Akamai
Experience the Edge

Akamai eCommerce Seminar

Agenda

Akamai
eCommerce Seminar

- ✓ Recent Cyber Security Threats
- ✓ Demonstrating Live Cyber Attacks/Protections
- ✓ Akamai Security Solutions
- ✓ Proof of Concept for Akamai Security Solutions
- ✓ Conclusions
- ✓ Q&A

Akamai
Experience the Edge

Akamai

eCommerce Seminar

Recent Cyber Security Threats

Akamai
Experience the Edge

Commerce Data Breaches

Akamai
eCommerce Seminar

Saks HACKED Avenue

(5 M Records breached)

"HBC says data breach lasted up to 9 months"

https://www.cbc.ca/news/business/hbc-saks-data-breach-1.4638249

TICKETFLY

(27 M Records breached)

"Ticketfly has been offline since last week after a data breach leaked…

https://globalnews.ca/news/4250616/ticketfly-breach-hacked-online-conert/

Panera BREAD®

(37 M Records breached)

"…exposed in these records included the customer 's Panera loyalty card number"

https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

pumpup

(6 M Records Records)

"…roughly 6 million users of Canadian-based fitnes s app, PumpUp, have been exposed to a cyber atta ck…"

https://evolvemga.com/pumpup/

Akamai
Experience the Edge

Commerce Dark WEB "Price List"

Akamai eCommerce Seminar

Large U.S. Airline Points Accounts — varies based on amount	Price based on points in account 1,500,000 points cost $450 300,000 cost $90 200,000 cost $60
Large International Hotel Chain Points Account	Price based on points in account 1,000,000 points cost $200 400,000 cost $80 300,000 cost $60 200,000 cost $40 100,000 cost $20 50,000 cost $10
Large Middle East Airline Points Accounts — varies based on amount	Price based on points in account 500,000 cost $150 450,000 cost $90 250,000 cost $50

Akamai Experience the Edge

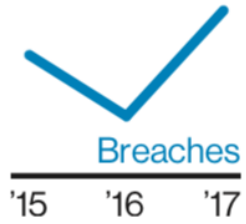
Source : SecureWorks Underground Hacker Markets – 2016

Data Breach from Verizon DBIR

Akamai eCommerce Seminar

Retail

Who	91% external, 10% internal
What	73% payment, 16% personal, 8% credentials
How	46% hacking, 40% physical

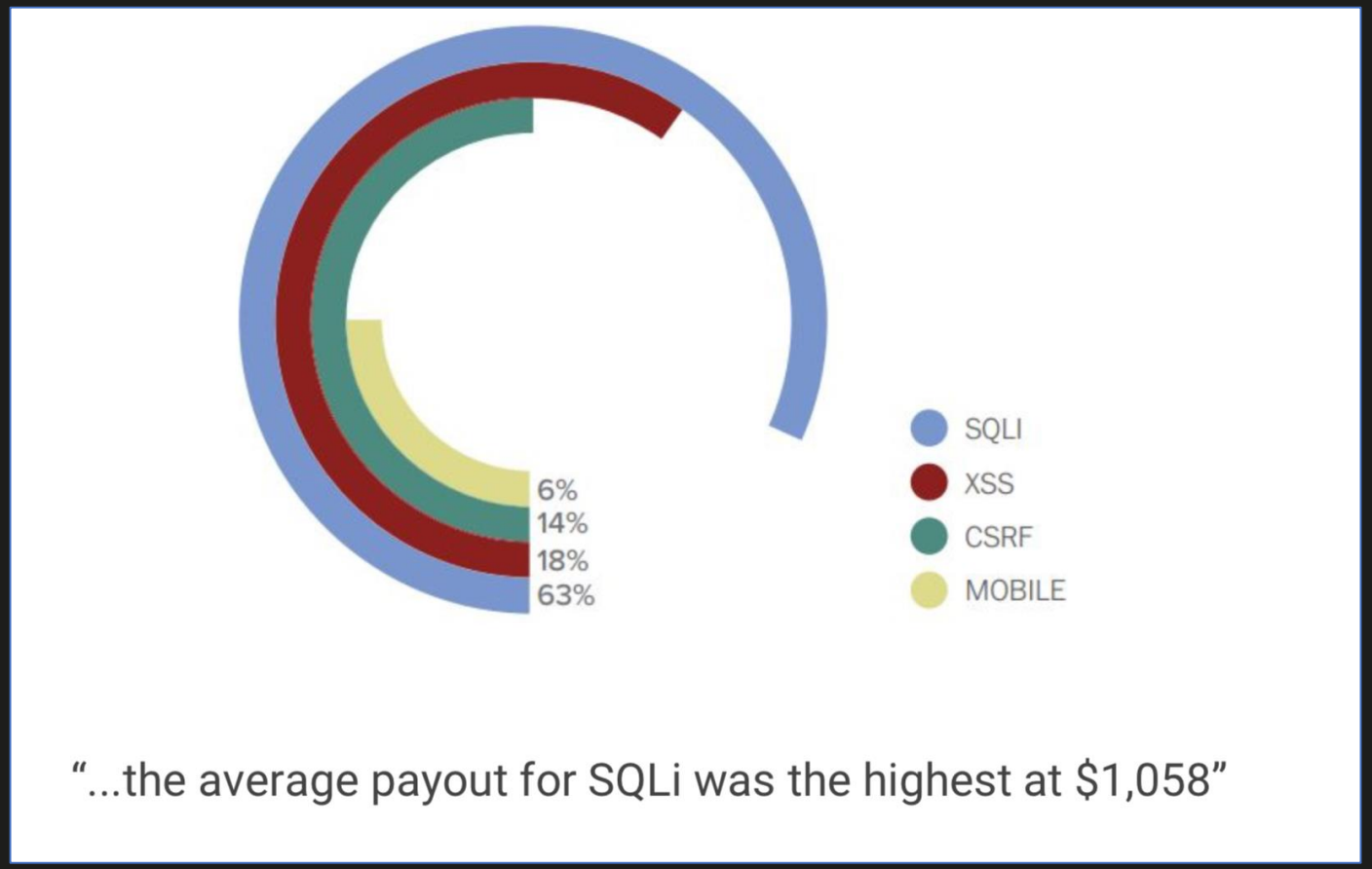


In terms of data theft, web application attacks leveraging poor validation of inputs or stolen credentials came top. But it's not just the theft of data you need to worry about. Denial of service attacks can have serious consequences, including preventing transactions being processed and slowing down your website and in-store systems.

"How" as "46% Hacking" has significance in DBIR Report

Akamai
Experience the Edge

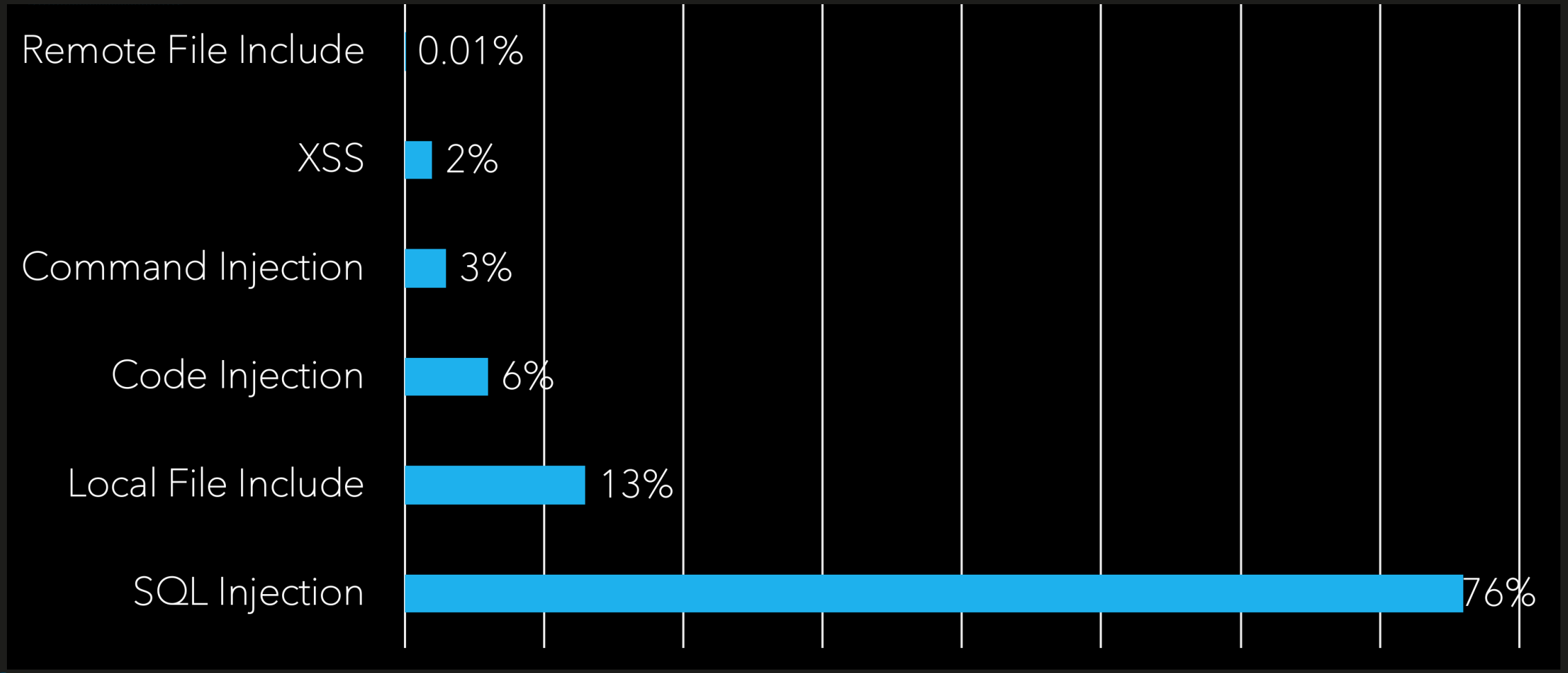
Bug Bounty Report 2017



SQL Injection been top vulnerability been identified in general

APPLICATION LAYER API ATTACKS

Akamai
eCommerce Seminar



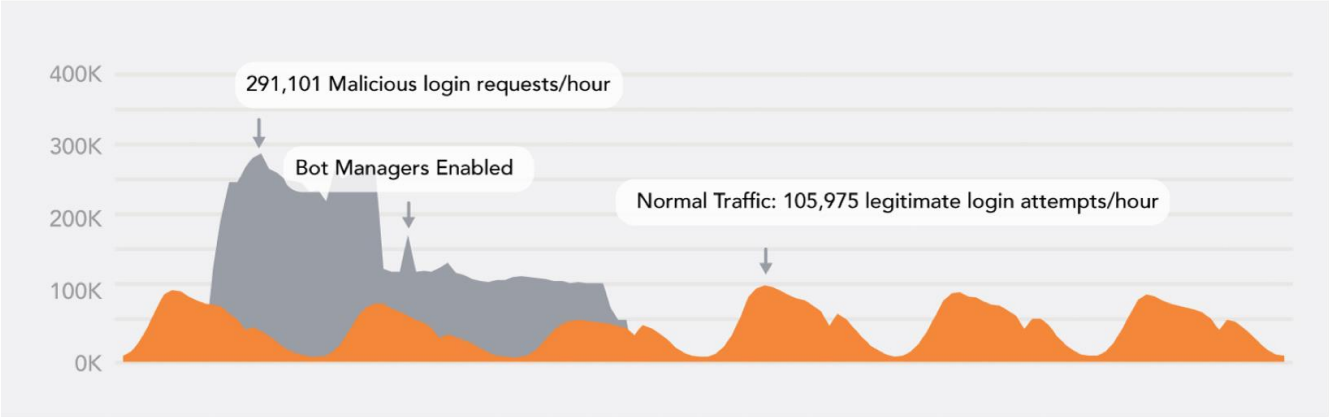
Akamai
Experience the Edge

SQL Injection Tops the League

Credential Stuffing Attacks

Akamai
eCommerce Seminar

Highly Distributed Attack



Top user agent

95% of all bot requests gave the Samsung Galaxy SM-G531H smartphone as the user agent

Top IP address

The top IP was responsible for **0.7%** of the login requests seen in this highly distributed attack

Top countries

Credential stuffing attack against a login endpoint for a Fortune 500 financial services institution

Human logins
6,947,896

Malicious logins
8,502,762

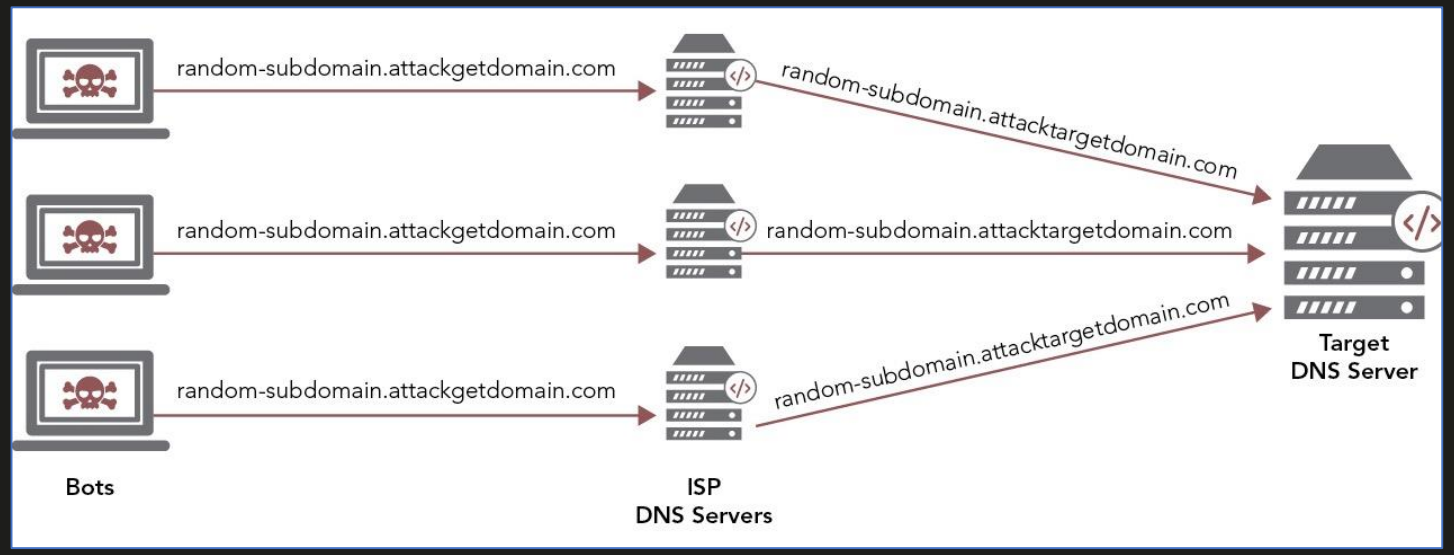
IP addresses
10,000+

ASNs
4923

User agents
9,999

Akamai
Experience the Edge

Mirai DNS Water Torture Attack




```
    1 0.000000  192.168.56.102  192.168.56.104  DNS   81 Standard query 0x79f2 A we4ongq6pgt3.demo.com
    2 0.000026  192.168.56.102  192.168.56.104  DNS   81 Standard query 0xaa97 A w8gemv41aj33.demo.com
    3 0.000029  192.168.56.102  192.168.56.104  DNS   81 Standard query 0x3157 A d5agf3tb1dok.demo.com
    4 0.000030  192.168.56.102  192.168.56.104  DNS   81 Standard query 0xa20e A tg8darf8vemb.demo.com
    5 0.000396  192.168.56.104  192.168.56.102  DNS  122 Standard query response 0x79f2 No such name A we4ongq6pgt3.demo.com SOA demo.com
    6 0.000445  192.168.56.104  192.168.56.102  DNS  122 Standard query response 0xaa97 No such name A w8gemv41aj33.demo.com SOA demo.com
    7 0.000479  192.168.56.104  192.168.56.102  DNS  122 Standard query response 0x3157 No such name A d5agf3tb1dok.demo.com SOA demo.com
    8 0.000514  192.168.56.104  192.168.56.102  DNS  122 Standard query response 0xa20e No such name A tg8darf8vemb.demo.com SOA demo.com
```

Mirai DNS attack queries with random subdomains are sent from bots to their local DNS servers. When the DNS servers can't find the subdomain, they send the query on to the target authoritative server.

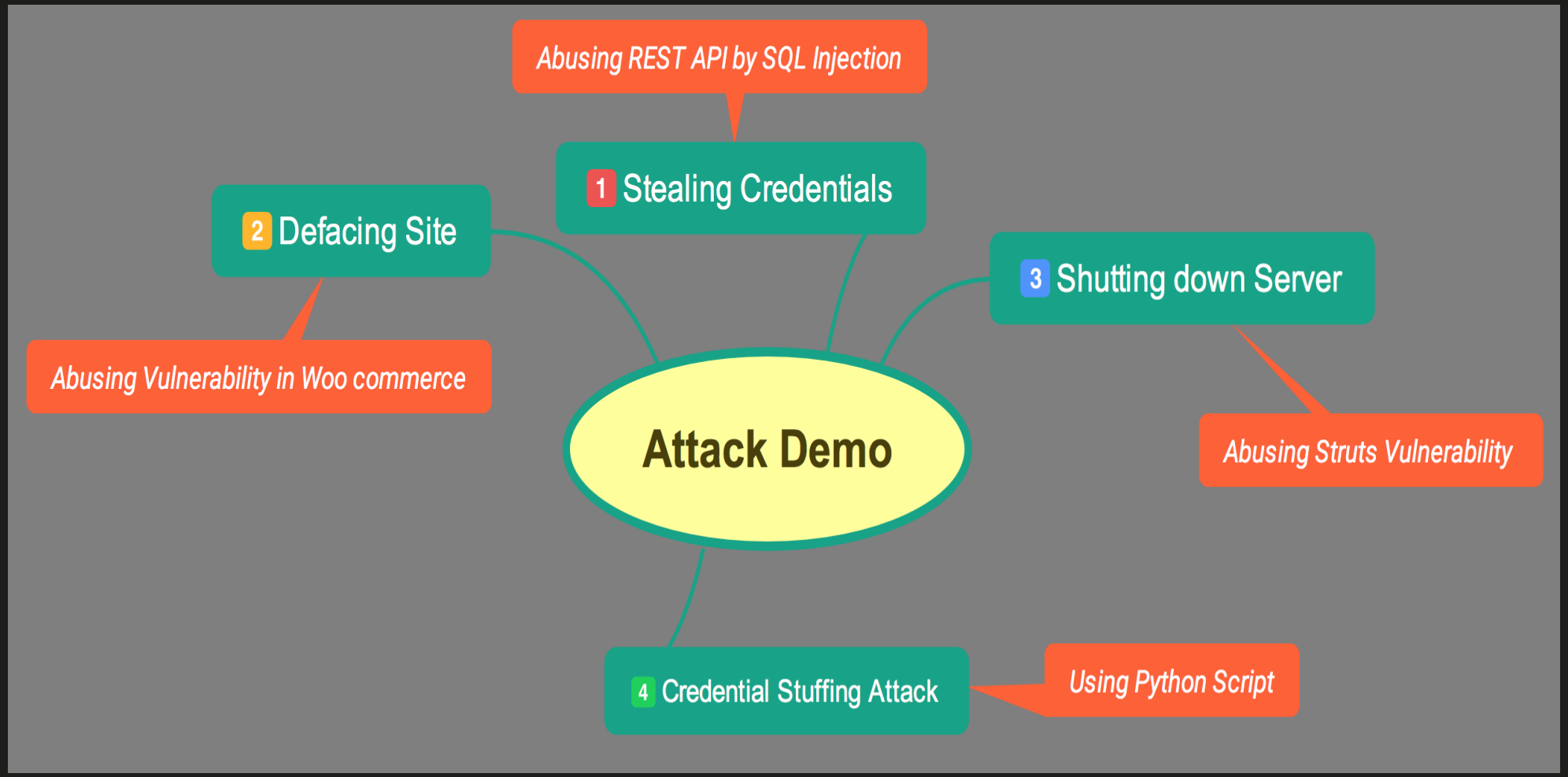
Akamai

eCommerce Seminar

Demonstrating Live Cyber Attacks

Akamai
Experience the Edge

Attack Demo


Abusing REST API by SQL Injection
1 Stealing Credentials
2 Defacing Site
Abusing Vulnerability in Woo commerce
3 Shutting down Server
Abusing Struts Vulnerability
Attack Demo
4 Credential Stuffing Attack
Using Python Script

Defacing Web Site: Abusing Vulnerability

Akamai
eCommerce Seminar

Site Defacement by Blog ID

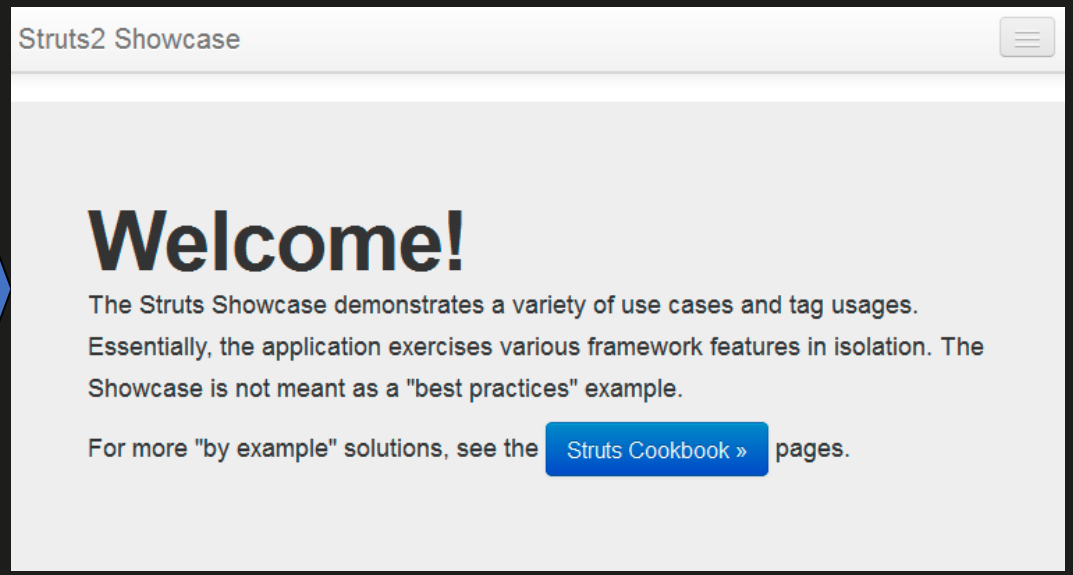
Attack Tools: python script
Target Application: Woo Commerce

Akamai
Experience the Edge

Shutting Down Entire Server: Abusing Struts Vulnerability

Akamai
eCommerce Seminar

Remote Command Execution



Attack Tools: python script
Target Application : Struts Showcase Application

Akamai
Experience the Edge

Credential Stuffing Attack against Login Page

Akamai
eCommerce Seminar


```
1 cred1:pass1
2 cred2:pass2
3 cred3:pass3
4 cred4:pass4
5 cred5:pass5
6 cred6:pass6
7 cred7:pass7
8 cred8:pass8
9 cred6:pass6
10 cred7:pass7
11 cred8:pass8
```

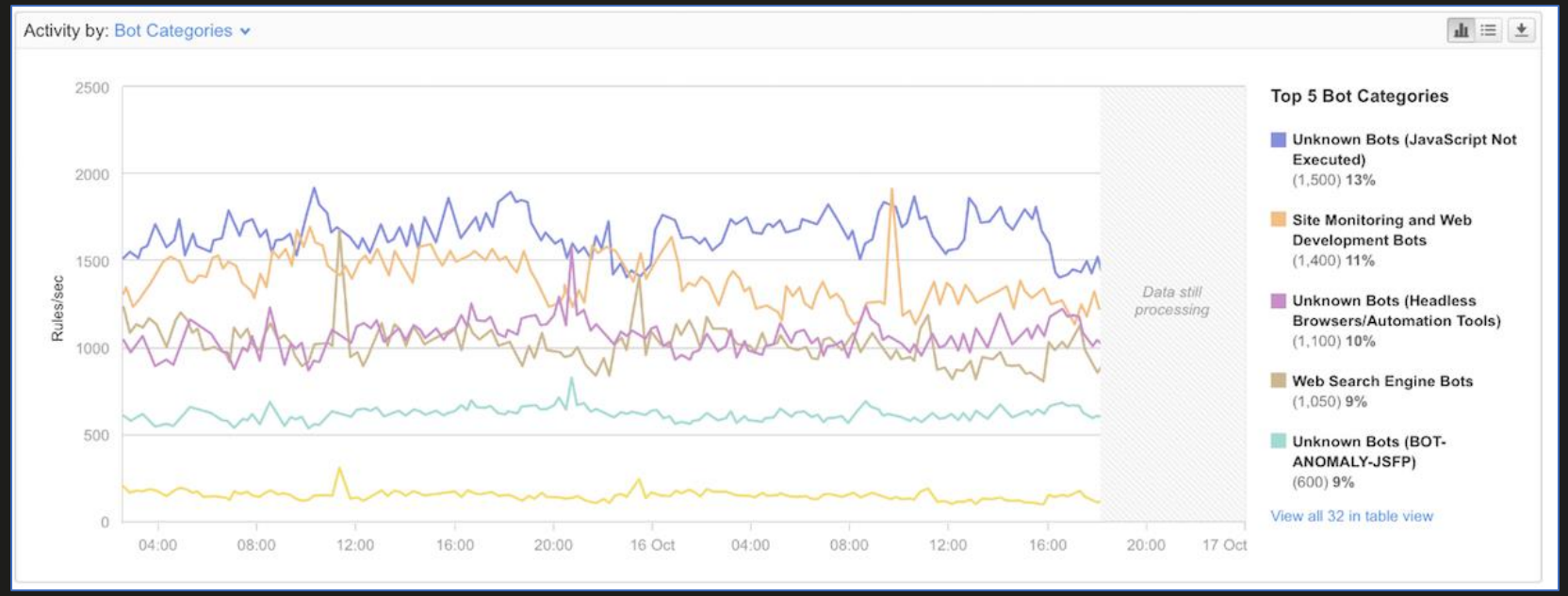
Credential Stuffing Attacks

Attack Tools: python script
Target Application : PHP Login Page

Akamai
Experience the Edge

Bot manager Credential Stuffing Report

Akamai
eCommerce Seminar



Akamai
Experience the Edge

Akamai

eCommerce Seminar

Deep Diving Reasons of Success of few Attacks

Akamai
Experience the Edge

Demonstrating Live Protection

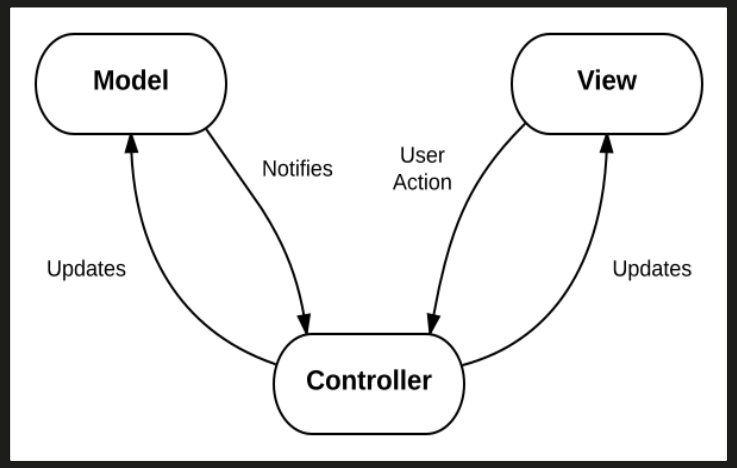
Akamai
eCommerce Seminar

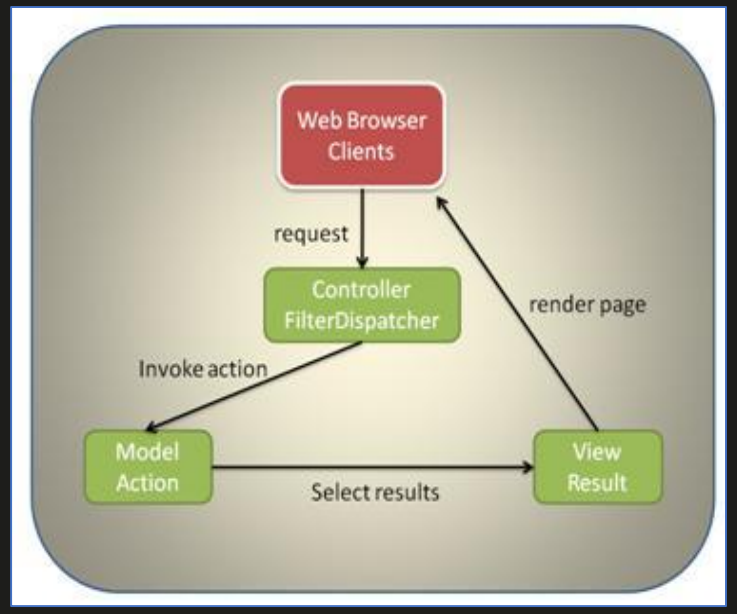
3000063	AKAMAI/WEB_ATTACK/WORDPRESS	id=303abcd-content=Lets have fun	Wordpress wp-json Attack Attempt - non-integer character(s) in ID parameter paylaod	deny

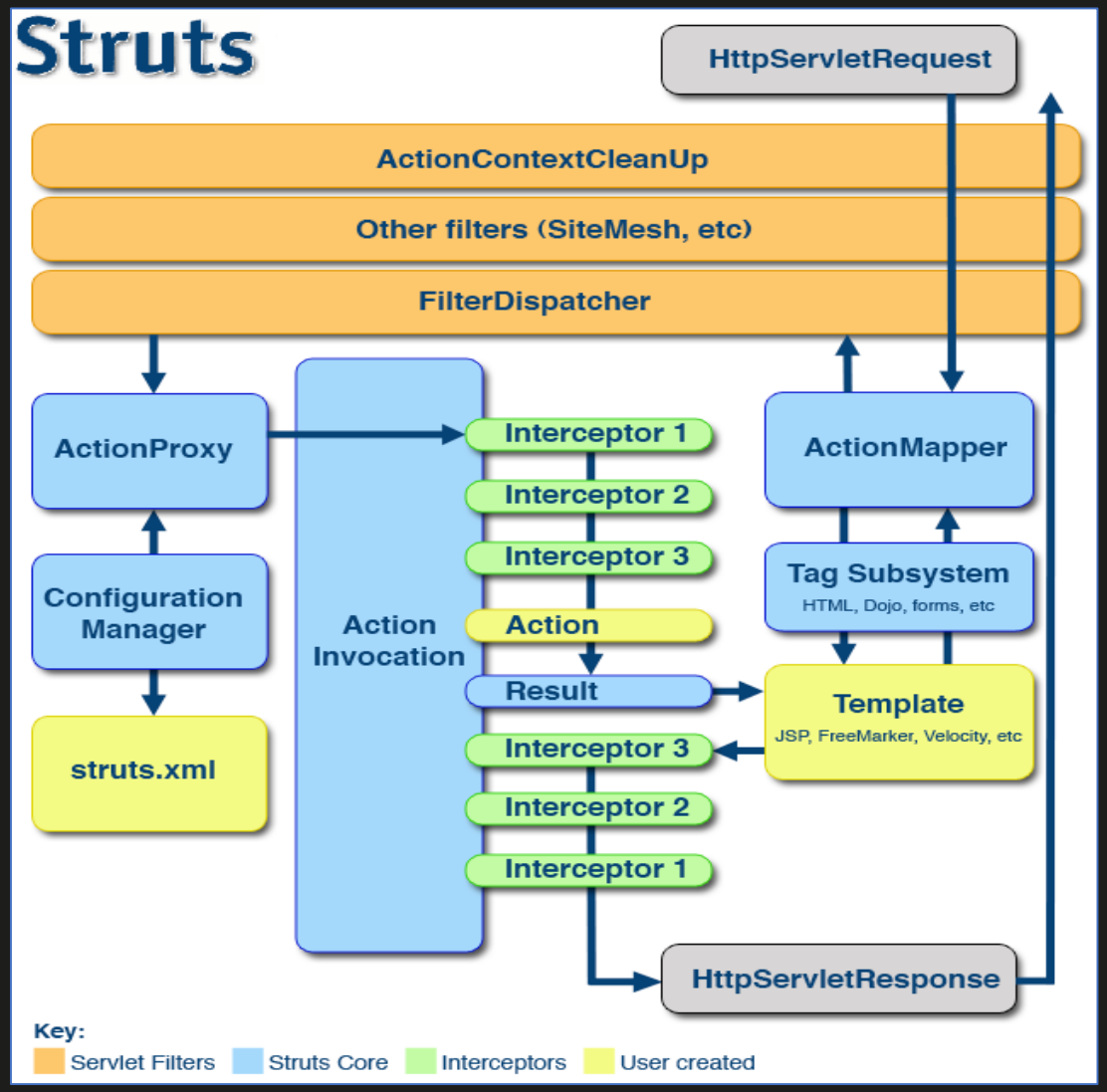
Akamai Security Rule of "3990001" is capable to detect and Protect from Content Injection/Code Injection Vulnerability

Akamai
Experience the Edge

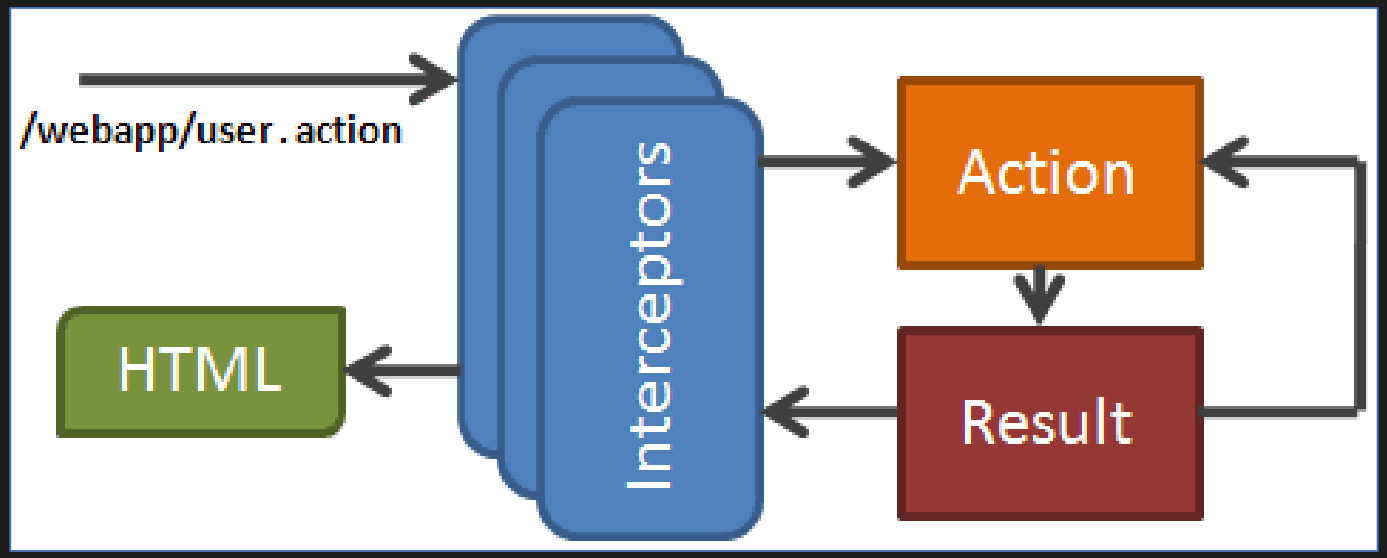
Apache Struts Framework: Model View Controller Architecture







Struts Interceptor: File Upload Interceptor



Struts2 uploads using the default *org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest* class and by configuring the *struts.multipart.parser* property, you can specify a different parsing class.

> *As per documentation, struts.multipart.parser used by the fileUpload interceptor to handle HTTP POST requests, encoded using the MIME-type multipart/form-data, can be changed out. Currently there are two choices, jakarta and pell. The jakarta parser is a standard part of the Struts 2 framework needing only its required libraries added to a project. As from Struts version 2.3.18 a new implementation of MultiPartRequest was added – JakartaStreamMultiPartRequest. It can be used to handle large files.*

https://blog.qualys.com/securitylabs/2017/03/14/apache-struts-cve-2017-5638-vulnerability-and-the-qualys-solution

Demonstrating Live Protection

Akamai
eCommerce Seminar

▼ Rules

RULE	TAG	SELECTOR	USER DATA	MESSAGE	ACTION
3000014	AKAMAI/WEB_ATTACK/OGNL_INJECTION	REQUEST_HEADERS:Content-Type	%{(#_='multipart/form-data'). (#dm=@ognl.ognlcontext@default_member_access).(#_memberaccess? (#_memberaccess=#dm): ((#container=#context['com.opensymphony.xwork2.actioncontext.container'] (#ognlutil=#container.getinstance(@com.opensymphony.xwork2.ognl.ognluti (#ognlutil.getexcludedpackagenames().clear()). (#ognlutil.getexcludedclasses().clear()). (#context.setmemberaccess(#dm))))).(#cmd='cat/etc/passwd').(#iswin= (@java.lang.system@getproperty('os.name').tolowercase().contains('win'))). (#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})). (#p=newjava.lang.processbuilder(#cmds)).(#p.redirecterrorstream(true)). (#process=#p.start()).(#ros= (@org.apache.struts2.servletactioncontext@getresponse().getoutputstream((@org.apache.commons.io.ioutils@copy(#process.getinputstream(),#ros)). (#ros.flush())}	Apache Struts Remote Command Execution (OGNL Injection)	alert
3900000	AKAMAI/BOT/REQUEST_ANOMALY	&REQUEST_HEADERS:Accept-Language		Missing Accept-Language Header	monitor

Akamai Security Rule of "3000014" is capable to detect and Protect from CVE-2017-5638

Akamai
Experience the Edge

Attacks so far & Protections from Akamai

Akamai
eCommerce Seminar

Attack ID	Attack Name	Protections
Attack1	Stealing Credential by SQLi	*Kona Site Defender(KSD)*
Attack2	Site Defacement	*Kona Site Defender(KSD)*
Attack3	Shutting down server	*Kona Site Defender(KSD)*
Attack4	Credential Stuffing	*Bot Manager Premier*
Attack5	DDoS(Water torture) Attacks	*Fast DNS & Prolexic*

Akamai
Experience the Edge

Akamai

eCommerce Seminar

Akamai Security Solutions

Akamai
Experience the Edge

Akamai
eCommerce Seminar

Akamai Security History

20년 – DDoS 및 웹공격 방어

44+ 회 – 일일 평균 DDoS 방어수

2017년 1년 총 공격방어수 15,965회(1일 평균 44회)
2017년 Q4 총 공격방어수 4,364회(1일 평균 48회)

65+ Tbps - 플랫폼상의 트래픽 기록

1.35 Tbps - 단일 규모 최대 DDoS 방어용량

보안 시장에서의 아카마이

Akamai
eCommerce Seminar

TOP 리서치 기관에 의한 평가

Gartner Gartner

아카마이 : 웹방화벽 리더

Named a LEADER in
Gartner's *Magic Quadrant for Web Application Firewalls, Q4 2017*

Forrester FORRESTER

아카마이 : 웹방화벽/디도스/봇 분야에서 리더

Named a LEADER in:

- *The Forrester Wave™: Web Application Firewalls, Q2 2018*
- *The Forrester Wave™: DDoS Mitigation Solutions, Q4 2017*
- *The Forrester New Wave™: Bot Management, Q3 2018*

Frost & Sullivan FROST & SULLIVAN

아카마이 : 봇 위험 관리 리더

MARKET LEADERSHIP AWARD for:

- *2018 Global Holistic Web Protection*
- *2018 Global Bot Risk Management*

Akamai has had the strongest and broadest Edge Security offering for quite some time…

—Source: IDC, Akamai: Cloud Content Delivery and Security Services Vendor Profile, #EMEA44060518, July 2018

Akamai
Experience the Edge

웹방화벽(WAF) 최상위 리더

Akamai
eCommerce Seminar

Forrester Wave™: Web Application Firewalls Scorecard, Q2, 2018

	Forrester's weighting	Akamai Technologies	Amazon Web Services	Barracuda Networks	Cloudflare	F5 Networks	Fortinet	Imperva Incapsula	Imperva SecureSphere	Positive Technologies	Radware	Rohde & Schwarz Cybersecurity
Current Offering	50%	3.85	1.24	2.91	2.65	3.83	2.50	3.48	2.58	2.34	3.30	2.22
Attack detection	25%	4.20	1.00	2.90	2.40	4.30	2.40	2.90	3.90	2.80	3.70	3.00
Attack response	30%	3.80	1.00	3.60	3.80	5.00	3.60	4.40	1.60	1.60	3.60	2.40
Management interface	10%	3.60	2.60	2.30	1.50	2.10	2.10	2.90	3.60	2.00	3.10	2.30
Zero-day attacks	20%	5.00	1.40	2.60	3.00	3.00	1.40	4.20	1.40	3.00	3.00	1.00
Reporting and analytics	10%	2.20	1.00	1.80	1.00	3.00	1.80	2.20	3.00	2.20	1.80	1.80
Feedback loops	5%	1.60	1.00	3.40	1.20	2.80	3.00	1.60	3.60	2.80	4.00	2.80
Strategy	50%	4.30	1.40	3.00	2.10	3.50	2.20	3.60	4.10	2.10	3.00	3.60
Product strategy	50%	3.80	1.80	3.00	2.20	3.40	2.20	3.40	4.20	3.00	2.20	3.40
Market approach	25%	5.00	1.00	3.00	3.00	3.00	3.00	5.00	5.00	1.00	5.00	5.00
Execution road map	20%	5.00	1.00	3.00	1.00	5.00	1.00	3.00	3.00	1.00	3.00	3.00
Training	5%	3.00	1.00	3.00	1.00	1.00	3.00	1.00	3.00	3.00	1.00	1.00
Market Presence	0%	4.46	2.60	2.80	4.42	4.48	3.12	2.94	2.62	2.90	1.50	1.32
Install base	60%	4.60	1.00	3.00	4.20	4.80	3.20	3.40	3.20	2.00	2.00	1.20
Growth rate	10%	2.00	5.00	1.00	4.00	1.00	3.00	3.00	1.00	5.00	3.00	0.00
Corporate profitability	30%	5.00	5.00	3.00	5.00	5.00	3.00	2.00	2.00	4.00	0.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Wave™: 웹방화벽(WAF)평가, Q2 2018

Akamai
Experience the Edge

아카마이 클라우드 보안 방어

Akamai
eCommerce Seminar

DNS 공격

정상 사용자

DDoS 공격(L3/4/7)

웹 애플리케이션 공격
API 공격

AKAMAI INTELLIGENT PLATFORM™
240,000+ servers | 19 scrubbing centers

고객 오리진
(IDC/클라우드)

아카마이 클라우드 보안 서비스

Akamai
eCommerce Seminar

멀티 레이어 방어 체제

- ✓ DNS 서버 공격
- ✓ 대용량 디도스 공격

Fast DNS
DNS 보안

Prolexic Routed/Proxy
디도스 전용 우회 서비스

- ✓ 웹 & API 취약점 공격
- ✓ L7 디도스 공격
- ✓ 제로데이 웹 취약점

Web Application Protector(WAP)
자동화된 방어(보안인력X)

Kona Site Defender(KSD)
커스터마이즈된 전문 보안 관리

Client Reputation
클라이언트 인텔리전스

- ✓ 봇 공격
- ✓ Web Scrapers/Aggregators
- ✓ Grey Marketers/Spam봇
- ✓ 크리덴셜 스터핑(계정탈취)

Bot Manager Std
봇 트래픽 가시성 확보(관리)

Bot Manager Premier
비정상 행위기반의 크리덴셜 스터핑 공격 방어(정보도용)

Akamai
Experience the Edge

Before Moving to Product: POC Concept

Akamai eCommerce Seminar

Step1: Sales Activity (Contract Processing)

1 Week

Step2:POC Settings

1 Week

Step3: Monitoring Period

3 Week

Step4: Creating Report

1 Week

Step5: Presenting Report

Total Six Weeks

Akamai Experience the Edge

Conclusions

Akamai
eCommerce Seminar

- New Attack Techniques Never Stops, will keep on evolving
- New Vulnerability keep on emerging
- Proof of Concept(POC) your Threat Landscape
- Make Decision on Security Investment after POC

Akamai
Experience the Edge

감사합니다!
Q&A