Web Attack Survival Guide

What Is Your Worst Security Nightmare?

Receiving a "ransom note" with an ultimatum to pay millions of dollars or to watch your company's website buckle under a deluge of DDoS requests? Or opening an ominous Google alert that reveals your company is the next target of a hacktivist campaign? Or discovering the application framework that powers your website is riddled with vulnerabilities—and learning it will take months to fix them?

What Do You Do When Your Worst Nightmare Becomes Reality?

The Web Attack Survival Guide describes today's application threat landscape, including the attack methods and tools used by hacktivists and cybercriminals. It explains the processes and the technologies you can use to safeguard your website from attack. It also helps you prioritize security efforts and it lists security tips and tricks that you might otherwise have overlooked.

After reading the Web Attack Survival Guide, you will be able to confidently face an impending web attack with a well-thought out strategy.

A Blueprint for Web Attack Survival

1	**Understand the Threat Actor**
2	**Develop a Security Response Plan**
3	**Locate and Assess Applications and Servers**
4	**Strengthen Application, Network, and End-Point Security Controls**
5	**Counter the Attack: Monitoring and Tuning Procedures When Under Attack**
6	**Bring in the Experts: Optional Security Consulting Services**
7	**Conduct a Post Mortem of the Attack**

The State of Application Security

The Application Threat Landscape

74% of organizations received a DDoS attack in the past year[1]

86% of all websites have at least one serious vulnerability[2]

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

33% of all websites had at least one serious vulnerability every day of the year in 2012[4]

Web applications sit at the top of the list of hackers' favorite attack targets. In fact, 75% of all cyber-attacks target web applications. Most websites suffer dozens of attacks per day and some sites sustain, on average, up to 26 attacks per minute.

While web attacks are not new—they have existed since the dawn of the Internet—one attack trend is the emergence of hacktivism and prolonged attack campaigns.

Rise of Hacktivism

Hacktivism vaulted onto the scene and into the collective imagination in late 2010, with the emergence of hacktivist groups like Anonymous, LulzSec, and Anti-Sec. Initially targeting financial institutions, Anonymous and its imitators quickly moved on to dozens of other government and business targets. Within two years, 58% of all data theft[5] was attributed to hacktivist attacks.

In 2012, new players, like the Syrian Electronic Army, AnonGhost, and Iranian Cyber Army, joined the party and launched a spree of attacks against U.S. banks and other western targets. Many of these attacks combine traditional web attacks, like SQL injection and cross-site scripting, with Distributed Denial of Service (DDoS) assaults. Hacktivist attacks not only pose public relations disasters for the targeted companies, but many also result in costly data breaches and prolonged website outages.

Distributed Denial of Service (DDoS) Attacks Go Commercial

DDoS Attack Tools Used by Hacktivist and Commercial DDoS Services

Besides the specter of hacktivism, organizations must contend with DDoS attacks launched by competitors or cyber extortionists. These industrialized DDoS attacks can be extraordinarily powerful—hundreds of times greater than typical bandwidth levels, reaching over 300 Gbps or more. And DDoS attacks are becoming more advanced in order to outwit conventional security controls. Instead of simply inundating targets with a flood of TCP or UDP packets, many DDoS attacks now exploit application and database flaws.

Fighting Back

Every day, hackers unleash massive attack campaigns designed to take websites offline, steal confidential data, and deface content. Fortunately, organizations can prepare for and repel these attacks. Based on feedback from application security consultants and from IT security personnel on the front lines of attack, this survival guide lays out a step-by-step plan to fend off web threats.

[1] "2012 Data Breach Investigations Report," Verizon Business, 2012
[2] "WhiteHat website Security Statistic Report," WhiteHat Security, 12th Edition
[3] Gartner Research
[4] "State of Web Security," Ponemon Institute
[5] 2012 Data Breach Investigations Report," Verizon Business, 2012

Web Attack Survival: Step-by-Step Strategy

Step 1. Understand the Threat Actor

"If you know your enemies and know yourself, you will not be imperiled in a hundred battles... if you do not know your enemies nor yourself, you will be imperiled in every single battle."

– Sun Tzu, The Art of War[6]

To prepare for an attack, the first step is to understand the threat actor. What enemy do you face? A well-known hacktivist group such as Anonymous or the Syrian Electronic Army? A script kiddie? Industrialized cybercriminals? Research their attack techniques and identify the tools that they use.

Monitor Social Media

If hacktivists have threatened your organization, then track social media sites such as Twitter, Facebook, and YouTube for updates about their attack methods and timelines. Hacktivists may discuss vulnerabilities or weak points of your site.

Hacktivist groups will also disclose the types of DDoS attack tools that volunteer recruits can use to attack your site. Armed with this information, you can create application security signatures to easily block these attack tools.

With several recent attacks, hacktivists have published "booster packs" that configure attack tools to exploit web vulnerabilities or URLs in the targeted websites. Be aware of the contents of these booster packs, so you can implement policies to repulse them.

Profiling cybercriminals is more challenging than profiling hacktivists, simply because cybercriminals do not advertise their methods or strategies. Unless you monitor hacker forums, your best option is to talk to peers in your industry about attack sources, techniques, and tools.[7] Be sure to read hacker intelligence reports and security research that pertain to your industry.

Step 2. Develop a Security Response Plan

Change Is Unavoidable

Your incident response team may need to apply security policies quickly during an attack. Determine whether you need to relax your internal approval processes to ensure you can rapidly adapt to changing attack vectors.

If your organization is the target of a specific attack campaign, like a DDoS attack or a hacktivist attack, then you should organize an incident response team that will manage security response efforts. The response team may potentially need to be available around-the-clock. Depending on the severity of the attack, assign 24x7 coverage to assure that someone is available to respond to new threats, immediately.

The security response team will most likely be composed of IT security personnel, but may include members from the networking and application development teams.

Red Team

Create a "red team"—a team of security engineers that will look for vulnerabilities that attackers could exploit. The red team should evaluate all potential risks including, application, network, end-user, social engineering, and even physical threats.

[6] Although over-quoted, Sun Tzu's suggestions—from preparation, to the art of deception, to battle tactics—are surprisingly apropos for defending against web attacks.

[7] Security information sharing and analysis organizations include National Council of ISACs, Financial Services ISAC, SANS Internet Storm Center, and National Healthcare ISAC.

Your Little Black Book of Contacts

Prepare a contact list with the names, phone numbers, and email addresses of the following groups:

1. IT security (including members of your security response team), IT operations, networking, application development, database administration, legal, and executive management
2. DNS and Internet Service Providers
3. DDoS Protection Services
4. Relevant security specialists or consultants—for example, record the contact information of field engineers at your web application firewall (WAF), Security Information and Event Management (SIEM), and Intrusion Prevention System (IPS) vendors. You may need to enlist their help when you are under attack.

Document Network and Server Information

Gather network and server information, including:

1. IP addresses of web servers, databases, DNS servers, network firewalls, web application firewalls, database firewalls, and routers and switches
2. Disaster recovery IP addresses, if applicable

Also, prepare network architecture diagrams of all data centers at risk. If architecture diagrams already exist, review them, and make sure they are up-to-date.

Security Tip

DO: Keep your response plan information, network diagrams, and IP address schemes secure.

DON'T: Email your network architecture and contact lists to the entire security department or store them in a public file share titled "Steal me first."

Notify Executive Management and Employees

When you know about an impending attack, inform your executive management team about the threat and provide periodic status updates. In addition, you may need to warn company employees of the attack. For DDoS attacks, notify all relevant users of potential application or network downtime.

If your organization faces a hacktivist attack or a targeted attack, instruct users to update any non-secure passwords and educate them about the risk of phishing attacks. Prepare your IT personnel for social engineering threats. Ask them to verify any IT helpdesk and password change requests.

Hackers may resort to physical attacks when necessary. Secure employee laptops, cables, and network devices.

Establish a War Room

Assign a "general" for the war room. This person will be in charge of all high-level security decisions during the attack.

Designate a war room that will be "ground zero" for all planning and communications during the web attack. The war room will be a centralized place to review security updates and to strategize defense schemes. Choose a location to conduct security operations such as an existing Security Operations Center (SOC), Network Operations Center (NOC), or even a private conference room.

Step 3. Locate and Assess Servers and Applications

Even if you have documented your servers in network architecture diagrams, it is still important to scan your network for rogue servers and applications. Application developers or QA testers may have spun up new web applications or databases; other departments may have deployed unsanctioned applications. Until you have scanned your network and located all servers and applications, you cannot completely assess your risks.

Classify, Classify, Classify

Once you have located your applications and databases, determine which ones contain sensitive data like Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card numbers, or intellectual property. Determine which applications are needed for your business to function properly. Even if your corporate website does not contain sensitive information, it may still be a top target for attack, because it is the most visible to customers and partners.

Once you have identified your servers and applications and determined which are the highest risk, prioritize your efforts on these assets.

Look at the Cloud

Digital assets today are not just limited to the devices on the physical network. Be sure to locate third-party applications like CRM systems, intranet applications, email applications, and internally developed websites that are hosted in the cloud. These applications may contain confidential information. Hacktivists have targeted externally hosted applications in the past, so it is essential to make sure these applications are secure.

Scan Your Network and Applications for Vulnerabilities

Use a combination of different scanners to test your applications. Each scanner may find unique vulnerabilities.

One of the most important steps for fortifying your applications is to test them for vulnerabilities. Scan your servers and networking devices for system vulnerabilities and unpatched software. More importantly, scan your web applications using a purpose-built web application scanner. Network scanners are a starting point, but only web application scanners will uncover the application vulnerabilities that hackers are most likely to exploit.

Do not limit your assessments to your corporate website. Scan all of your applications, including partner portals, CRM applications, extranets, and other potential attack targets. All of these sites could be brought down by hackers and, therefore, damage your company's brand.

Include the same tools used by hacktivists—such as the Havij SQL injection tool and free application scanners—in your scanning arsenal.

To prepare for an application DDoS attack, analyze the URLs in your applications that connect to a backend database and could potentially be an attack target, such as the login, registration, password change, or search pages. Submit application forms with characters like wildcards to determine if they are susceptible to business logic exploits.

Once you have scanned your applications, fix identified vulnerabilities and rescan your applications. If time constraints prevent you from fixing all vulnerabilities, then focus your efforts on virtually patching critical vulnerabilities in your high-risk applications.

Assess Databases

Since sensitive data is typically stored in databases, verify these databases are secure by scanning them for vulnerabilities and configuration flaws. Based on the assessment results, determine if you need to apply any operating system or database security patches or any configuration changes.

To strengthen the security of your database servers, delete default database user accounts and disable unnecessary services like vulnerable database listeners. To fortify the underlying server from attack, disable any unneeded services such as Telnet, FTP and rlogin.

Step 4. Strengthen Application, Network, and End-Point Security Controls

After you have assessed and patched your applications and servers, you can ratchet up your defenses. To thwart a web attack, you should apply stricter web application, network and server-level security policies.

Protect Network Devices and Servers

To prevent network and server attacks:

- Enforce stringent network firewall and Intrusion Prevention System (IPS) policies. Restrict inbound traffic to your web application servers to necessary services like HTTP and HTTPS. Configure IPS policies to block high and critical security violations.
- Install anti-virus or anti-malware software on your servers. Make sure virus, malware, and spyware definition files are up-to-date.
- Configure your database firewall to virtually patch unpatched vulnerabilities. The database firewall can also control access and block unauthorized queries to the database.

Lockdown Web Applications

Work closely with application developers when enforcing stricter profile policies. Developers can help analyze the profile for accuracy. They can also review security alerts to ensure that your new, heightened security controls did not block legitimate requests.

Since the web application is the ultimate target of a web attack, organizations must focus their efforts on tuning and testing their web application firewall to stave off an impending attack. The following reflects a list of best practices to ensure your WAF will block all online threats.

- Review and tune the web application profile—also called the "white list" security model. Confirm that the profile is accurate:
  - Check for URLs or directories that have been removed from the website, but still appear in the profile.
  - Review acceptable characters and parameter value lengths in the profile and look for irregularities in the profile.
  - Compare the application profile to vulnerability scan results to make sure that all URLs in assessment reports appear in the application profile and all URLs in the profile have been assessed by the scanner.
  - Tighten profile policies to block on white-list security violations like parameter values with unauthorized characters such as brackets and question marks. Block excessively long form field values to prevent buffer overflows and SQL injection attacks.
- Configure the WAF to enforce HTTP protocol compliance. Review and tune protocol-related security policies like double encoding, extremely long URLs, and malformed Apache URI messages. Enforcing HTTP protocol compliance, at least during the attack, will foil evasion techniques, as well as buffer overflow and DoS exploits.
- Ensure that standard web application firewall policies such as SQL injection and cross-site scripting (XSS) are enabled. All high risk attacks, such as directory traversal, remote file inclusion (RFI), local file inclusion (LFI,) and cross-site request forgery (CSRF), should be blocked.
- Block malicious sources that have attacked other websites. Leverage intelligence from the global community to stop malicious users and malicious attack strings used against your peers.
- Web application firewalls can detect requests from common scanning and hacking tools like Nikto, Paros, and Nessus based on header agent information. They can also block scanning tools by detecting a frequent number of security violations in a short period of time. To prevent attackers from uncovering vulnerabilities in your site, configure your WAF to block scanners and website reconnaissance.

If your organization hosts customer-facing, partner, or extranet applications in the cloud, ensure that these applications are protected by a WAF. Various solutions exist to safeguard hosted applications, including Security as a Service (SaaS) and virtual appliance-based web application firewalls.

Prevent Application DDoS Attacks

Application-layer DDoS attacks, which account for over 25% of all DDoS attacks, are designed to overwhelm application resources or exploit application vulnerabilities. To stop application DDoS attacks, configure the following policies.

- Block high rates of requests in a short period of time by user, by IP address, and by session. For this DDoS mitigation rule and many of the subsequent rules, configure extended blocking policies—block the offending user for minutes or even hours after the initial violation.
- Block users that download large amounts of data in a short period of time. In addition, to prevent attackers from overwhelming server resources, block users that request multiple files with extensions like ".pdf", ".mp3", ".mpg", or ".mp4" in a short period of time.
- Block users that initiate multiple requests that cause extremely slow web server response times. Such users may be exploiting business logic flaws in the application. In addition, block users that perform multiple HTTP requests that result in web server errors, like 400, 405, or 503 error codes.
- Limit requests to high-risk URLs such as login pages and search pages. These pages are frequent attack targets. To prevent DDoS attacks targeting login pages, create policies that prevent:

  A. An excessive number of failed logins

  B. Multiple successful logins from the same user
- Many application DDoS attacks are launched by botnets. In addition, many attackers attempt to cloak their identity by using anonymizing services. To stop these high-risk sources, block known malicious IP addresses, anonymous proxies, and Tor networks.
- For hacktivist attacks, targeted organizations can monitor social media sites to learn which DDoS tools will be used to conduct the attack. To develop laser-precise DDoS mitigation policies, download the DDoS tool and test it. Look for unusual header or payload strings that can be used to create custom attack signatures. Then define new policies in your web application firewall to block these DDoS tools.

Always On

Make sure you can manage all of your security products from an out-of-band network. Otherwise, they may be unreachable when you need them most—at the peak of a DDoS attack.

Use Cloud-Based DDoS Mitigation Services to Stop Network DDoS Threats

To combat network-layer, or volumetric, DDoS attacks, your network must be able to handle large volumes of traffic—to the tune of tens of gigabits, or even hundreds of gigabits, of traffic per second. To avoid expensive infrastructure and Internet bandwidth costs, many organizations rely on a cloud-based DDoS service to mitigate DDoS attacks.

Cloud DDoS mitigation services can scale on-demand to prevent massive attacks and ensure that malicious traffic never reaches your network.

When evaluating DDoS mitigation services, consider the following capabilities:

- Can the service block both network and application DDoS attacks?
- Can the service accurately detect bots? Can it present various challenges like browser checks and CAPTCHA tests to ensure that only malicious bots are blocked?
- Does the service support anycast DNS routing to ensure that its own DDoS filtering datacenters aren't targeted for attack?
- Does the service offer around-the-clock monitoring and tuning from security specialists?

Prepare!

To reduce the risk of downtime, develop bot mitigation and rate control policies before the attack occurs. Then, enable and adjust the policies when you are under attack.

"Prepare for a cyber-attack as you would prepare for a hurricane. Have a strategy, supplies, and batten down the hatches before the storm starts. When it does start, stay calm and focus on protecting your most important assets."

– Cyber Security Expert in Florida

Step 5. Counter the Attack: Monitoring and Tuning Procedures When Under Attack

Once the web attack is underway, your security response team should devote all available resources to monitor and manage the attack. For intense attacks, you may need to assign shifts to ensure coverage at night and on weekends.

Your security response team should continuously review security alerts from your web application firewalls.

- If attacks are coming from a specific geographic region, create policies to block requests from that region, if it does not represent an important segment of your customer base.
- Analyze bot activity and determine which URLs bots are targeting. Create bot mitigation rules that block bots from accessing those URLs.
- Look for attack patterns and tune policies to block those attacks. For example, if you determine that hackers are attacking a search page, create a policy to block users if they perform 10 search requests in a minute. Create a second policy to block users for 4 hours if they perform 25 requests in 10 minutes. Make it challenging for hackers to recognize the thresholds.

In addition to reviewing application security alerts and adjusting policies, monitor alerts from other networking and security equipment.

- Review log messages from your database firewall; look for unusual activity indicative of a breach.
- Analyze security alerts from network performance monitoring tools to detect bursts of traffic or performance issues.
- Examine aggregated log messages from routers, switches, web servers, and network security tools in your SIEM.

Continue reviewing social media, hacker forums, Internet Relay Chat (IRC) rooms, and sites that catalog website defacements[8] for attack information or evidence that your site has been penetrated. Hacktivists often use the phrase "#TangoDown" on IRC channels to announce they have brought a website down.

Depending on the impact of the attack, it may be necessary to inform your organization's public relations and legal teams of any website outages or data breaches.

[8] Zone-H lists recent of Website defacements at www.zone-h.org/archive.

Step 6. Bring in the Experts: Optional Security Consulting Services

If you face an impending attack and you're worried your organization might not have the experience or the expertise to counter it efficiently, consider engaging outside consultants to assist you through the process. Security consultants can help you prepare for an attack by evaluating your application infrastructure for weaknesses. They can also review your application defenses and help you fine-tune the policies of your security products, such as your web application firewall.

Security consultants can act as an extension of your own security response team during the attack, helping you monitor web attack traffic and adjust mitigation rules accordingly. Based on their extensive experience defeating web attacks, they can help ensure that your organization is well defended against any type of attack.

Step 7. Conduct a Post Mortem of the Attack

According to several interview sources, when the web attack is over, the first order of business for your security response team will often be "to get a beer."[9] After enduring a stressful and prolonged web attack, your security engineers will need some time to recover. However, once the dust has settled, your organization should conduct a post-mortem of the attack.

As part of the post-mortem, review the impact of the attack. Analyze security reports from your web application firewall to investigate attack trends. Examine alert logs from your WAF, your SIEM, and your network monitoring tools.

Your post-mortem assessment should address the following questions:

- Did your network suffer any downtime during the attack?
- Did the attack affect application performance or latency?
- Was any sensitive data compromised?
- What security technologies and processes were in place? Were they effective?
- What improvements can be made in the future?

Once you have completed your post-mortem, you will be better prepared to tackle future web attacks.

Conclusions and Recommendations

Web attacks vary drastically. A script kiddie probing an online retailer for credit card numbers uses starkly different attack methods than hacktivists trying to take down a Fortune 50 banking site. Attack tools change over time—hackers develop new attack tools to evade signature detection and outwit application developers. As a result, your response will need to be flexible.

By including interviews with a number of security experts on the front lines of cyber-warfare—the consultants that help enterprises prepare for, and triage attacks every day, and the security professionals that have locked down their own websites against attack—this survival guide successfully covers a vast swath of today's attacks. It provides an excellent starting point for any organization facing an imminent attack.

[9] Non-alcoholic beer and coffee are suitable alternatives.

Regardless of their motivation, most hackers target websites they deem potentially vulnerable. Once they have exhausted their portfolio of attack techniques, they will move on to the next potential victim. As a result, if organizations can make their websites seemingly impenetrable to attack by implementing ironclad defenses such as real-time attack blocking, anti-automation, multi-gigabit bandwidth elasticity, and session protection, then hackers will move to easier prey.

By following the best practices outlined in the Web Attack Survival Guide, organizations can fortify their websites against threats like hacktivist attacks, application DDoS, and industrialized cyber-attacks.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

IMPERVA®

www.imperva.com