_Policy&oldid=59756330](http://de.wikipedia.org/w/index.php?title=Same_Origin_Policy&oldid=59756330),  
2009. – Online, Stand 20. Mai 2009
- [43] WIKIPEDIA: *Spiralmodell* — *Wikipedia, Die freie Enzyklopädie*.  
<http://de.wikipedia.org/w/index.php?title=Spiralmodell&oldid=57612723>,  
2009. – Online, Stand 18. Mai 2009
- [44] WIKIPEDIA: *Tschebyschow-Ungleichung* — *Wikipedia, Die freie Enzyklopädie*.  
<http://de.wikipedia.org/w/index.php?title=Tschebyschow-Ungleichung&oldid=58169537>,  
2009. – Online, Stand 20. Mai 2009