Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University

Vulnerability assessment of university website

Two important website/web application/webserver vulnerability scanner tools on Kali Linux.

In this assessment I have used some important vulnerability scanning tools on kali Linux for assessment. I have also shared some screenshots of the results while using all the important commands.

Following are important terms before going to scanning part :-

Nikto: - It is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers.

Some features of Nikto:

1. SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
2. Full HTTP proxy support
3. Checks for outdated server components
4. Save reports in plain text, XML, HTML, NBE or CSV
5. Template engine to easily customize reports
6. Scan multiple ports on a server, or multiple servers via input file (including nmap output)
7. LibWhisker's IDS encoding techniques
8. Easily updated via command line
9. Identifies installed software via headers, favicons and files
10. Host authentication with Basic and NTLM

OWASP ZAP : It is an open-source web application security scanner. Owasp is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It can be used for professionals as well as new users.

Following are the features of OSWAP: -

Website Scanning assessment

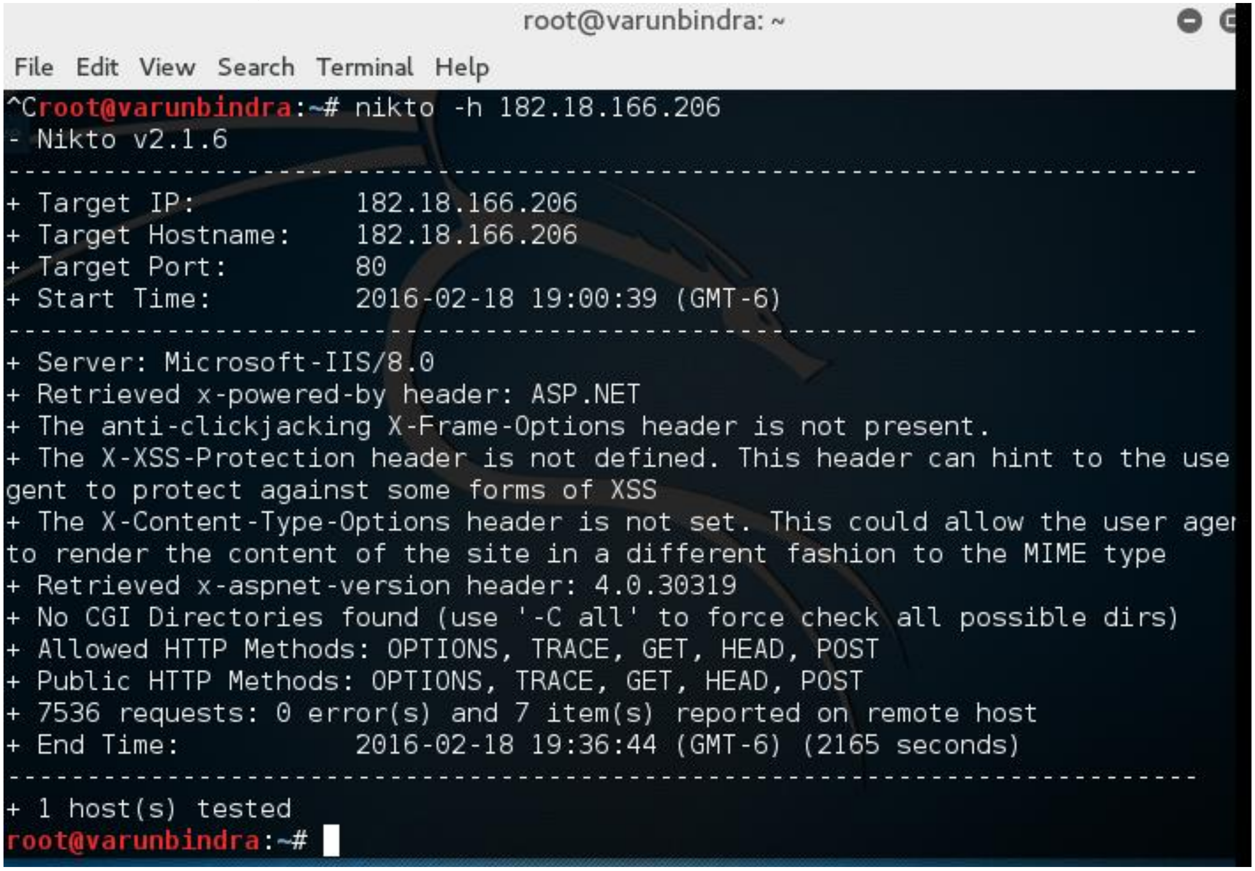
Varun Bindra
Management Information Systems
Texas A&M University

1. Intercepting Proxy
2. Automated Scanner
3. Passive Scanner
4. Brute Force Scanner
5. Fuzzer
6. Port Scanner
7. Spider
8. Web Sockets
9. REST API

Name of Website	URL	IP Address
Lucknow University	**http://www.lkouniv.ac.in**	**182.18.166.206**
UP Government:	**http://up.gov.in**	164.100.52.81

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University



```
^Croot@varunbindra:~# nikto -h 182.18.166.206
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          182.18.166.206
+ Target Hostname:    182.18.166.206
+ Target Port:        80
+ Start Time:         2016-02-18 19:00:39 (GMT-6)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user ager
to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7536 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2016-02-18 19:36:44 (GMT-6) (2165 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@varunbindra:~#
```

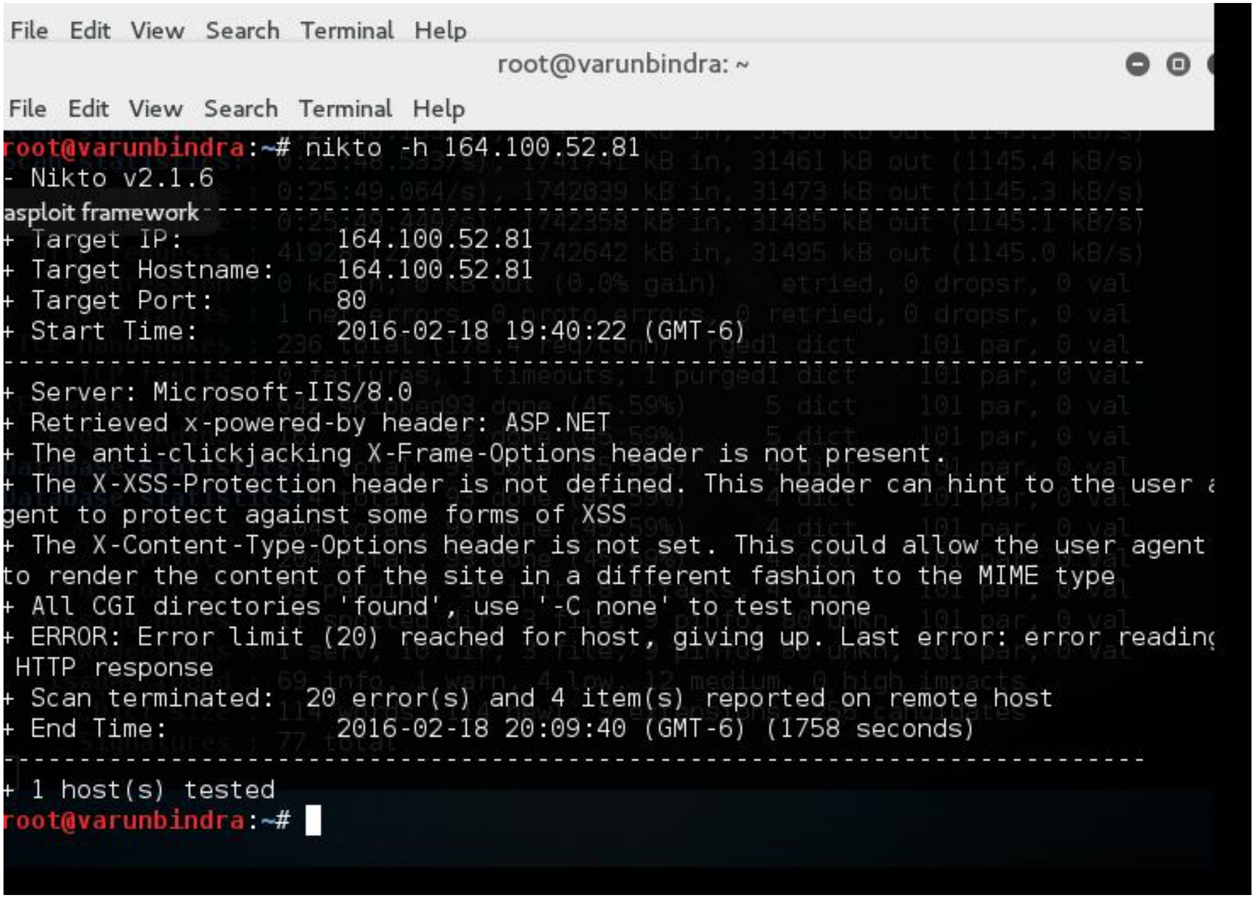
Using Nikto on -> UP Government: http://up.gov.in

IP address: - 164.100.52.81

Command: nikto –h 164.100.52.81

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University

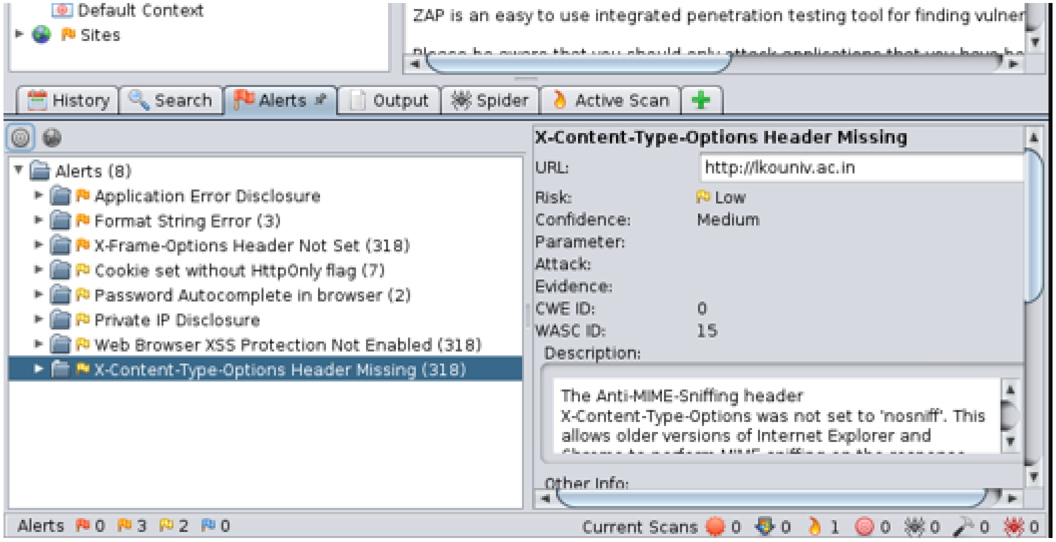

File Edit View Search Terminal Help
root@varunbindra: ~
File Edit View Search Terminal Help

```
root@varunbindra:~# nikto -h 164.100.52.81
- Nikto v2.1.6
asploit framework-------------------------------------------------------------
+ Target IP:          164.100.52.81
+ Target Hostname:    164.100.52.81
+ Target Port:        80
+ Start Time:         2016-02-18 19:40:22 (GMT-6)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading
 HTTP response
+ Scan terminated:  20 error(s) and 4 item(s) reported on remote host
+ End Time:           2016-02-18 20:09:40 (GMT-6) (1758 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@varunbindra:~#
```

Using OWASP on -> http://www.lkouniv.ac.in

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University



ZAP is an easy to use integrated penetration testing tool for finding vulner

- Alerts (8)
  - Application Error Disclosure
  - Format String Error (3)
  - X-Frame-Options Header Not Set (318)
  - Cookie set without HttpOnly flag (7)
  - Password Autocomplete in browser (2)
  - Private IP Disclosure
  - Web Browser XSS Protection Not Enabled (318)
  - X-Content-Type-Options Header Missing (318)

X-Content-Type-Options Header Missing

URL:	http://lkouniv.ac.in
Risk:	Low
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	
CWE ID:	0
WASC ID:	15

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and

Other Info:

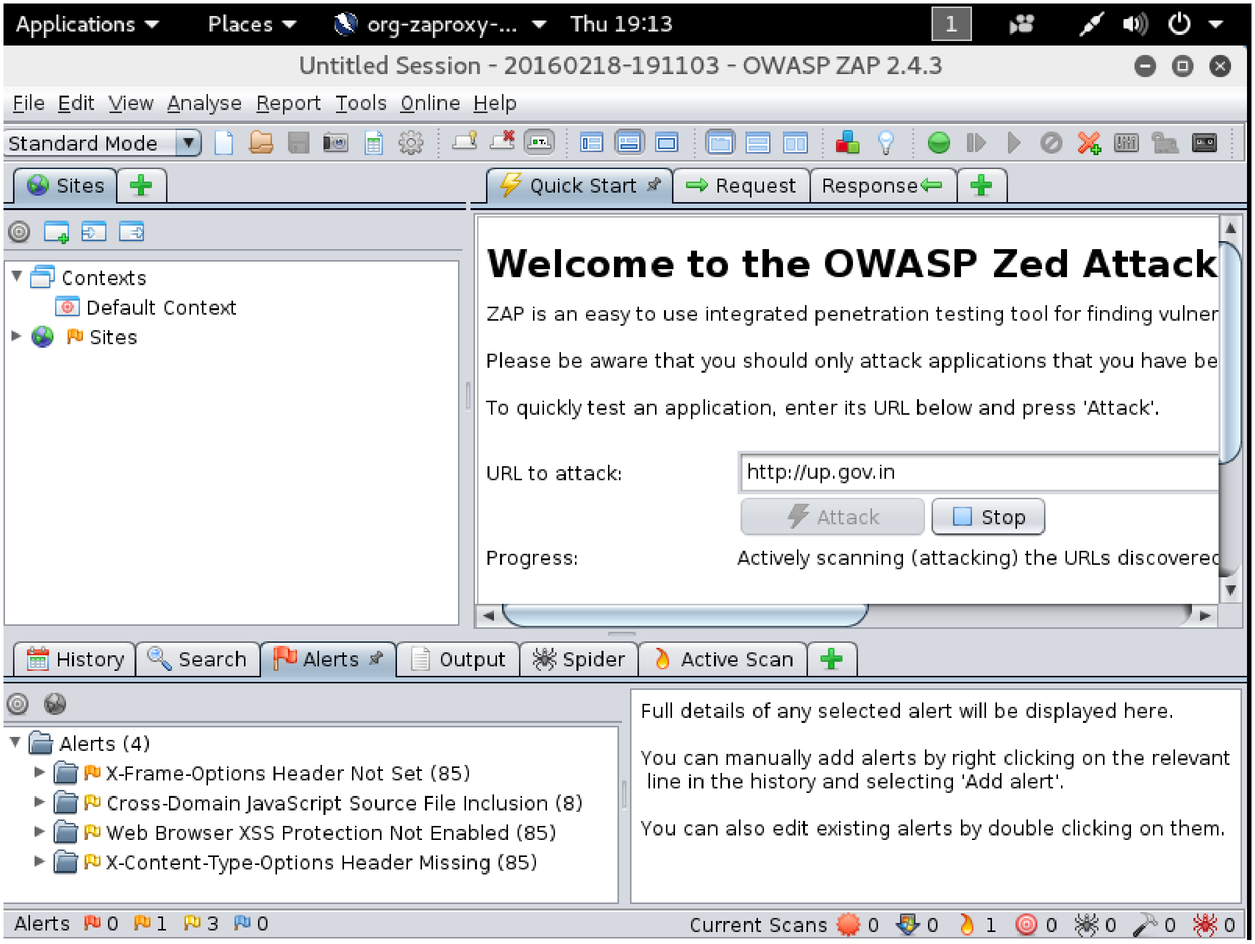
Alerts 0 3 2 0 Current Scans 0 0 1 0 0 0 0

Using OWASP on -> http://up.gov.in

IP address: - 164.100.52.81

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University



Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulner

Please be aware that you should only attack applications that you have be

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://up.gov.in

Progress: Actively scanning (attacking) the URLs discovered

Alerts (4)
- X-Frame-Options Header Not Set (85)
- Cross-Domain JavaScript Source File Inclusion (8)
- Web Browser XSS Protection Not Enabled (85)
- X-Content-Type-Options Header Missing (85)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University

Difference between OWASP and Nikto

OWASP	Nikto
QWASP is detailed description of vulnerabilities	Less detailed
Graphical application so it is easy to check	Command shell is used
Any security issue is in Alert tab	Security issue is in main screen (terminal)
Each folder contains different security and the file path is also defined.	

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University

Following were the loopholes which were discovered during scanning of both the websites. Below is some basic detail of what are the types of vulnerabilities found during scanning.

1) **X-frame-options header not set owasp:**

It is the uncommon kind of attack. The attacker either uses a happy link to send message to the user or makes sure the visitor is logged into the site by social engineering. Henceforth, when the user will browse his mail, if he accidently hits the link, the click jacks up many variants. Therefore, the use of X-Frame-Options at pages is recommended, since they do not run into a frame. The older frame busting method is less effective, but useful for older browsers, like IE7.

2) **Cross domain JavaScript source file inclusion:**

This mode makes use of third party script files, which are beyond the web application control of the web application and as such may contain unexpected functionality. Herein, the attacker executes malicious scripts into authorized website or web application through client side code injection. This common error is vulnerable to web application and generally occurs when a web application makes use of invalidated user input within the output it generates. The hacker instead of targeting the victim directly targets and exploits the weakness of the website/web application to transfer the malicious script to the victim. The attacker in should find a way initially find a way to inject a payload into a web page that the victim visits then insert a string that will be used within the web page and treated as code by the victim's browser.

3) **X- content type option header is not set:**

This could allow the user agent to render the content of the site in a different fashion to the MIME type.

4) **Private IP address disclosure:**

The private IP addresses reveals a lot about the layout of the organizational network. And generally its best to avoid disclosing internal IP addresses in HTTP response headers. But actually load balancing devices, majority of web servers and web application reveal the same over the HTTP protocol.

Website Scanning assessment

Varun Bindra
Management Information Systems
Texas A&M University

5) Password autocomplete in browser:

Generally the browsers offer to save the passwords of the users and the users happily agree to save the same since the ease they are at whenever the same site is visited. Additionally some websites will offer custom remember me functionality to allow users to persist log on a specific client system. The hacker in this case attacks the network, steals the data and then accordingly misuses the data.

6) Format String Error:

This kind o error generally occurs when the submitted data of an input string is evaluated as a command by the application. In this case, the attacker could easily execute code, read the stack, or because segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system. execute code, read the stack, or because segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system

7) Application error disclosure:

Our web application has an error page that displays the absolute URL path and query of the page on which the error occurred, the date/time of the error, and the exception message.

8) Cookie without httponly flag set:

Generally, when a cookie is set with HTTPonly flag, the cookie can only be accessed by the server and not the client. The area of concern herein is the protection of the session cookie. Otherwise the attacker may access the cookie and fetch important data.

9) Web browser xss protection not enabled:

The XSS-Protection is a HTTP header understood by Internet. This header lets domains toggle on and off the XSS Filter of internet explorer, which prevents some categories of XSS attacks. IE8 has the filter activated by default, but servers can switch if off by setting. Hacker can exploit this vulnerability if the settings are switched off.