Web Attacks: The Biggest Threat to Your Network

Web Security by the Numbers

94% of compromised records are due to hacking and external threats[2]

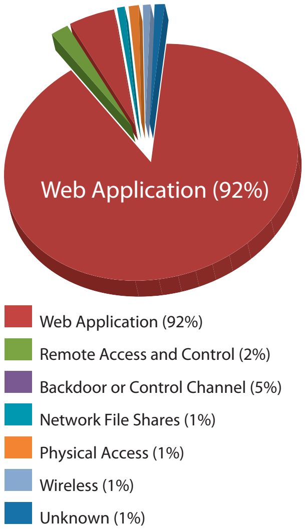
75% of all cyber attacks target web applications[3]

80%+ of discovered vulnerabilities are web vulnerabilities[4]

82% of web applications have had critical vulnerabilities[5]

55% of security professionals believe developers are too busy to address web security[6]

$6.75 Million is the average cost of a data breach[7]



Web application attacks are the single most prevalent and devastating security threat facing organizations today. Attacks such as SQL injection and Cross-Site Scripting (XSS) are responsible for some of the largest security breaches in history, including the top three credit card breaches between 2005 and 2010. At one retailer, hackers used SQL injection to compromise servers and steal 45 million records, costing the organization an estimated $256 million.

Web attacks are growing in number, with 100% of organizations in a broad survey reporting that they had recently suffered a web attack.[1] The same survey found that Web attacks are also the most detrimental type of attack; they cost organizations over 100 times more than malware and 50 times more than viruses, worms and trojans annually.

Web Attacks Are Targeted

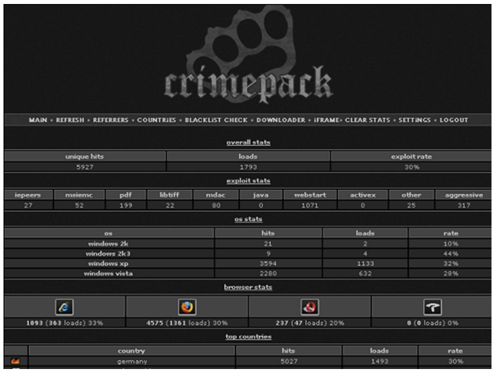
Web applications are easily accessible to hackers. They are also a lucrative attack target because they often store valuable data such as credit card numbers, personally identifiable information (PII) and financial data.

Web Attacks Are Often Successful

Most Web applications – over 80% – have had high, critical, or urgent vulnerabilities. This is due in part to the lack of effort applied to secure coding; most developers are motivated to write code quickly or create new functionality rather than to develop secure applications.

Web Attacks Are Becoming More Advanced

Sophisticated attack techniques have enabled hackers to launch large-scale attacks more quickly. Hackers have also become more organized, building criminal networks and sharing exploits in underground forums. New automated attack tools now leverage search engines to rapidly discover and attack tens of thousands of sites. For even greater efficiency and scale, hackers have built networks of bots – remotely controlled computers – to unleash large-scale attacks.[8] Because Web attacks have become so effective, regulations such as PCI DSS now mandate Web application security.


crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • IFRAME• CLEAR STATS • SETTINGS • LOGOUT

overall stats

unique hits	loads	exploit rate
5927	1793	30%

exploit stats

iepeers	msiemc	pdf	libtiff	mdac	java	webstart	activex	other	aggressive
27	52	199	22	80	0	1071	0	25	317

os stats

os	hits	loads	rate
windows 2k	21	2	10%
windows 2k3	9	4	44%
windows xp	3594	1133	32%
windows vista	2280	632	28%

browser stats

1093 (363 loads) 33%	4575 (1361 loads) 30%	237 (47 loads) 20%	0 (0 loads) 0%

top countries

	country	hits	loads	rate
	germany	5027	1493	30%

Example of a Botnet Management Dashboard

Traditional Network Security Solutions Cannot Stop Web Attacks

Firewalls and intrusion prevention systems (IPSs) are essential for preventing network attacks. "Next generation" firewalls go one step further by adding application awareness, which compares traffic against fingerprints of known applications. Unfortunately, none of these products understand acceptable Web user behavior, such as Web form field input length and allowed characters. Without this application understanding, or white list, network security products cannot accurately detect application attacks like SQL injection, XSS, CSRF, and parameter tampering. In addition, they do not monitor application sessions, so they can't stop cookie poisoning, cookie injection, or session replay attacks. Hackers can also evade network security products using encoding and other Web based evasion techniques. And most network security products cannot decrypt HTTPS (SSL) traffic.

[1] First Annual Cost of Cyber Crime Study, Ponemon Institute, 2010

[2] "2010 Data Breach Investigations Report," Verizon Business, 2010

[3] Gartner Research

[4] "SANS 2009 Top Cyber Security Risks Report," Sans Institute, 2009

[5] "WhiteHat Website Security Statistic Report," WhiteHat Security, Fall 2009, 8th Edition

[6] "State of Web Security," Ponemon Institute, 2010

[7] "US Cost of a Data Breach," Ponemon Institute, 2010

[8] "Industrialization of Hacking," Imperva, 2010

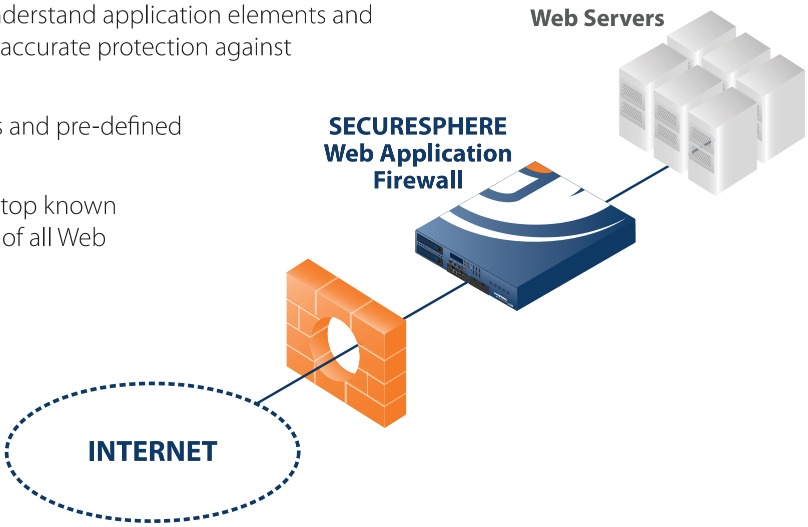
Manual Vulnerability Mitigation Can Be Costly and Expose Applications

One approach to thwarting Web attacks is to follow secure coding best practices and fix outstanding application vulnerabilities. Unfortunately, manually fixing vulnerabilities, particularly in production, can be costly and time consuming. Fixing one vulnerability in production costs $12,000 on average[9] and takes 2 to 4 months,[10] putting applications at risk for long periods of time. While every organization should always follow secure application coding best practices, relying on manual coding and fix processes alone can be costly and expose applications to compromise.

Web Application Firewalls: Purpose Built to Stop Web Attacks

Web Application Firewalls (WAFs) are specifically designed to prevent the biggest threat for every organization with a Web presence today: Web attacks. WAFs combine several security measures together to offer accurate protection against a myriad of threats, including SQL injection, XSS, CSRF, Web site scraping, reconnaissance, application Distributed Denial of Service (DDoS) attacks, and many more.

Web Application Firewall Features



- **Application Profiling (White List) Security** – WAFs understand application elements and expected user behavior, providing input validation and accurate protection against application-specific attacks.
- **Known Attack (Black List) Security** –Attack signatures and pre-defined policies detect known attacks.
- **Reputation-Based Protection** – WAFs recognize and stop known malicious users who account for a growing percentage of all Web attacks.
- **Virtual Patching Through Vulnerability Scanner Integration** – WAFs integrate with vulnerability assessment tools to immediately patch vulnerabilities and eliminate the window of exposure.
- **PCI Compliance** – WAFs address compliance mandates such as PCI DSS #6.6.
- **SSL Inspection** – WAFs inspect and protect encrypted HTTPS (SSL) communications.
- **HTTP Protocol Validation** – WAFs stop buffer overflow attacks, application DDoS, and other abuse.
- **Normalization** – WAFs detect evasion techniques by normalizing traffic and decoding encoded data.
- **Detailed Security Reports and Alerts** – WAFs offer custom and pre-defined security and PCI DSS compliance reports to illustrate security status.

Most WAFs are easy to deploy and offer line speed performance. Most importantly, WAFs help protect your valuable Web assets from dangerous Web application attacks.

[9] “Web Application Security: Don’t Bolt It On; Build It In,” HP, 2008
[10] “WhiteHat Website Security Statistic Report,” WhiteHat Security, Fall 2009, 8th Edition