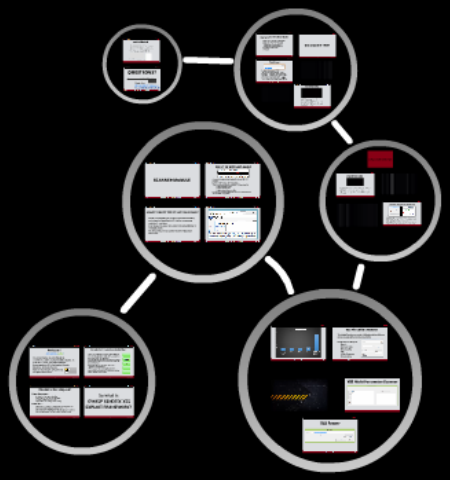
DETECTING AND EXPLOITING XSS WITH OWASP XENOTIX XSS EXPLOIT FRAMEWORK V3

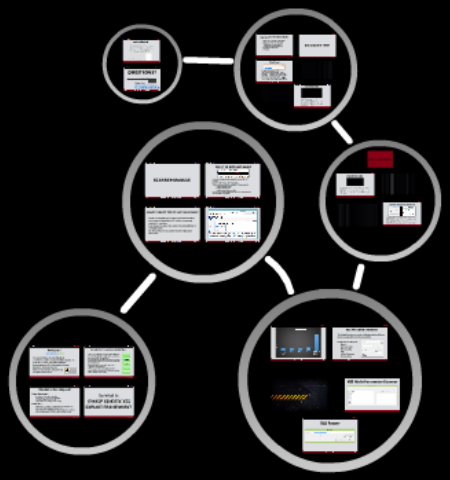
AJIN ABRAHAM
(><302)



nullcon security conference GOA

DETECTING AND EXPLOITING XSS WITH OWASP XENOTIX XSS EXPLOIT FRAMEWORK V3

AJIN ABRAHAM
(><302)



nullcon security conference GOA

#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.

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.

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?

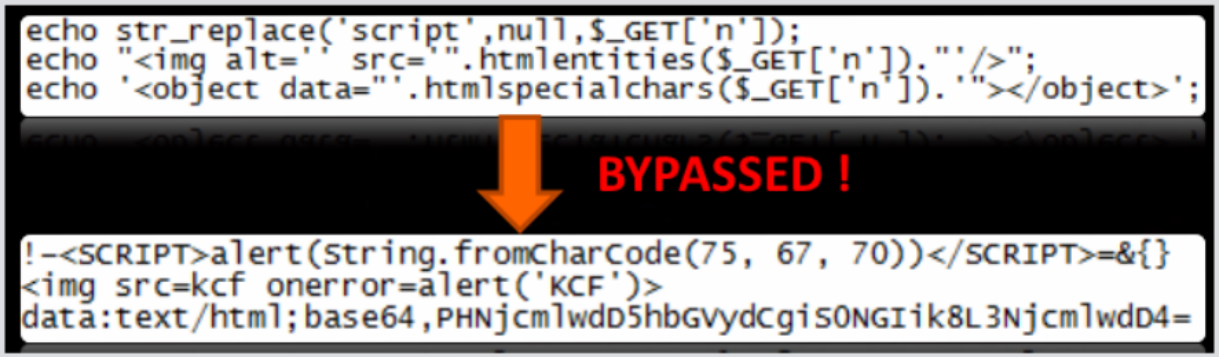

OWASP Xenotix XSS Exploit Framework 2013 v3
<< >> Refresh View Source Encoders XSS Keylogger XSS Executable Drive-by XSS Reverse Shell XSS DDoSer XSS Cookie Thief About
Payloads: 540
URL: http://
Parameter:
Select Test Mode
Inbuilt XSS Payloads
Custom XSS Payloads
<h1>Xenotix XSS</h1>
Manual Mode
Auto Mode
Multiple Parameter Scanner
XSS Fuzzer
https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework
Go
Log in / create account
OWASP
The Open Web Application Security Project
Page Discussion
Read View source View history
Go Search
Navigation
Home
News
OWASP Projects
Downloads
Local Chapters
OWASP Initiatives
Volunteer With OWASP
Global Committees
AppSec Job Board
OWASP Xenotix XSS Exploit Framework
Contents [hide]
1 Xenotix XSS Exploit Framework
2 Features of Xenotix XSS Exploit Framework
3 Support us on Facebook
4 White Paper
5 Videos
6 Download
7 IMPORTANT
Source
Done

OWASP XENOTIX XSS EXPLOIT FRAMEWORK

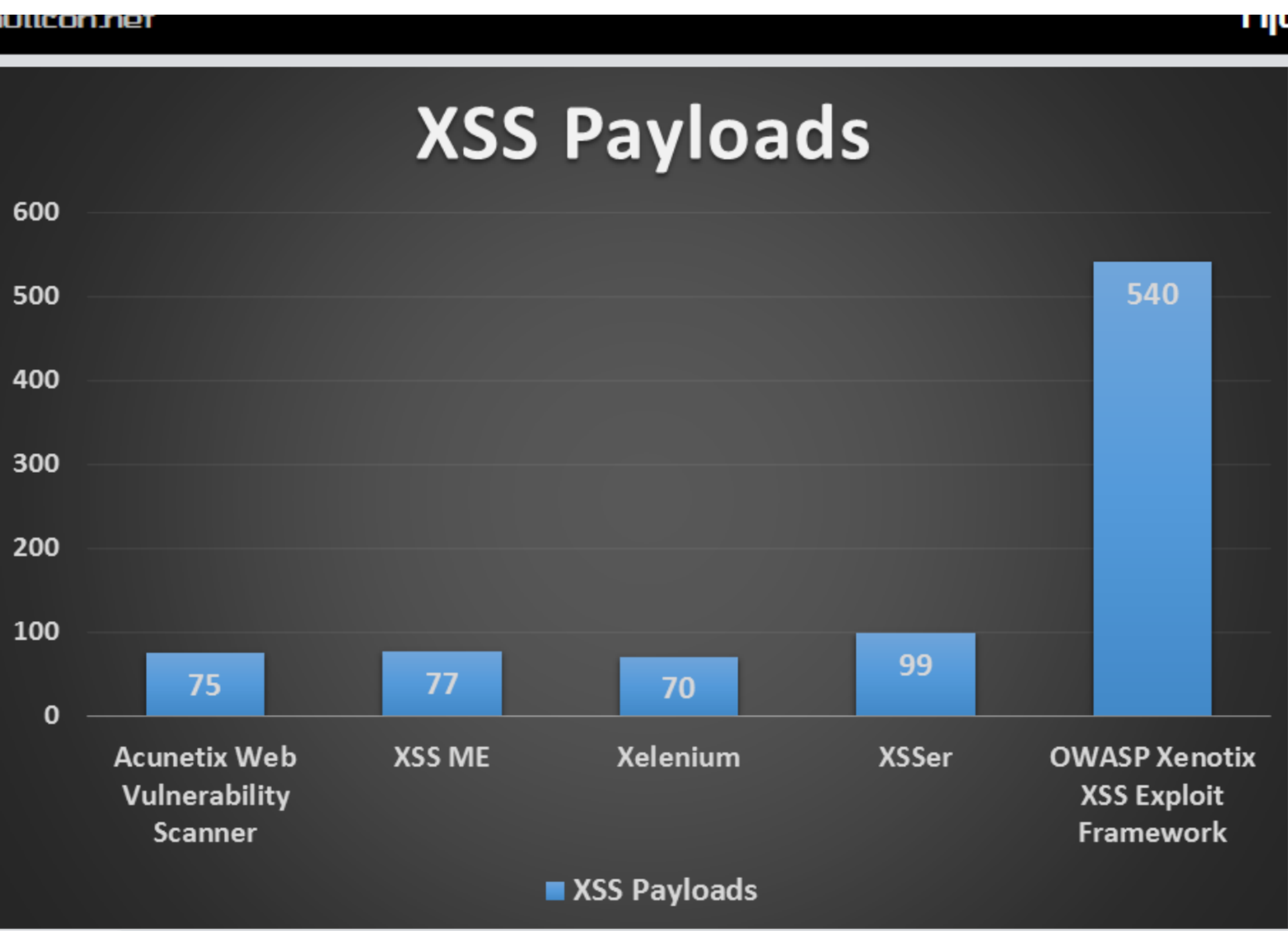
- Xenotix XSS Exploit Framework is a penetration testing tool written in Visual Basic.NET with it's components coded in C++ and Java.
- It can be used to detect and exploit XSS vulnerabilities in web applications.
- It is divided into an XSS Scanner and an Exploitation Framework.

SCANNER MODULE

BUILT IN XSS PAYLOADS



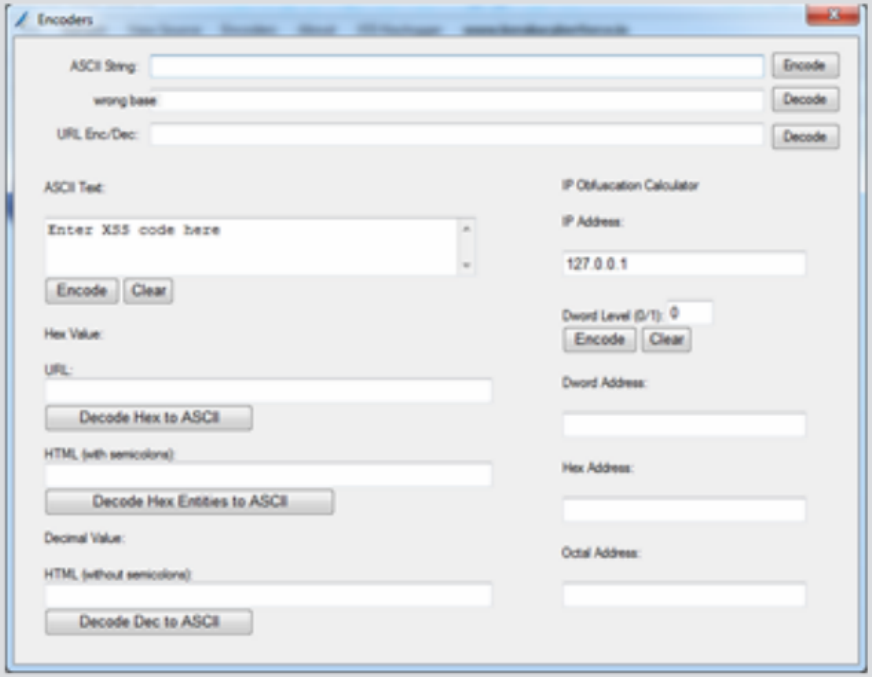
- Currently its having an inbuilt payload list of over 500+ XSS payloads.
- Includes HTML5 compactable XSS payloads.
- There are different methods available for XSS protection like
- Using String Replace filter.
- Using htmlentities filter.
- Using htmlspecialcharacters filter.
- Most of these weakly 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

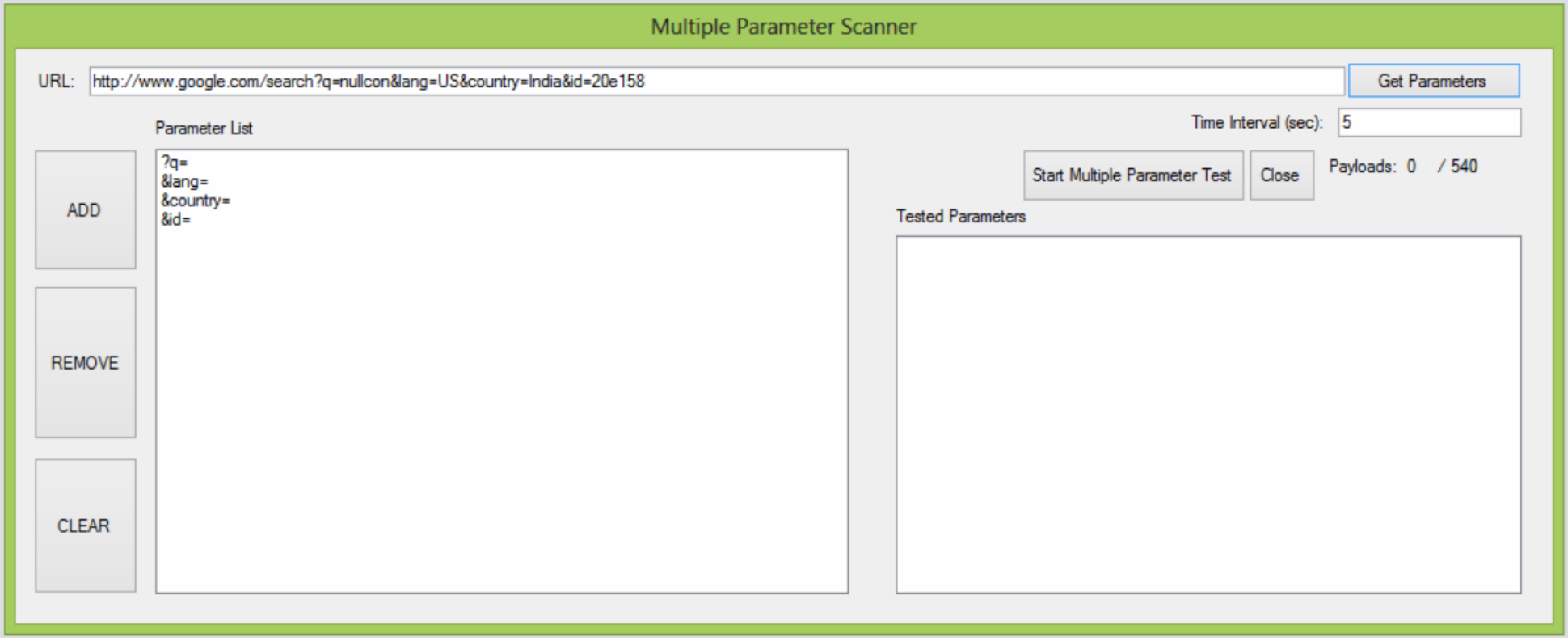
- The inbuilt Encoder can encode XSS payloads into different forms to bypass different filters and WAFs.

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

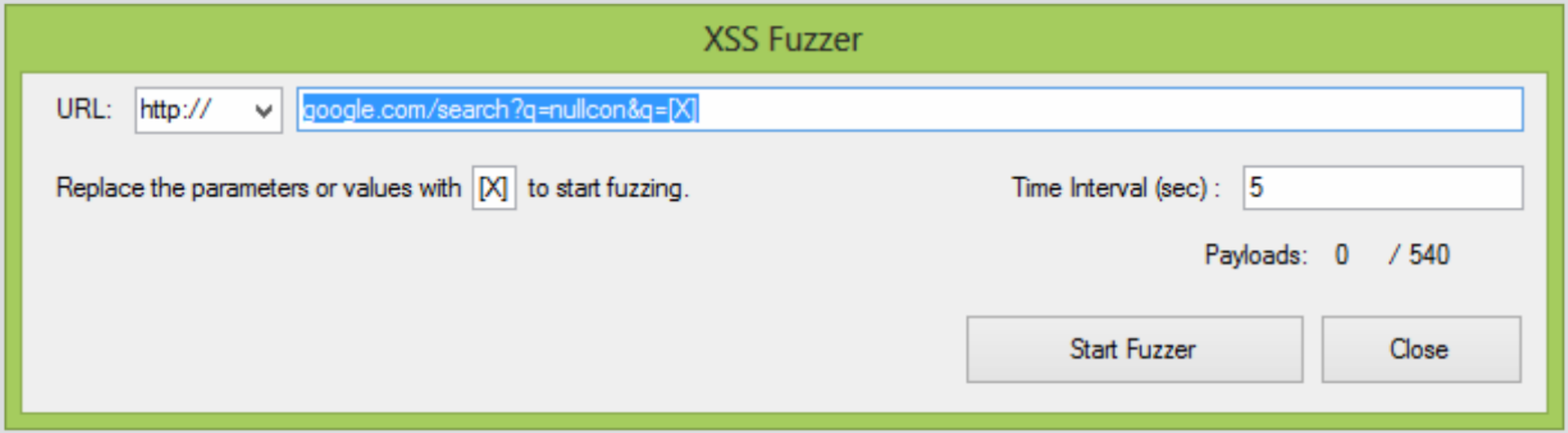


http://nullcon.net

XSS Multi Parameter Scanner

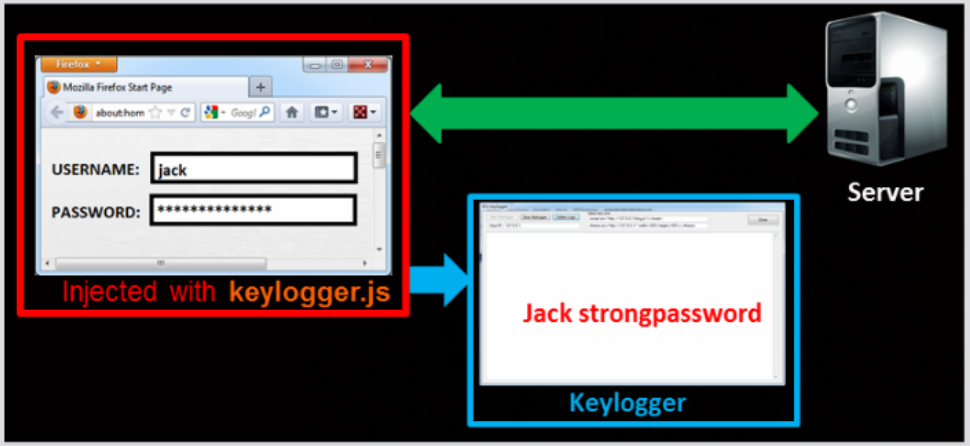


XSS Fuzzer



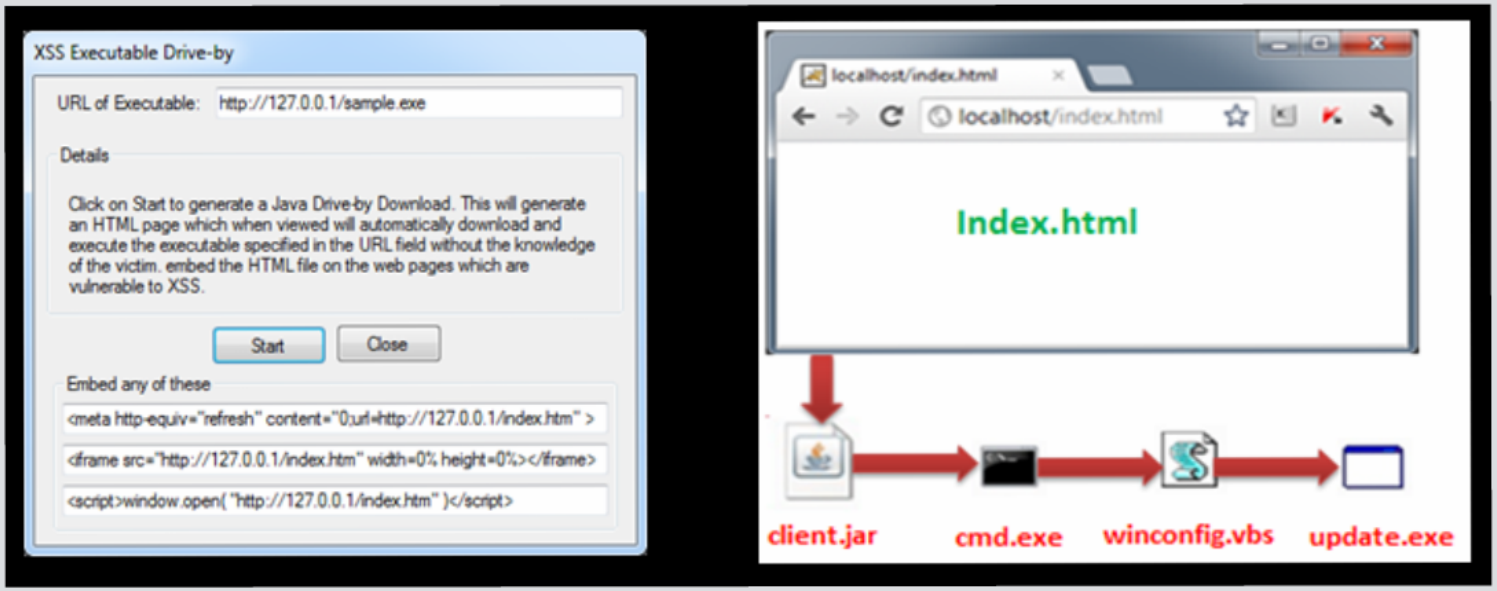
EXPLOTATION FRAMEWORK

XSS KEYLOGGER



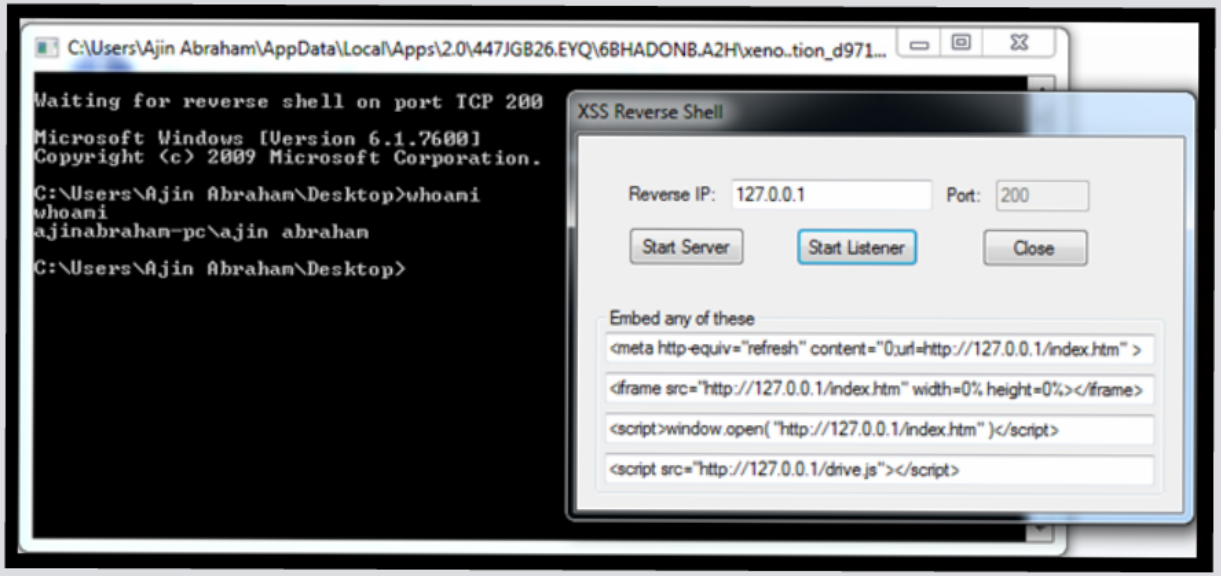
- It's having a Key logger feature implemented with JavaScript and PHP using QuickPHP Server.
- A vulnerable Web Application injected with a JavaScript file and presented to the victim.
- All the keystrokes made by the victim is send to the PHP file which logs it into a text file.

XSS EXECUTABLE DRIVE-BY DOWNLOADER



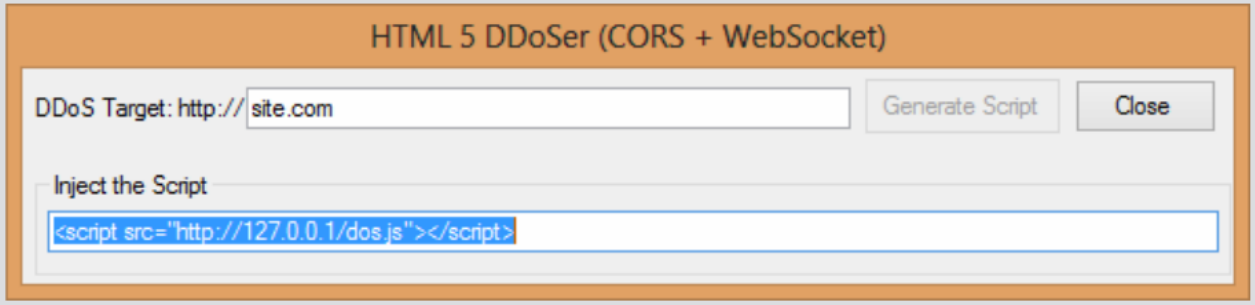
- Java Drive-by download can be implemented. JRE should be installed in the victims machine already.
- It allows the attacker to download a malicious executable file & run it on the victim's system without his knowledge and permission.
- Give the URL for your RAT, worm, virus etc. and then embed the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

XSS REVERSE SHELL



- 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



- 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

- So go for XSS hunting and grab your bounty .

QUESTIONS?

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

Thank You

ajin.abraham@owasp.org
fb.com/ajinabrahamofficial