
360
www.360.cn

Web应用安全发展的挑战和趋势

Safe3
http://wangzhan.360.cn

- Web应用安全挑战
- Web应用安全趋势
- Web应用安全云防护

- 常见网站安全问题
  - 使用开源的web应用(Discuz、phpmyadmin)
  - 网站开发人员安全意识薄弱
  - Web server本身漏洞
  - 网站管理人员缺乏安全意识(弱口令等)
  - 网站安全环境差(旁站入侵、嗅探等)
  - Web框架漏洞(Struct2)
  - 网站、DNS拒绝服务攻击

- Struts2远程命令执行漏洞

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0394

众多政府jsp网站存在该漏洞

图：工业和信息化部信息中心分站

- 时尚巴黎女装网遭遇上亿次DDOS攻击

- 新的时代web应用安全面临着新的挑战，这其中包括:

1. 如何拦截web 2.0 js worm 攻击
2. 如何拦截未知web框架漏洞
3. 如何抵御http flood攻击
4. 如何抵御DNS ddos攻击
5. 如何拦截webshell上传以及webshell行为

- Web应用安全挑战
- Web应用安全趋势
- Web应用安全云防护

当前WAF产品分类

- 网络层过滤型（Barracuda 、Imperva 等）
- 内嵌型（ModSecurity 等）
- 云防护型（网站卫士、Cloudflare）
- 代码防御型（phpids、dotnetids等）

当前WAF优缺点对比

- 网络层过滤型

  性能高、受限于网络区域、抗DDOS能力高

- 内嵌型

  性能中、需要本机安装、抗DDOS能力中

- 云防护型

  性能极高、不限网络区域、抗DDOS能力极高

- 代码防御型

  性能低、需要插入代码、抗DDOS能力差

- 新兴网站云防护

国外Cloudflare(市值10亿美元，每月35亿PV，服务12%的网络用户)

国内360网站卫士，普遍采用云防护模式，部署灵活使用简单

- Web应用安全挑战
- Web应用安全趋势
- Web应用安全云防护

- 网站云防护优点

1. 利用分布式架构可以有效解决大型ddos攻击
2. 隐藏后端真实网站ip，杜绝对网站服务器漏洞的直接利用
3. 由专业安全团队及时更新安全规则，第一时间拦截已知和0day漏洞
4. 更精准的用户浏览统计，帮助站长了解网站的发展情况

Q&A

谢 谢 ！

北京市朝阳区建国路71号惠通时代广场D座1号楼 100025
Block 1, Area D, Huitong Times Plaza No.71 JianGuo Road, ChaoYang District Beijing 100025, P.R.C.
Tel: +86 10 5878 1000 **Fax:** +86 10 5878 1001

360
WWW.360.CN