Timothy Kang
Assignment #3
ITMS 543-02

Vulnerability Assessment Report
Target: http://demo.testfire.net/

Contents

Executive Summary 2
Summary of Results 2
Attack Narrative 3
Nslookup 3
Nmap 3
Sparta (for confirmation) 4
Nikto 5
OpenVAS 7
Vega 8
OWASP 9
Of course…it works… Admin/Admin 10

Executive Summary

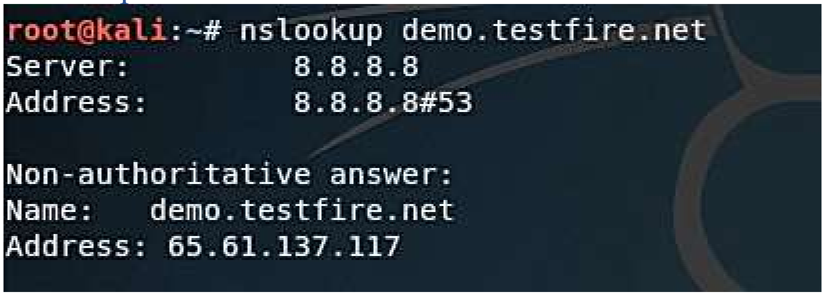
Timothy Kang was “contracted” by professor Kevin Vaccaro to create a vulnerability assessment report on the target http://demo.testfire.net/ without exploiting it. Series of tools were used for this assessment in order to identify any open ports and vulnerabilities, be it ones connected to those ports or to the code of the target. Based on how serious these vulnerabilities are, action is recommended.

Summary of Results

Multiple port scans were done to get an idea of what this target has to offer. From these scans, we can see 3 open ports and their versions. A tool called Sparta was used to further confirm these results. Now that this was done, Nikto was used to find vulnerabilities for each of these open ports. There were certain headers that were not set, defined, or present which can result in XSS attacks, content sniffing, and dangerous transmissions of sensitive information over HTTP. OpenVAS was used to find even more specific vulnerabilities and their possible fixes. Apache Tomcat, SSL/TLS, and other vulnerabilities were found. Some can be easily fixed with vendor provided software upgrades while others have workarounds or no fixes at all. Lastly, the coding vulnerabilities were observed using Vega and OWASP. The use of HTTP authentication and cleartext, cookies, XSS, and SQL injections are all vulnerabilities that can be found from this target’s code. Not to mention the fact that admin login credentials are unsurprisingly admin/admin. Clearly, there are many vulnerabilities of this target that can be exploited by an attacker. It is highly recommended that immediate action is taken.

Attack Narrative

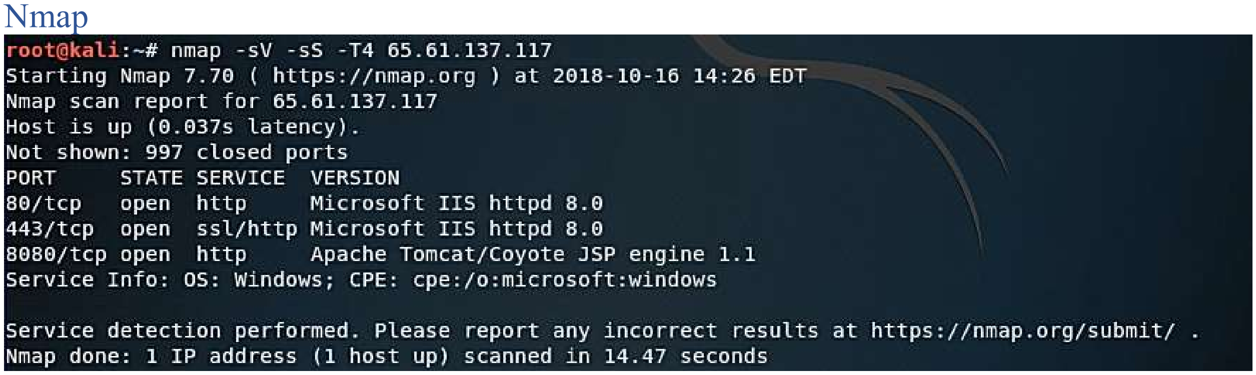
Nslookup



```
root@kali:~# nslookup demo.testfire.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   demo.testfire.net
Address: 65.61.137.117
```

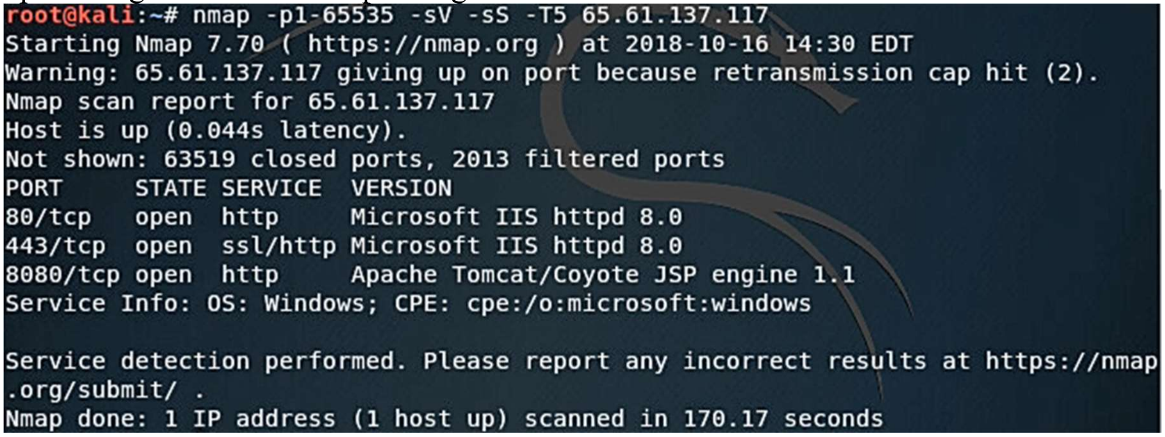
Since only the target's URL is given, I begin with a simple nslookup to find the IP address. This information will come in handy for certain commands and tools.

Nmap



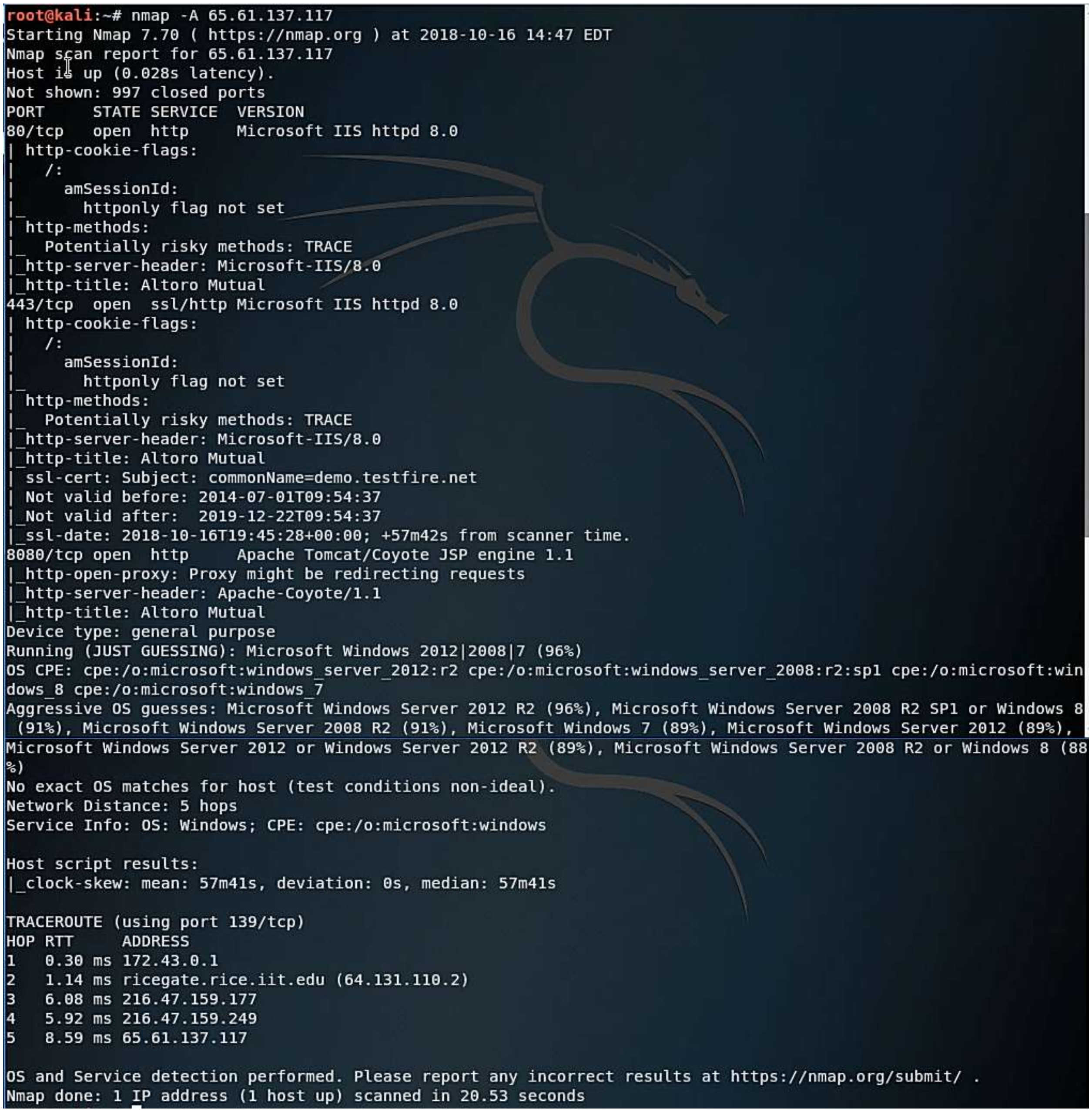
```
root@kali:~# nmap -sV -sS -T4 65.61.137.117
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-16 14:26 EDT
Nmap scan report for 65.61.137.117
Host is up (0.037s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Microsoft IIS httpd 8.0
443/tcp  open  ssl/http Microsoft IIS httpd 8.0
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
```

Now I can scan this target to scan the network for open ports using nmap. The options allow for TCP open ports along with version numbers to be displayed. One thing to note is that only the first 1000 pots have been scanned. Based on this scan, we can see that port 80, 443, and 8080 are open along with their corresponding versions.



```
root@kali:~# nmap -p1-65535 -sV -sS -T5 65.61.137.117
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-16 14:30 EDT
Warning: 65.61.137.117 giving up on port because retransmission cap hit (2).
Nmap scan report for 65.61.137.117
Host is up (0.044s latency).
Not shown: 63519 closed ports, 2013 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Microsoft IIS httpd 8.0
443/tcp  open  ssl/http Microsoft IIS httpd 8.0
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.17 seconds
```

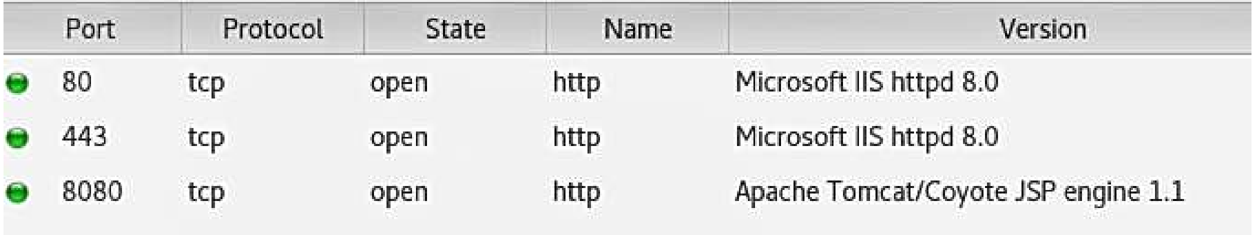
This nmap command will basically do the same thing as previous scan but will do a full scan where it scans 65535 ports. There does not seem to be any other open ports other than the ones listed before.



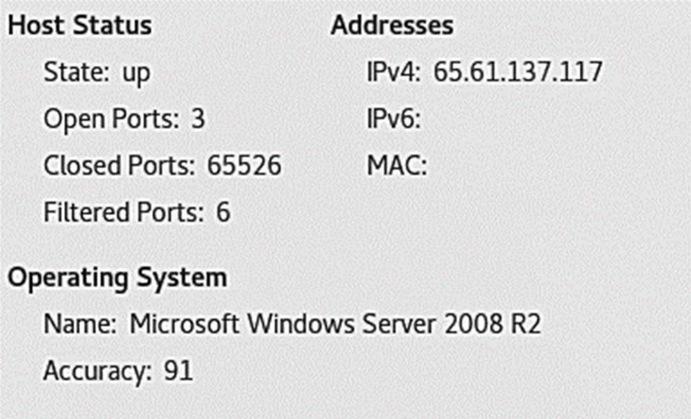
```
root@kali:~# nmap -A 65.61.137.117
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-16 14:47 EDT
Nmap scan report for 65.61.137.117
Host is up (0.028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Microsoft IIS httpd 8.0
| http-cookie-flags:
|   /:
|     amSessionId:
|_      httponly flag not set
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.0
|_http-title: Altoro Mutual
443/tcp  open  ssl/http Microsoft IIS httpd 8.0
| http-cookie-flags:
|   /:
|     amSessionId:
|_      httponly flag not set
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.0
|_http-title: Altoro Mutual
| ssl-cert: Subject: commonName=demo.testfire.net
| Not valid before: 2014-07-01T09:54:37
|_Not valid after:  2019-12-22T09:54:37
|_ssl-date: 2018-10-16T19:45:28+00:00; +57m42s from scanner time.
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2008|7 (96%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:win
dows_8 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (96%), Microsoft Windows Server 2008 R2 SP1 or Windows 8
 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 7 (89%), Microsoft Windows Server 2012 (89%),
Microsoft Windows Server 2012 or Windows Server 2012 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8 (88
%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 57m41s, deviation: 0s, median: 57m41s

TRACEROUTE (using port 139/tcp)
HOP RTT     ADDRESS
1   0.30 ms 172.43.0.1
2   1.14 ms ricegate.rice.iit.edu (64.131.110.2)
3   6.08 ms 216.47.159.177
4   5.92 ms 216.47.159.249
5   8.59 ms 65.61.137.117

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.53 seconds
```

Nmap with the -A option gives the versions for each port and some extra information. The previous nmap scans have basically showed this information so not much more is learned other than confirming the previous findings.

Sparta (for confirmation)



	Port	Protocol	State	Name	Version
●	80	tcp	open	http	Microsoft IIS httpd 8.0
●	443	tcp	open	http	Microsoft IIS httpd 8.0
●	8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

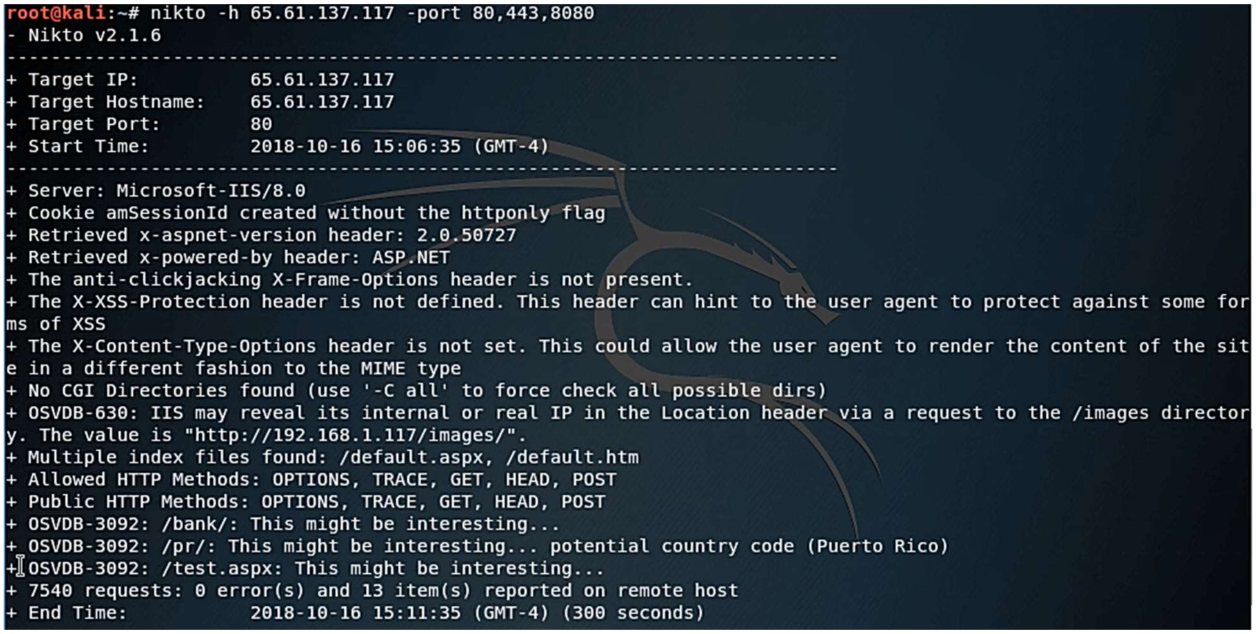


```
Host Status                  Addresses
    State: up                    IPv4: 65.61.137.117
    Open Ports: 3                IPv6:
    Closed Ports: 65526          MAC:
    Filtered Ports: 6

Operating System
    Name: Microsoft Windows Server 2008 R2
    Accuracy: 91
```

These screenshots from Sparta are to just confirm the results found from the nmap scans on the terminal. Vulnerability databases can be observed to see if any of these versions have documented vulnerabilities.

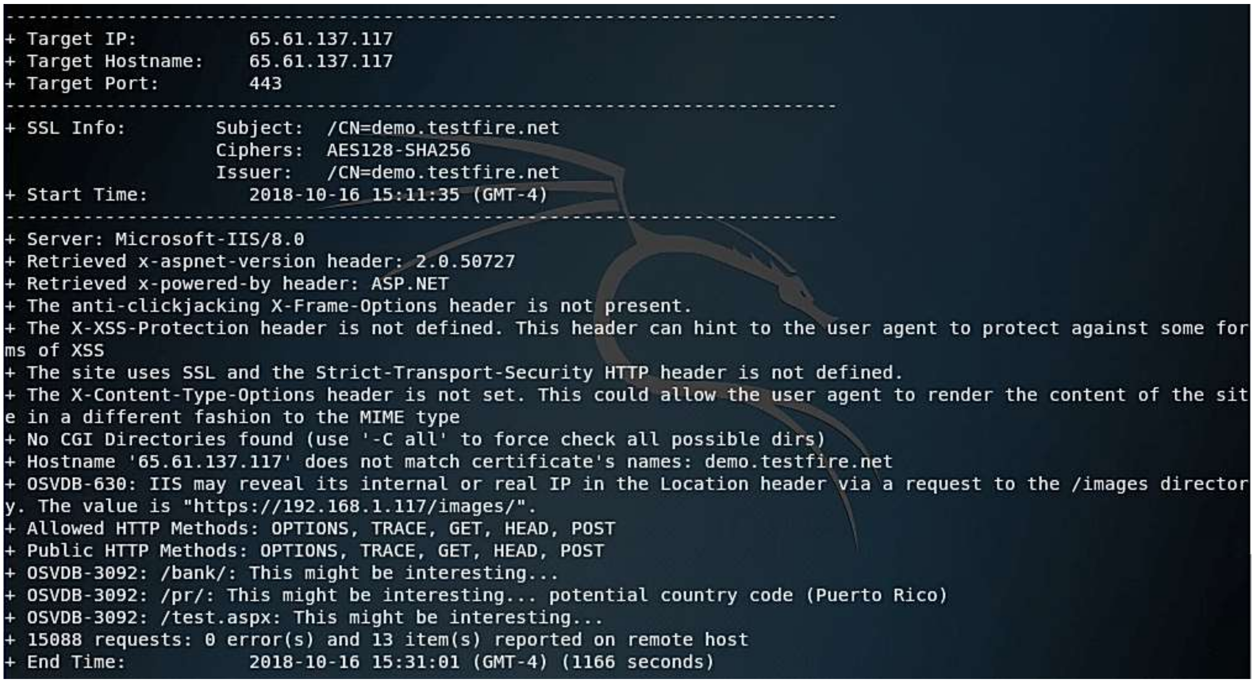
Nikto

Nikto is another scanner tool to test web servers. It was run with the 3 open ports to see the vulnerabilities associated with each one.



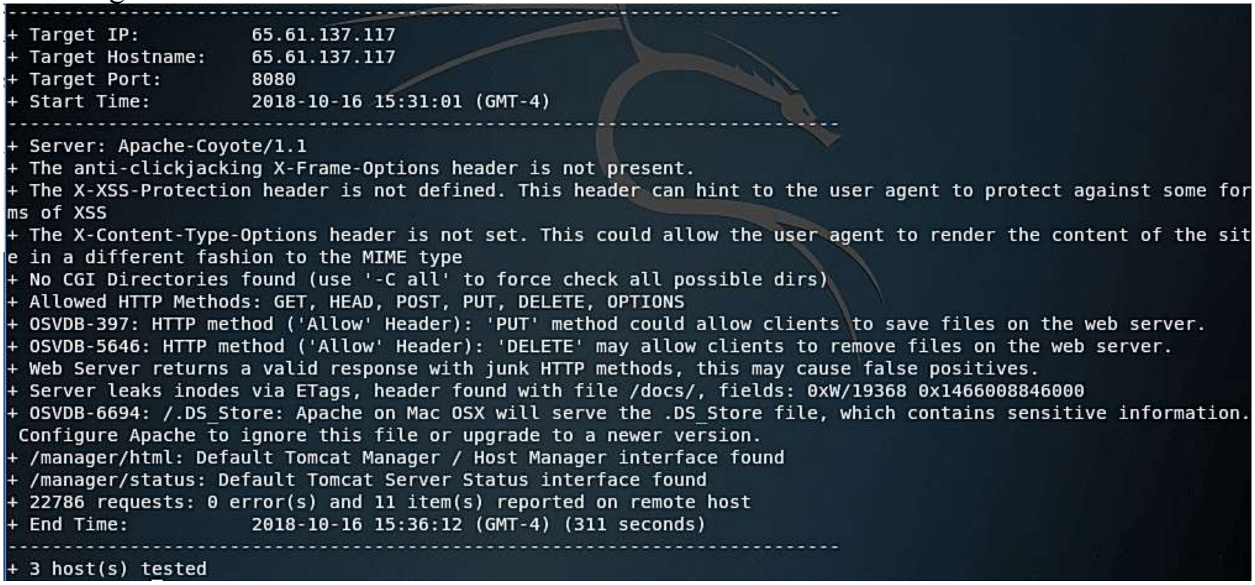
```
root@kali:~# nikto -h 65.61.137.117 -port 80,443,8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    65.61.137.117
+ Target Port:        80
+ Start Time:         2018-10-16 15:06:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Cookie amSessionId created without the httponly flag
+ Retrieved x-aspnet-version header: 2.0.50727
+ 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 agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images director
y. The value is "http://192.168.1.117/images/".
+ Multiple index files found: /default.aspx, /default.htm
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-3092: /bank/: This might be interesting...
+ OSVDB-3092: /pr/: This might be interesting... potential country code (Puerto Rico)
+ OSVDB-3092: /test.aspx: This might be interesting...
+ 7540 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2018-10-16 15:11:35 (GMT-4) (300 seconds)
```

First off, for port 80, it shows that there are certain headers (X-XSS-Protection and X-Content-Type-Options) that are either not defined or set. The undefined header means that some forms of cross-site scripting could be used. The header that was not set could be used to block content sniffing so it should be set just incase. The X-Frame Options header is not present which is needed to avoid clickjacking attacks.



```
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    65.61.137.117
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=demo.testfire.net
                   Ciphers:  AES128-SHA256
                   Issuer:   /CN=demo.testfire.net
+ Start Time:         2018-10-16 15:11:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Retrieved x-aspnet-version header: 2.0.50727
+ 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 agent to protect against some for
ms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '65.61.137.117' does not match certificate's names: demo.testfire.net
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images director
y. The value is "https://192.168.1.117/images/".
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-3092: /bank/: This might be interesting...
+ OSVDB-3092: /pr/: This might be interesting... potential country code (Puerto Rico)
+ OSVDB-3092: /test.aspx: This might be interesting...
+ 15088 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2018-10-16 15:31:01 (GMT-4) (1166 seconds)
```

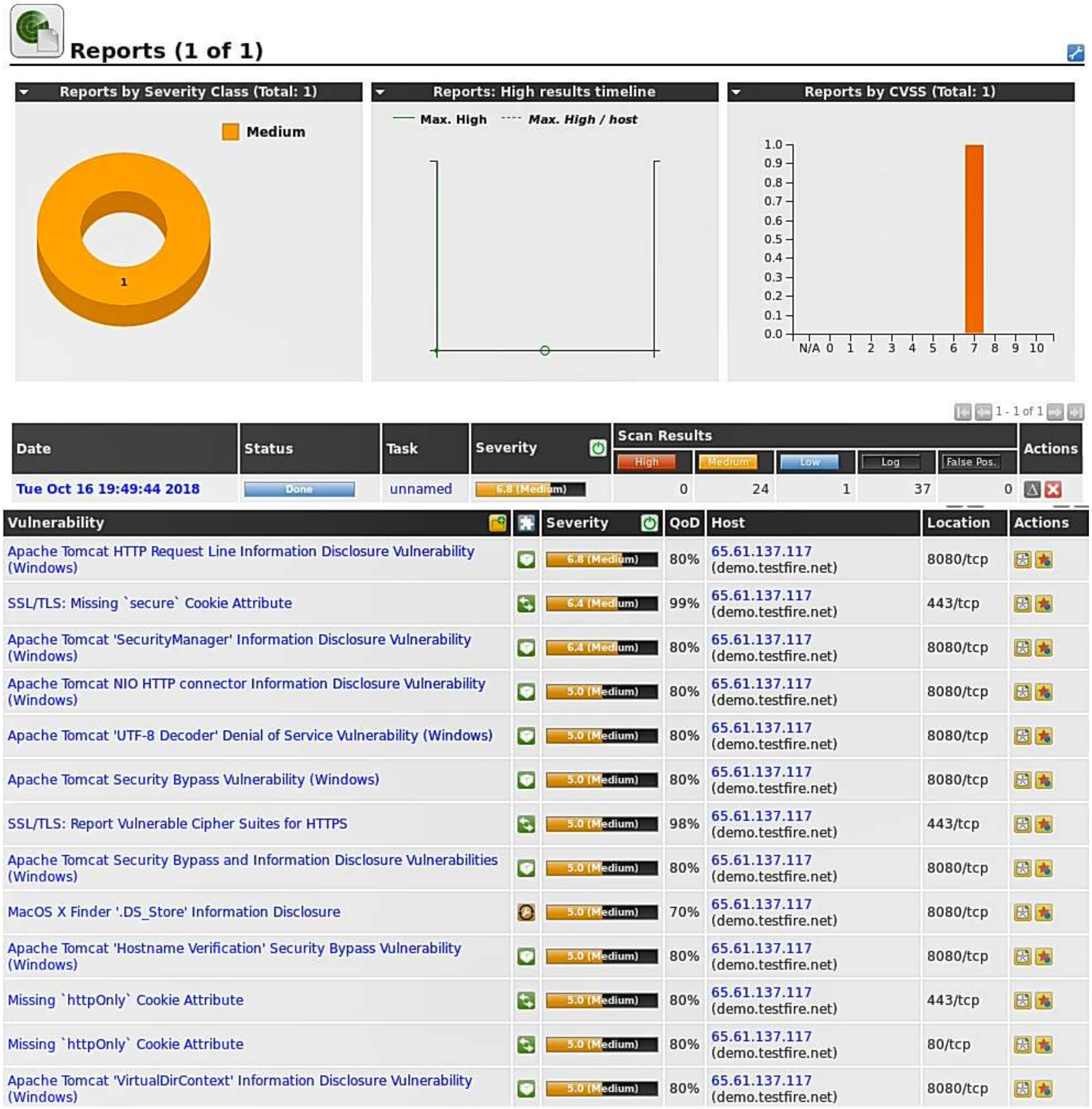
For port 443, it is similar to port 80 with an addition of Strict-Transport-Security HTTP header not being defined. This is quite important for a banking site since it tells browsers to access the site using HTTPS instead of HTTP.



```
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    65.61.137.117
+ Target Port:        8080
+ Start Time:         2018-10-16 15:31:01 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ 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 agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Server leaks inodes via ETags, header found with file /docs/, fields: 0xW/19368 0x1466008846000
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information.
 Configure Apache to ignore this file or upgrade to a newer version.
+ /manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/status: Default Tomcat Server Status interface found
+ 22786 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2018-10-16 15:36:12 (GMT-4) (311 seconds)
---------------------------------------------------------------------------
+ 3 host(s) tested
```

Port 8080 basically has the same vulnerabilities as 80.

OpenVAS

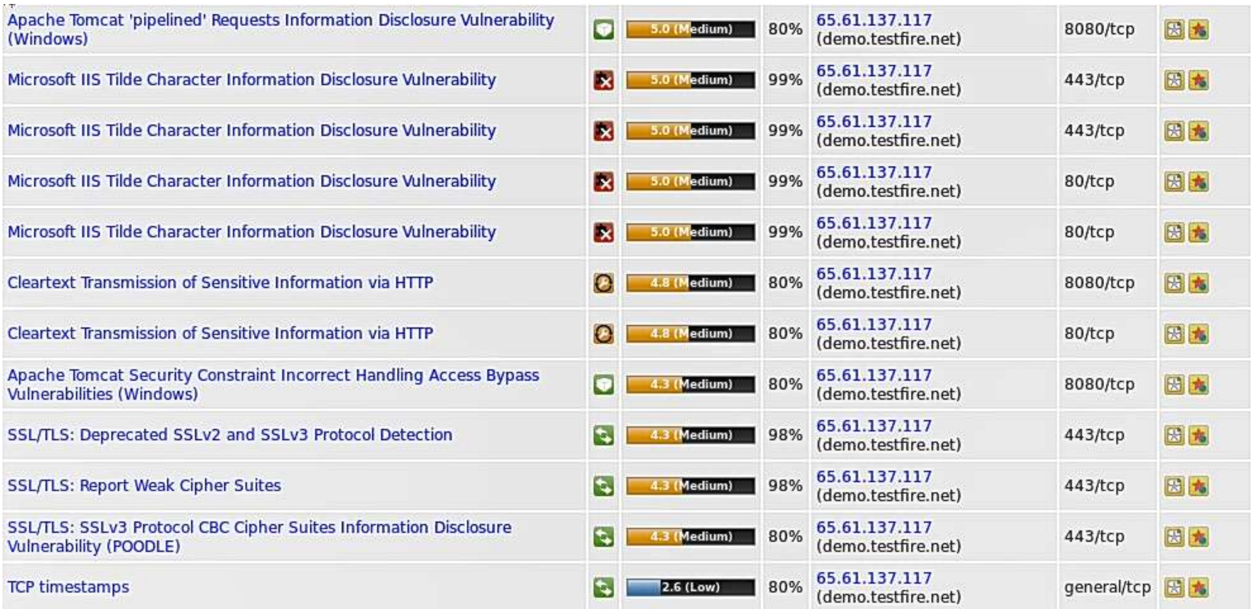


Reports (1 of 1)

Reports by Severity Class (Total: 1)
Medium
1
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
N/A
0
1
2
3
4
5
6
7
8
9
10
1 - 1 of 1

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Tue Oct 16 19:49:44 2018	Done	unnamed	6.8 (Medium)	0	24	1	37	0	

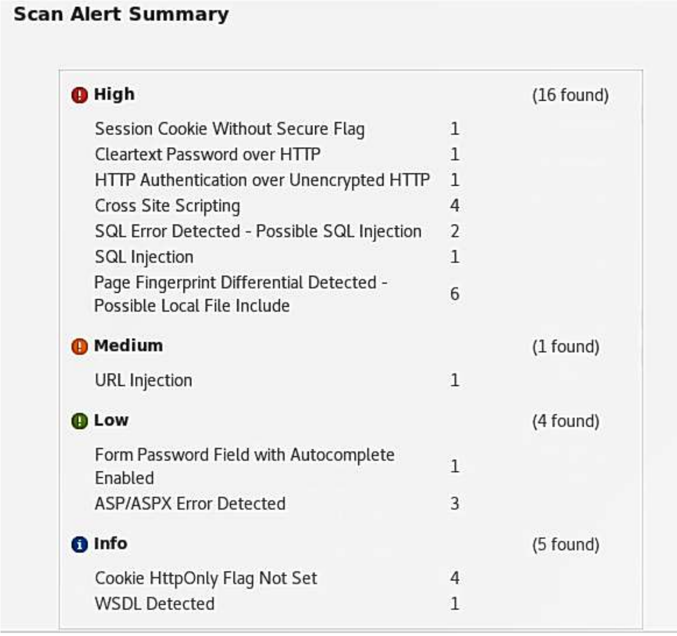
Vulnerability		Severity	QoD	Host	Location	Actions
Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Windows)		6.8 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
SSL/TLS: Missing `secure` Cookie Attribute		6.4 (Medium)	99%	65.61.137.117 (demo.testfire.net)	443/tcp	
Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability (Windows)		6.4 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
Apache Tomcat Security Bypass Vulnerability (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	65.61.137.117 (demo.testfire.net)	443/tcp	
Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
MacOS X Finder '.DS_Store' Information Disclosure		5.0 (Medium)	70%	65.61.137.117 (demo.testfire.net)	8080/tcp	
Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	
Missing `httpOnly` Cookie Attribute		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	443/tcp	
Missing `httpOnly` Cookie Attribute		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	80/tcp	
Apache Tomcat 'VirtualDirContext' Information Disclosure Vulnerability (Windows)		5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp	



Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Windows)	5.0 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp
Microsoft IIS Tilde Character Information Disclosure Vulnerability	5.0 (Medium)	99%	65.61.137.117 (demo.testfire.net)	443/tcp
Microsoft IIS Tilde Character Information Disclosure Vulnerability	5.0 (Medium)	99%	65.61.137.117 (demo.testfire.net)	443/tcp
Microsoft IIS Tilde Character Information Disclosure Vulnerability	5.0 (Medium)	99%	65.61.137.117 (demo.testfire.net)	80/tcp
Microsoft IIS Tilde Character Information Disclosure Vulnerability	5.0 (Medium)	99%	65.61.137.117 (demo.testfire.net)	80/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%	65.61.137.117 (demo.testfire.net)	80/tcp
Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities (Windows)	4.3 (Medium)	80%	65.61.137.117 (demo.testfire.net)	8080/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	65.61.137.117 (demo.testfire.net)	443/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	65.61.137.117 (demo.testfire.net)	443/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	65.61.137.117 (demo.testfire.net)	443/tcp
TCP timestamps	2.6 (Low)	80%	65.61.137.117 (demo.testfire.net)	general/tcp

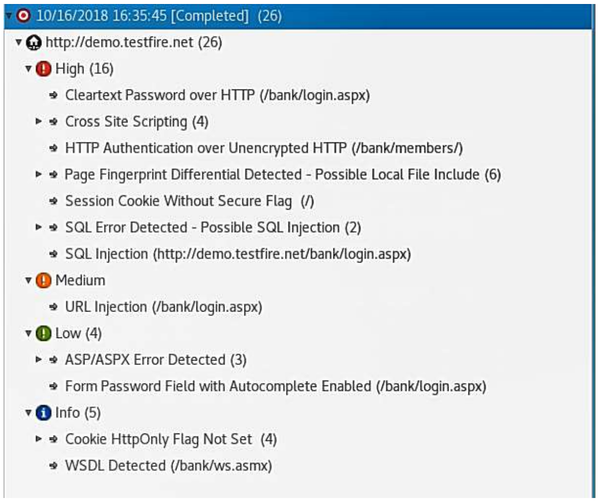
Many vulnerabilities are listed when using OpenVAS. The severity along with what is needed to fix, mitigate, and work around should be considered. Especially since it is not always feasible to fix every problem. For example, Apache Tomcat vulnerabilities should be fixed by upgrading to the recommended versions given by the vendor. This will prevent XSS attacks, sensitive information from being obtained, denial-of-service attacks, and bypassing security restrictions. For the MacOS X vulnerability, changing configurations to block access to hidden files will help prevent giving attackers extra information about contents of a directory. For some bizarre reason, usernames and passwords are transmitted in cleartext via HTTP which is the last thing someone wants when visiting a banking site. Last but not least, for the SSL/TLS vulnerabilities, SSL options should be disabled and TLS should be enabled.

Vega



Scan Alert Summary

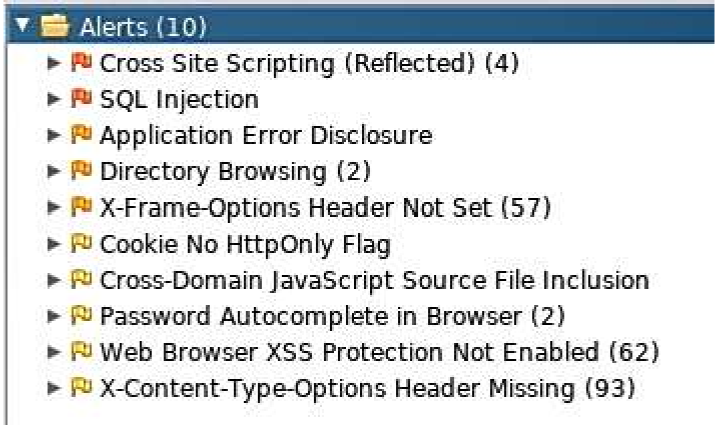
High		(16 found)
Session Cookie Without Secure Flag	1	
Cleartext Password over HTTP	1	
HTTP Authentication over Unencrypted HTTP	1	
Cross Site Scripting	4	
SQL Error Detected - Possible SQL Injection	2	
SQL Injection	1	
Page Fingerprint Differential Detected - Possible Local File Include	6	
Medium		(1 found)
URL Injection	1	
Low		(4 found)
Form Password Field with Autocomplete Enabled	1	
ASP/ASPX Error Detected	3	
Info		(5 found)
Cookie HttpOnly Flag Not Set	4	
WSDL Detected	1	



```
▾ 10/16/2018 16:35:45 [Completed]  (26)
  ▾ http://demo.testfire.net (26)
    ▾ High (16)
        Cleartext Password over HTTP (/bank/login.aspx)
      ▸ Cross Site Scripting (4)
        HTTP Authentication over Unencrypted HTTP (/bank/members/)
      ▸ Page Fingerprint Differential Detected - Possible Local File Include (6)
        Session Cookie Without Secure Flag  (/)
      ▸ SQL Error Detected - Possible SQL Injection (2)
        SQL Injection (http://demo.testfire.net/bank/login.aspx)
    ▾ Medium
        URL Injection (/bank/login.aspx)
    ▾ Low (4)
      ▸ ASP/ASPX Error Detected (3)
        Form Password Field with Autocomplete Enabled (/bank/login.aspx)
    ▾ Info (5)
      ▸ Cookie HttpOnly Flag Not Set  (4)
        WSDL Detected (/bank/ws.asmx)
```

Vega will be used to find vulnerabilities with the code for this website. Once again, HTTP strikes again as a highly dangerous vulnerability. By requiring HTTP authentication and using cleartext for sensitive information rather than encrypting it, there is no stopping someone from eavesdropping. For a bank website, sensitive information such as usernames and passwords should be nowhere near an unauthorized user. Another problem this site seems to have is being vulnerable to cross-site scripting (XSS) which is dangerous for sites dealing with sensitive information. Session cookies should be secured which in this case, is not. Another vulnerability is the possibility of a SQL injection which can result in remote attackers gaining access privileges to the database and its server.

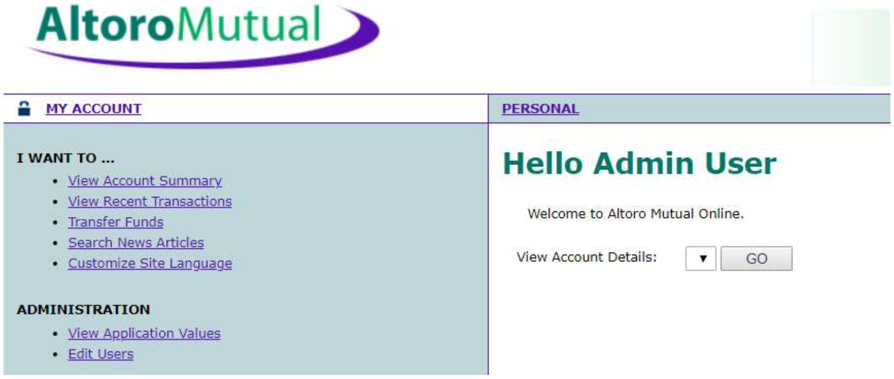
OWASP



```
▼ Alerts (10)
    ▶ Cross Site Scripting (Reflected) (4)
    ▶ SQL Injection
    ▶ Application Error Disclosure
    ▶ Directory Browsing (2)
    ▶ X-Frame-Options Header Not Set (57)
    ▶ Cookie No HttpOnly Flag
    ▶ Cross-Domain JavaScript Source File Inclusion
    ▶ Password Autocomplete in Browser (2)
    ▶ Web Browser XSS Protection Not Enabled (62)
    ▶ X-Content-Type-Options Header Missing (93)
```

OWASP provides another assessment of the coding problems. All of these vulnerabilities have been discussed in previous sections of this report. Clearly, there is quite a few coding problems that should be taken into account.

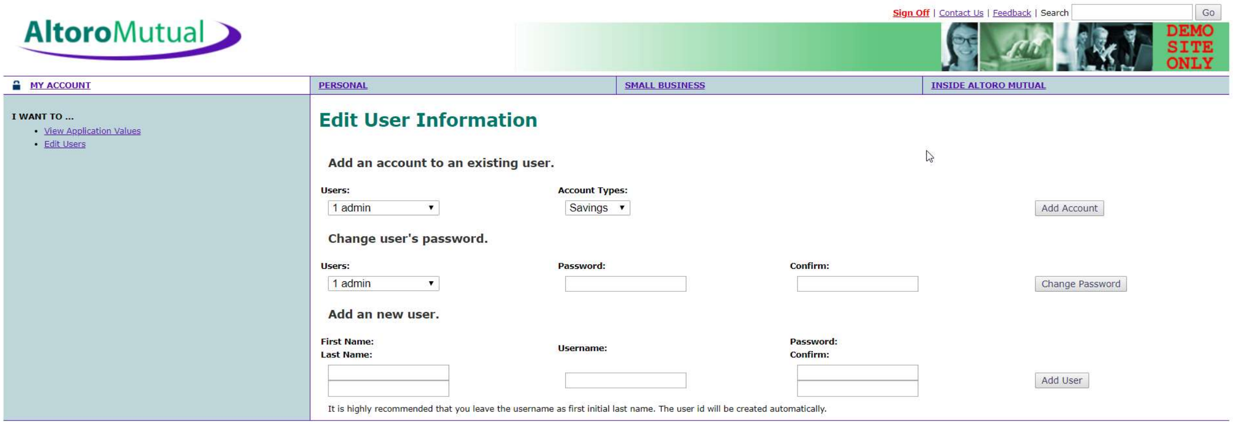
Of course…it works… Admin/Admin



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: ▾



Edit User Information

Add an account to an existing user.

Users: 1 admin ▾ Account Types: Savings ▾

Change user's password.

Users: 1 admin ▾ Password: Confirm:

Add an new user.

First Name: Last Name: Username: Password: Confirm:

It is highly recommended that you leave the username as first initial last name. The user id will be created automatically.

Based on how there were so many vulnerabilities, I attempted to try a couple basic username and password combinations to find out that admin/admin worked. No words can express how dangerous this is for a banking site. The screenshot shows that editing user information is possible. On this page, I could add an account or user and even change the password.