

Practical 1: OSINT (Open source Intelligence)

The OSINT framework is a methodology that integrates data, processes, methods, tools and techniques to help the security team identify information about an adversary or their actions quickly and accurately. An OSINT framework can be used to: Establish the digital footprint of a known threat.

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for \$\$\$, but you should be able to get at least a portion of the available information for no cost.

Examples for OSINT:

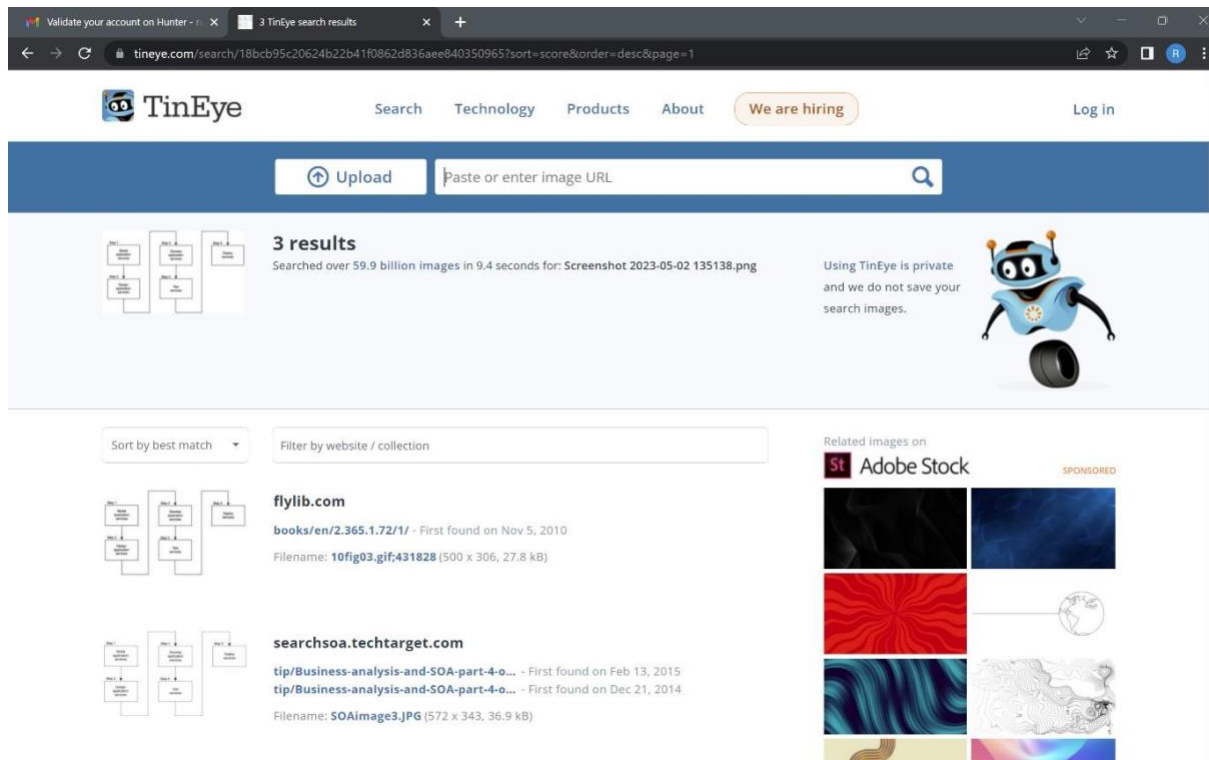
1. Hunter.io

The top screenshot shows the Hunter.io homepage. It features a navigation bar with links to Product, Pricing, Resources, and Company. The main content area is divided into three sections: 'Domain Search' (Find the best person to contact from a company name or website), 'Email Finder' (Type a name, get a verified email address), and 'Email Verifier' (Avoid bounces and protect your sender reputation). Each section includes a 'Try it now' or 'Find Email' button and a note that no account is required.

The bottom screenshot shows a search results page for 'somaiya.edu'. The search bar displays 'somaiya.edu' and '588 results'. The results are listed in a table with columns for Name, Email, and a 'Save as lead' button. The table shows three results: Mahima Sethi (mahima.sethi@somaiya.edu), Deepak Jagtap (deepak.jagtap@somaiya.edu), and Dinesh Vaidya (dinesh.vaidya@somaiya.edu). A sidebar on the right provides company information for 'Somaiya Vidyavihar' and a list of technologies.

2. TinEye.com

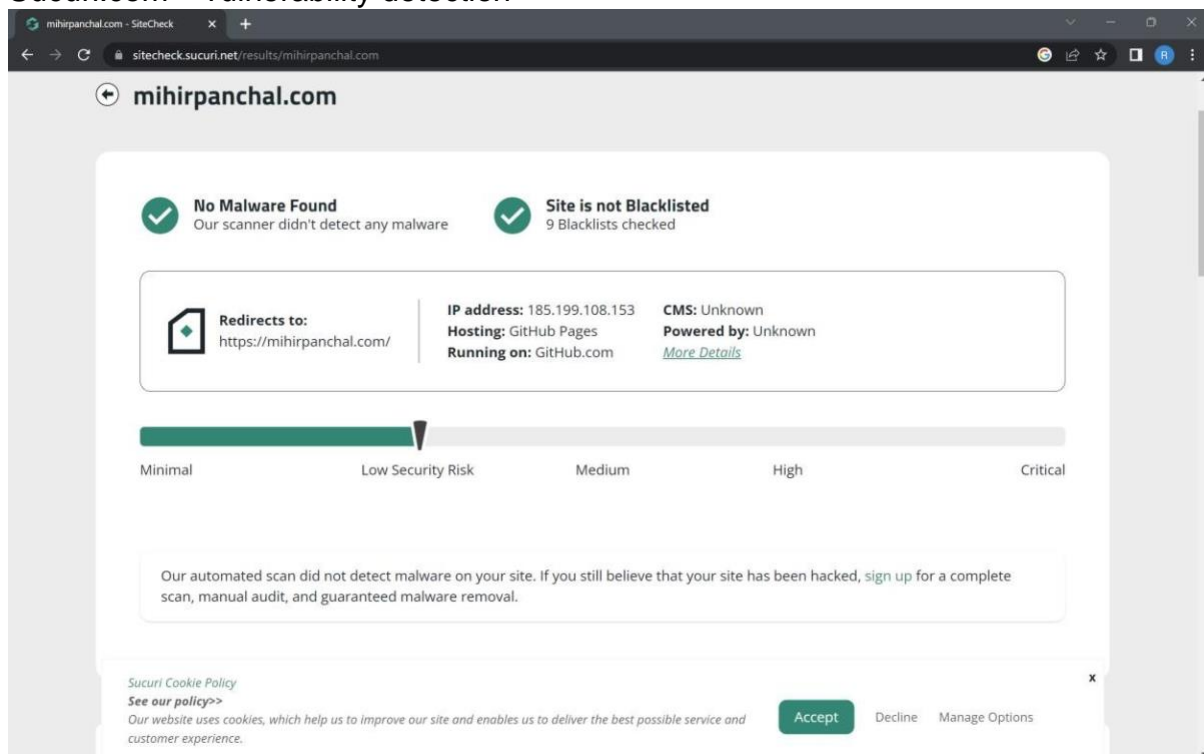
Used for reverse search of images



3. Pimeyes.com

Used for facial reverse search of images

4. Sucuri.com – vulnerability detection



5. Whois domain look up

The screenshot shows the Whois.com website with the domain mihirpanchal.com. The page is divided into two main sections: Domain Information and Registrant Contact. The Domain Information section lists details such as the domain name, registrar (Google LLC), registration and expiration dates, status, and name servers. The Registrant Contact section provides contact details for Contact Privacy Inc. Customer 7151571251, including address, city, state, postal code, country, and phone number. On the right side, there is a list of similar domains with 'Buy Now' buttons. A prominent red banner for '.mom' domains is also visible, showing a sale price of \$2.28.

Domain Information	
Domain:	mihirpanchal.com
Registrar:	Google LLC
Registered On:	2020-07-18
Expires On:	2023-07-18
Updated On:	2022-06-21
Status:	clientTransferProhibited
Name Servers:	ns-cloud-a1.googledomains.com ns-cloud-a2.googledomains.com ns-cloud-a3.googledomains.com ns-cloud-a4.googledomains.com

Registrant Contact	
Name:	Contact Privacy Inc. Customer 7151571251
Organization:	Contact Privacy Inc. Customer 7151571251
Street:	96 Mowat Ave
City:	Toronto
State:	ON
Postal Code:	M4K 3K1
Country:	CA
Phone:	+1.4165385487

Interested in similar domains?

- mihirsrivastava.com [Buy Now](#)
- mihirpanchalphotography.com [Buy Now](#)
- drmihirpanchal.com [Buy Now](#)
- mihirgoswami.com [Buy Now](#)
- mihirsrivastava.net [Buy Now](#)
- mihirparekh.net [Buy Now](#)

.mom Sale
~~\$39.88~~ **\$2.28**
[BUY NOW](#)
*Offer ends 31st May 2023

On Sale!

The screenshot shows the 'Raw Whois Data' section of the Whois.com website for the domain mihirpanchal.com. It displays a detailed text-based record of the domain's registration information, including registry ID, registrar details, creation and expiration dates, and contact information for the registrant, admin, and technical contacts.

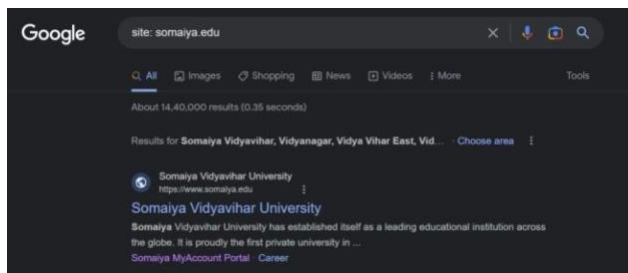
```
Domain Name: mihirpanchal.com
Registry Domain ID: 2546885397_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2022-06-21T16:07:16Z
Creation Date: 2020-07-18T12:46:36Z
Registrar Registration Expiration Date: 2023-07-18T12:46:36Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.877.237.6466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferPro
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 7151571251
Registrant Organization: Contact Privacy Inc. Customer 7151571251
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: https://domains.google.com/contactregistrant?domain=mihirpanchal.
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 7151571251
Admin Organization: Contact Privacy Inc. Customer 7151571251
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: https://domains.google.com/contactregistrant?domain=mihirpanchal.
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 7151571251
Tech Organization: Contact Privacy Inc. Customer 7151571251
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
```

Practical 2: To obtain specific results using google dorks

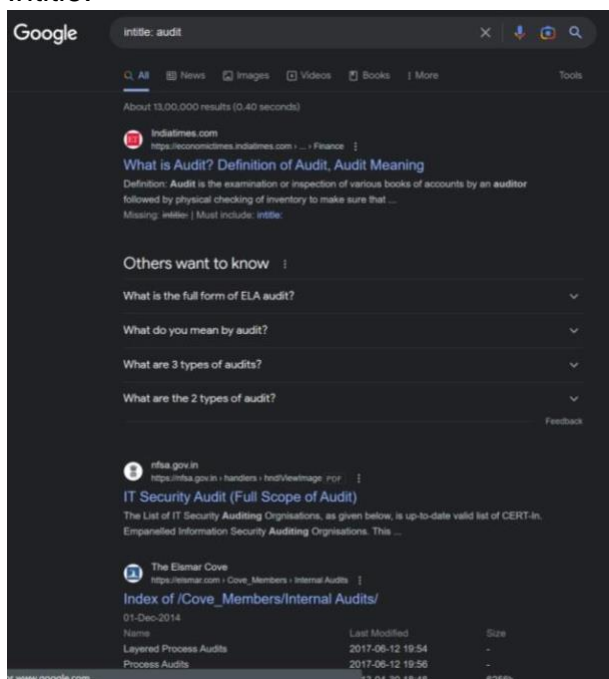
Google dorking is a passive attack or hacking method involving the use of a custom query.

Some examples of commonly used dorks are:

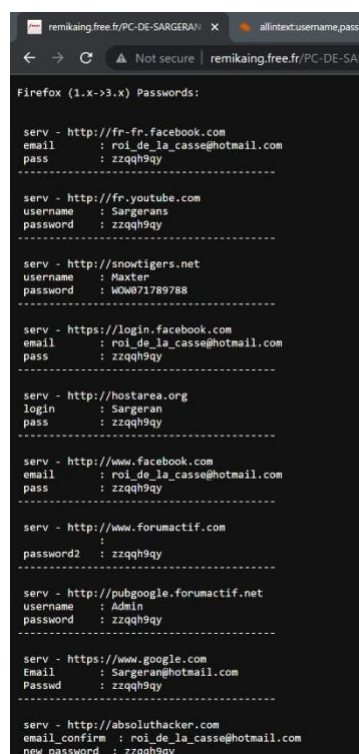
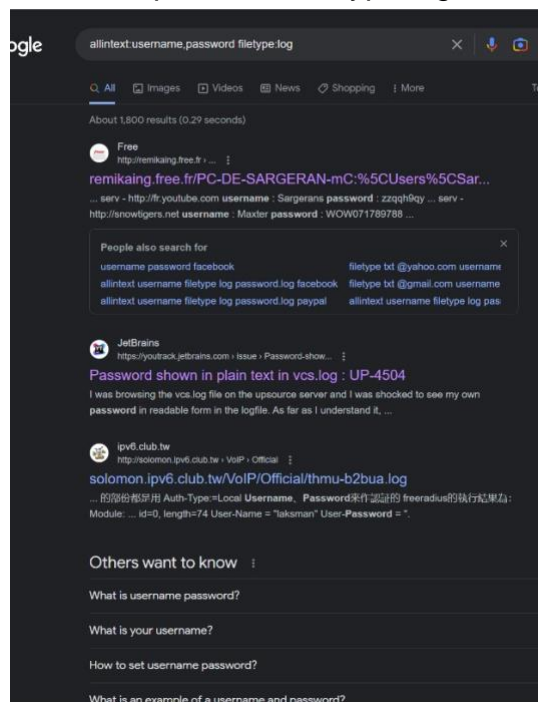
a. Site:____(site name)



b. Intitle:

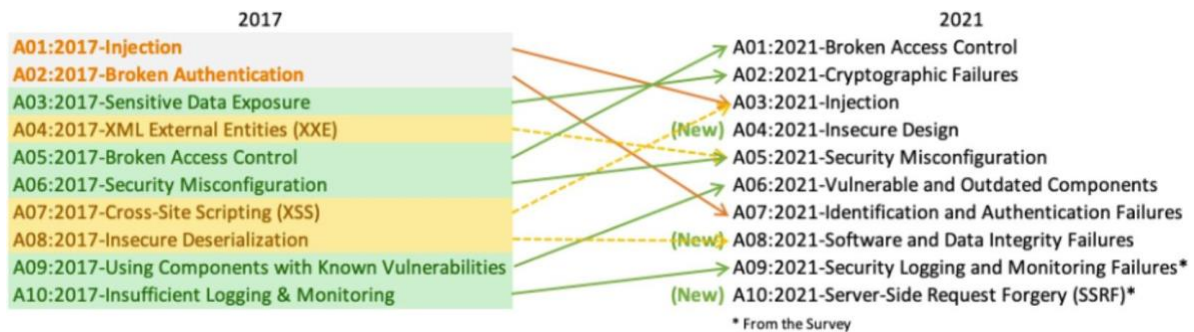


c. allintext: password filetype:log after:2020



Practical 3: OWASP Top 10

The OWASP Top 10 is a non-profit organization whose work is focused on improving software security. It finds most dangerous security threats to web applications and rank them according to their frequency of occurrence and severity of impact. These are the OWASP top 10 vulnerabilities that every developer should look out before proceeding with the development.



1. Broken access control:
Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.
2. Cryptographic failures:
A cryptographic failure is a critical web application security vulnerability that exposes sensitive application data on a weak or non-existent cryptographic algorithm. Those can be passwords, patient health records, business secrets, credit card information, email addresses, or other personal user information.
3. Injection:
Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections. Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged. Organizations can include static (SAST), dynamic (DAST), and interactive (IAST) application security testing tools into the CI/CD pipeline to identify introduced injection flaws before production deployment.
4. Insecure design:
Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation

defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

5. Security misconfiguration:

Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

6. Vulnerable and outdated components:

If the software is vulnerable, unsupported, or out of date it is vulnerable. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.

7. Identification and authentication failures:

Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application;

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".

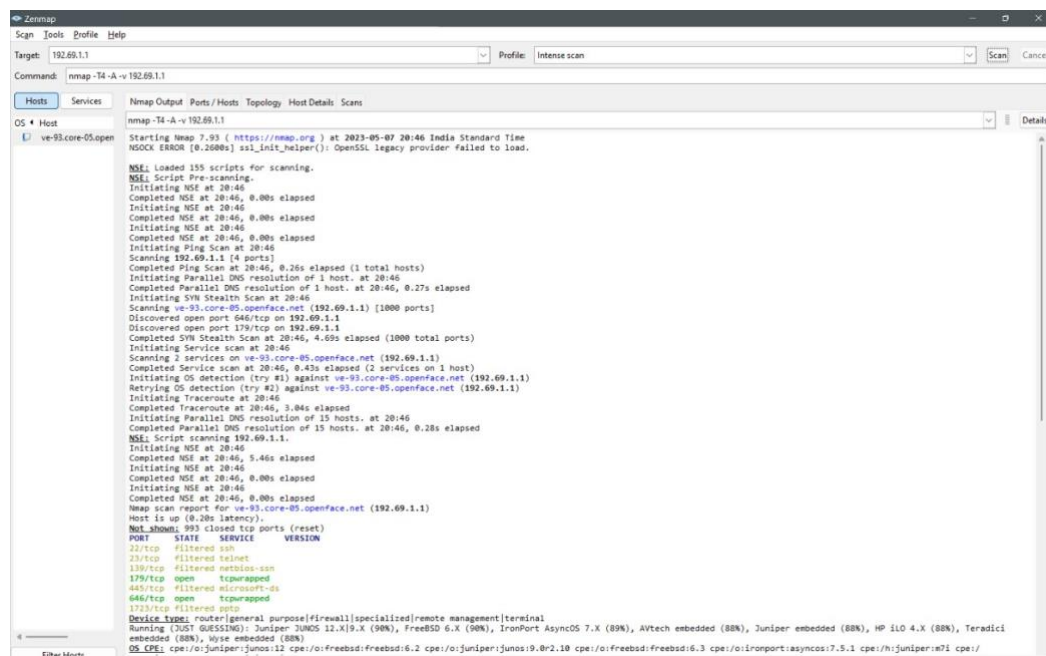
8. Software and data integrity failures:

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

9. Server-side request forgery:
SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).
10. Security logging and monitoring failures:
This is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time.

Practical 4: Network scanner

Nmap: Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. It is used for network exploration, host discovery, and security audit



```
nmap -T4 -A -v 192.69.1.1

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 20:46 India Standard Time
NSOCK ERROR [0.2000s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Initiating Ping Scan at 20:46
Completed Ping Scan at 20:46, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:46
Completed Parallel DNS resolution of 1 host. at 20:46, 0.27s elapsed
Initiating SYN Stealth Scan at 20:46
Scanning 192.69.1.1 [4 ports]
Completed SYN Stealth Scan at 20:46, 0.43s elapsed (2 services on 1 host)
Initiating Service scan at 20:46
Scanning 2 services on ve-93.core-05.openface.net (192.69.1.1)
Completed Service scan at 20:46, 3.04s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against ve-93.core-05.openface.net (192.69.1.1)
Retrying OS detection (try #2) against ve-93.core-05.openface.net (192.69.1.1)
Initiating Traceroute at 20:46
Completed Traceroute at 20:46, 3.04s elapsed
Initiating Parallel DNS resolution of 15 hosts. at 20:46
Completed Parallel DNS resolution of 15 hosts. at 20:46, 0.28s elapsed
NSE: Script scanning 192.69.1.1.
Initiating NSE at 20:46
Completed NSE at 20:46, 5.46s elapsed
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Nmap scan report for ve-93.core-05.openface.net (192.69.1.1)
Host is up (0.28s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
23/tcp    filtered telnet
139/tcp   filtered netbios-ssn
179/tcp   open  tcpwrapped
445/tcp   filtered microsoft-ds
646/tcp   open  tcpwrapped
1723/tcp  filtered neto
Device type: router[general purpose]firewall[specialized]remote management[terminal]
Running (JUST GUESSED): Juniper JUNOS 12.X(9%), FreeBSD 6.X(9%), IronPort AsyncOS 7.X(8%), AVTech embedded(8%), Juniper embedded(8%), HP iLO 4.X(8%), Teradici
embedded(8%), Wyse embedded(8%)
OS CPE: cpe:/o:juniper:junos:12 cpe:/o:freebsd:freebsd:6.2 cpe:/o:juniper:junos:9.0r2.10 cpe:/o:freebsd:freebsd:6.3 cpe:/o:ironport:asyncos:7.5.1 cpe:/h:juniper:n71 cpe:/
```

Practical 5: Power BI

Microsoft Power BI is an interactive data visualization software product developed by Microsoft with a primary focus on business intelligence. It is part of the Microsoft Power Platform.

The screenshot shows the Microsoft Power BI Desktop interface. The 'Table tools' ribbon is active, displaying options for 'Mark as date table', 'Manage relationships', 'New measure', 'Quick measure column', and 'New table'. The data table below has the following columns: Country, Product, Units Sold, Revenue per cookie, Cost per cookie, Revenue, Cost, Profit, Date, Month Number, Month Name, and Year. The table contains 525 rows of data, all for 'Chocolate Chip' products from various countries.

Country	Product	Units Sold	Revenue per cookie	Cost per cookie	Revenue	Cost	Profit	Date	Month Number	Month Name	Year
Canada	Chocolate Chip	292	\$5.00	\$2.00	\$1,460.00	\$584.00	\$876.00	02 January 2019	2	February	20
Mexico	Chocolate Chip	974	\$5.00	\$2.00	\$4,870.00	\$1,948.00	\$2,922.00	02 January 2019	2	February	20
Canada	Chocolate Chip	2518	\$5.00	\$2.00	\$12,590.00	\$5,036.00	\$7,554.00	06 January 2019	6	June	20
Germany	Chocolate Chip	1006	\$5.00	\$2.00	\$5,030.00	\$2,012.00	\$3,018.00	06 January 2019	6	June	20
Germany	Chocolate Chip	367	\$5.00	\$2.00	\$1,835.00	\$734.00	\$1,101.00	07 January 2019	7	July	20
Mexico	Chocolate Chip	883	\$5.00	\$2.00	\$4,415.00	\$1,766.00	\$2,649.00	08 January 2019	8	August	20
Mexico	Chocolate Chip	2472	\$5.00	\$2.00	\$12,360.00	\$4,944.00	\$7,416.00	09 January 2019	9	September	20
United States	Chocolate Chip	1143	\$5.00	\$2.00	\$5,715.00	\$2,286.00	\$3,429.00	10 January 2019	10	October	20
Canada	Chocolate Chip	1817	\$5.00	\$2.00	\$9,085.00	\$3,634.00	\$5,451.00	12 January 2019	12	December	20
Germany	Chocolate Chip	1513	\$5.00	\$2.00	\$7,565.00	\$3,026.00	\$4,539.00	12 January 2019	12	December	20
France	Chocolate Chip	3945	\$5.00	\$2.00	\$19,725.00	\$7,890.00	\$11,835.00	01 January 2019	1	January	20
France	Chocolate Chip	2296	\$5.00	\$2.00	\$11,480.00	\$4,592.00	\$6,888.00	02 January 2019	2	February	20
France	Chocolate Chip	1030	\$5.00	\$2.00	\$5,150.00	\$2,060.00	\$3,090.00	05 January 2019	5	May	20
United States	Chocolate Chip	1514	\$5.00	\$2.00	\$7,570.00	\$3,028.00	\$4,542.00	02 January 2019	2	February	20
United States	Chocolate Chip	4492.5	\$5.00	\$2.00	\$22,462.50	\$8,985.00	\$13,477.50	04 January 2019	4	April	20
United States	Chocolate Chip	727	\$5.00	\$2.00	\$3,635.00	\$1,454.00	\$2,181.00	06 January 2019	6	June	20
France	Chocolate Chip	787	\$5.00	\$2.00	\$3,935.00	\$1,574.00	\$2,361.00	06 January 2019	6	June	20
Mexico	Chocolate Chip	1823	\$5.00	\$2.00	\$9,115.00	\$3,646.00	\$5,469.00	07 January 2019	7	July	20
Germany	Chocolate Chip	747	\$5.00	\$2.00	\$3,735.00	\$1,494.00	\$2,241.00	09 January 2019	9	September	20
United States	Chocolate Chip	2905	\$5.00	\$2.00	\$14,525.00	\$5,810.00	\$8,715.00	11 January 2019	11	November	20
France	Chocolate Chip	2155	\$5.00	\$2.00	\$10,775.00	\$4,310.00	\$6,465.00	12 January 2019	12	December	20
Canada	Chocolate Chip	2363	\$5.00	\$2.00	\$11,815.00	\$4,726.00	\$7,089.00	02 January 2019	2	February	20
France	Chocolate Chip	918	\$5.00	\$2.00	\$4,590.00	\$1,836.00	\$2,754.00	05 January 2019	5	May	20
Germany	Chocolate Chip	1728	\$5.00	\$2.00	\$8,640.00	\$3,456.00	\$5,184.00	05 January 2019	5	May	20
United States	Chocolate Chip	1142	\$5.00	\$2.00	\$5,710.00	\$2,284.00	\$3,426.00	06 January 2019	6	June	20
Mexico	Chocolate Chip	662	\$5.00	\$2.00	\$3,310.00	\$1,324.00	\$1,986.00	06 January 2019	6	June	20
Canada	Chocolate Chip	1295	\$5.00	\$2.00	\$6,475.00	\$2,590.00	\$3,885.00	10 January 2019	10	October	20
Canada	Chocolate Chip	1916	\$5.00	\$2.00	\$9,580.00	\$3,832.00	\$5,748.00	12 January 2019	12	December	20
Canada	Chocolate Chip	2852	\$5.00	\$2.00	\$14,260.00	\$5,704.00	\$8,556.00	12 January 2019	12	December	20

Table: Sheet1 (525 rows)

The screenshot shows the Microsoft Power BI Desktop interface with the 'Column tools' ribbon active. The 'Product' column is selected, and a filter is applied, showing only 'Chocolate Chip' products. The data table below has the same columns as the previous screenshot, but only rows where the product is 'Chocolate Chip' are displayed.

Country	Product	Units Sold	Revenue per cookie	Cost per cookie	Revenue	Cost	Profit	Date	Month Number	Month Name	Year
Canada	Chocolate Chip	292	\$5.00	\$2.00	\$1,460.00	\$584.00	\$876.00	02 January 2019	2	February	20
Mexico	Chocolate Chip	974	\$5.00	\$2.00	\$4,870.00	\$1,948.00	\$2,922.00	02 January 2019	2	February	20
Canada	Chocolate Chip	2518	\$5.00	\$2.00	\$12,590.00	\$5,036.00	\$7,554.00	06 January 2019	6	June	20
Germany	Chocolate Chip	1006	\$5.00	\$2.00	\$5,030.00	\$2,012.00	\$3,018.00	06 January 2019	6	June	20
Germany	Chocolate Chip	367	\$5.00	\$2.00	\$1,835.00	\$734.00	\$1,101.00	07 January 2019	7	July	20
Mexico	Chocolate Chip	883	\$5.00	\$2.00	\$4,415.00	\$1,766.00	\$2,649.00	08 January 2019	8	August	20
Mexico	Chocolate Chip	2472	\$5.00	\$2.00	\$12,360.00	\$4,944.00	\$7,416.00	09 January 2019	9	September	20
United States	Chocolate Chip	1143	\$5.00	\$2.00	\$5,715.00	\$2,286.00	\$3,429.00	10 January 2019	10	October	20
Canada	Chocolate Chip	1817	\$5.00	\$2.00	\$9,085.00	\$3,634.00	\$5,451.00	12 January 2019	12	December	20
Germany	Chocolate Chip	1513	\$5.00	\$2.00	\$7,565.00	\$3,026.00	\$4,539.00	12 January 2019	12	December	20
France	Chocolate Chip	3945	\$5.00	\$2.00	\$19,725.00	\$7,890.00	\$11,835.00	01 January 2019	1	January	20
France	Chocolate Chip	2296	\$5.00	\$2.00	\$11,480.00	\$4,592.00	\$6,888.00	02 January 2019	2	February	20
France	Chocolate Chip	1030	\$5.00	\$2.00	\$5,150.00	\$2,060.00	\$3,090.00	05 January 2019	5	May	20
United States	Chocolate Chip	1514	\$5.00	\$2.00	\$7,570.00	\$3,028.00	\$4,542.00	02 January 2019	2	February	20
United States	Chocolate Chip	4492.5	\$5.00	\$2.00	\$22,462.50	\$8,985.00	\$13,477.50	04 January 2019	4	April	20
United States	Chocolate Chip	727	\$5.00	\$2.00	\$3,635.00	\$1,454.00	\$2,181.00	06 January 2019	6	June	20
France	Chocolate Chip	787	\$5.00	\$2.00	\$3,935.00	\$1,574.00	\$2,361.00	06 January 2019	6	June	20
Mexico	Chocolate Chip	1823	\$5.00	\$2.00	\$9,115.00	\$3,646.00	\$5,469.00	07 January 2019	7	July	20
Germany	Chocolate Chip	747	\$5.00	\$2.00	\$3,735.00	\$1,494.00	\$2,241.00	09 January 2019	9	September	20
United States	Chocolate Chip	2905	\$5.00	\$2.00	\$14,525.00	\$5,810.00	\$8,715.00	11 January 2019	11	November	20
France	Chocolate Chip	2155	\$5.00	\$2.00	\$10,775.00	\$4,310.00	\$6,465.00	12 January 2019	12	December	20
Canada	Chocolate Chip	2363	\$5.00	\$2.00	\$11,815.00	\$4,726.00	\$7,089.00	02 January 2019	2	February	20
France	Chocolate Chip	918	\$5.00	\$2.00	\$4,590.00	\$1,836.00	\$2,754.00	05 January 2019	5	May	20
Germany	Chocolate Chip	1728	\$5.00	\$2.00	\$8,640.00	\$3,456.00	\$5,184.00	05 January 2019	5	May	20
United States	Chocolate Chip	1142	\$5.00	\$2.00	\$5,710.00	\$2,284.00	\$3,426.00	06 January 2019	6	June	20
Mexico	Chocolate Chip	662	\$5.00	\$2.00	\$3,310.00	\$1,324.00	\$1,986.00	06 January 2019	6	June	20
Canada	Chocolate Chip	1295	\$5.00	\$2.00	\$6,475.00	\$2,590.00	\$3,885.00	10 January 2019	10	October	20
Canada	Chocolate Chip	1916	\$5.00	\$2.00	\$9,580.00	\$3,832.00	\$5,748.00	12 January 2019	12	December	20
Canada	Chocolate Chip	2852	\$5.00	\$2.00	\$14,260.00	\$5,704.00	\$8,556.00	12 January 2019	12	December	20

Table: Sheet1 (525 rows) Column: Product (6 distinct values)

firstbikvincookie - Power BI Desktop

File Home Help Table tools Column tools

Name Product % Format Text

Data type Text

Summarization Don't summarize

Data category Uncategorized

Sort by column

Data groups

Manage relationships

New column

Structure

Formatting

Properties

Sort

Groups

Relationships

Calculations

Data

Search

Sheet1

Column13

Cost

Cost per cookie

Country

Date

Month Name

Month Number

Product

Profit

Revenue

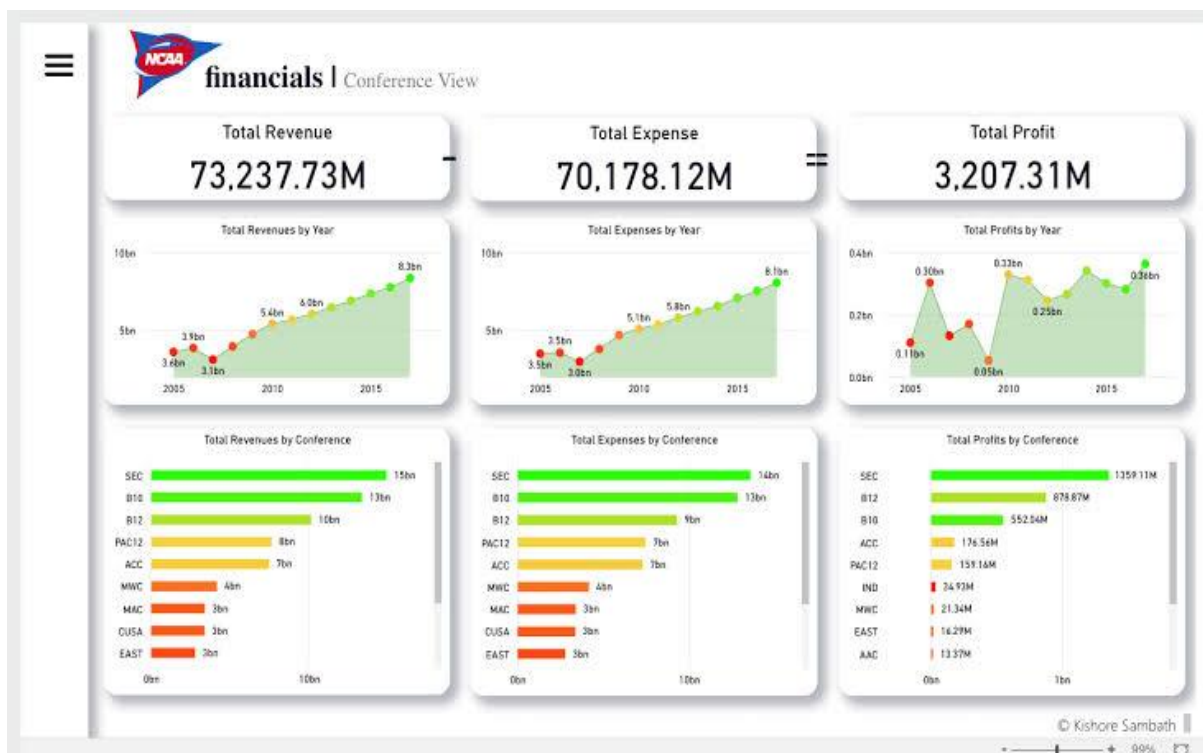
Revenue per cookie

Units Sold

Year

Country	Product	Units Sold	Revenue per cookie	Cost per cookie	Revenue	Cost	Profit	Date	Month Number	Month Name	Year
Mexico	Fortune Cookie	1368	\$1.00	\$0.20	\$1,368.00	\$273.60	\$1,094.40	02 January 2019	2	February	20
Mexico	Fortune Cookie	546	\$1.00	\$0.20	\$546.00	\$109.20	\$436.80	10 January 2019	10	October	20
Canada	Fortune Cookie	2300	\$1.00	\$0.20	\$2,300.00	\$460.00	\$1,840.00	12 January 2019	12	December	20
Canada	Fortune Cookie	388	\$1.00	\$0.20	\$388.00	\$77.60	\$310.40	09 January 2019	9	September	20
Canada	Fortune Cookie	200	\$1.00	\$0.20	\$200.00	\$40.00	\$160.00	05 January 2019	5	May	20
Germany	Fortune Cookie	1199	\$1.00	\$0.20	\$1,199.00	\$239.80	\$959.20	04 January 2019	4	April	20
Canada	Fortune Cookie	2227.5	\$1.00	\$0.20	\$2,227.50	\$445.50	\$1,782.00	01 January 2019	1	January	20
France	Fortune Cookie	293	\$1.00	\$0.20	\$293.00	\$58.60	\$234.40	02 January 2019	2	February	20
Canada	Fortune Cookie	1249	\$1.00	\$0.20	\$1,249.00	\$249.80	\$999.20	10 January 2019	10	October	20
Mexico	Fortune Cookie	2255	\$1.00	\$0.20	\$2,255.00	\$451.00	\$1,804.00	07 January 2019	7	July	20
Mexico	Fortune Cookie	604	\$1.00	\$0.20	\$604.00	\$120.80	\$483.20	06 January 2019	6	June	20
United States	Fortune Cookie	1298	\$1.00	\$0.20	\$1,298.00	\$259.60	\$1,038.40	02 January 2019	2	February	20
United States	Fortune Cookie	982.5	\$1.00	\$0.20	\$982.50	\$196.50	\$786.00	01 January 2019	1	January	20
Mexico	Fortune Cookie	2661	\$1.00	\$0.20	\$2,661.00	\$532.20	\$2,128.80	05 January 2019	5	May	20
Canada	Fortune Cookie	2734	\$1.00	\$0.20	\$2,734.00	\$546.80	\$2,187.20	10 January 2019	10	October	20
Mexico	Fortune Cookie	2420	\$1.00	\$0.20	\$2,420.00	\$484.00	\$1,936.00	09 January 2019	9	September	20
France	Fortune Cookie	1773	\$1.00	\$0.20	\$1,773.00	\$354.60	\$1,418.40	04 January 2019	4	April	20
United States	Fortune Cookie	677	\$1.00	\$0.20	\$677.00	\$135.40	\$541.60	03 January 2019	3	March	20
Mexico	Fortune Cookie	2157	\$1.00	\$0.20	\$2,157.00	\$431.40	\$1,725.60	12 January 2019	12	December	20
Germany	Fortune Cookie	766	\$1.00	\$0.20	\$766.00	\$153.20	\$612.80	01 January 2019	1	January	20
France	Fortune Cookie	2072	\$1.00	\$0.20	\$2,072.00	\$414.40	\$1,657.60	12 January 2019	12	December	20
United States	Fortune Cookie	2313	\$1.00	\$0.20	\$2,313.00	\$462.60	\$1,850.40	05 January 2019	5	May	20
United States	Fortune Cookie	2328	\$1.00	\$0.20	\$2,328.00	\$465.60	\$1,862.40	09 January 2019	9	September	20
United States	Fortune Cookie	2797	\$1.00	\$0.20	\$2,797.00	\$559.40	\$2,237.60	12 January 2019	12	December	20
Canada	Fortune Cookie	2321	\$1.00	\$0.20	\$2,321.00	\$464.20	\$1,856.80	11 January 2019	11	November	20
France	Fortune Cookie	1666	\$1.00	\$0.20	\$1,666.00	\$333.20	\$1,332.80	05 January 2019	5	May	20
Canada	Fortune Cookie	3802.5	\$1.00	\$0.20	\$3,802.50	\$760.50	\$3,042.00	04 January 2019	4	April	20
Germany	Fortune Cookie	711	\$1.00	\$0.20	\$711.00	\$142.20	\$568.80	12 January 2019	12	December	20
France	Fortune Cookie	1562	\$1.00	\$0.20	\$1,562.00	\$312.40	\$1,249.60	08 January 2019	8	August	20

Table: Sheet1 (525 rows, 70 filtered rows) Column: Product (6 distinct values, 1 filtered distinct values)

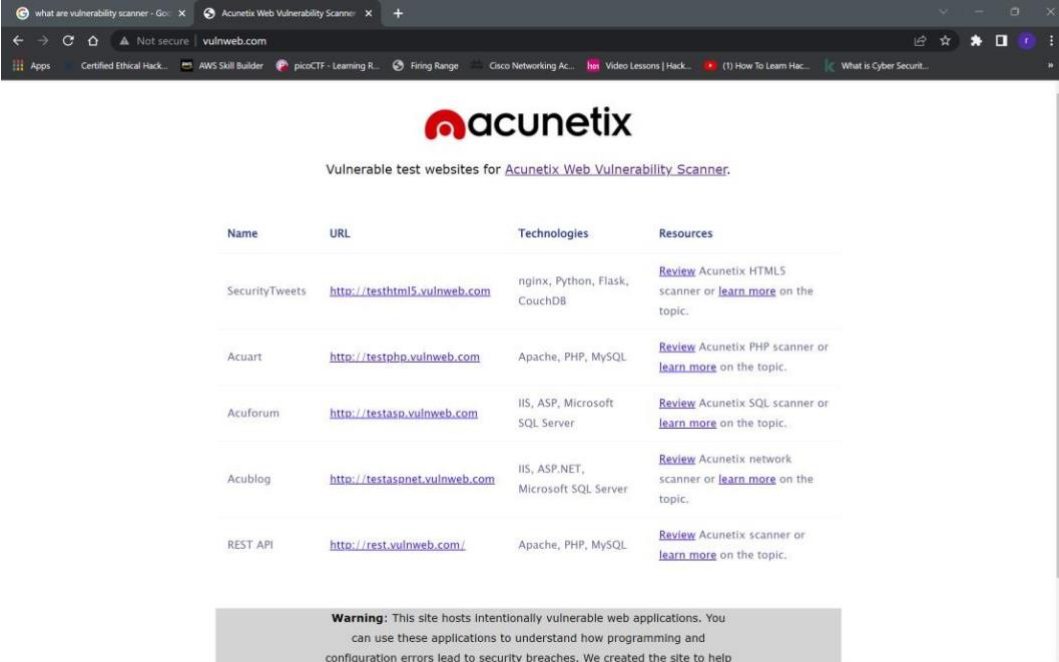


Practical 6: Vulnerability scanner

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. These scanners are used to discover the weaknesses of a given system.

Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting

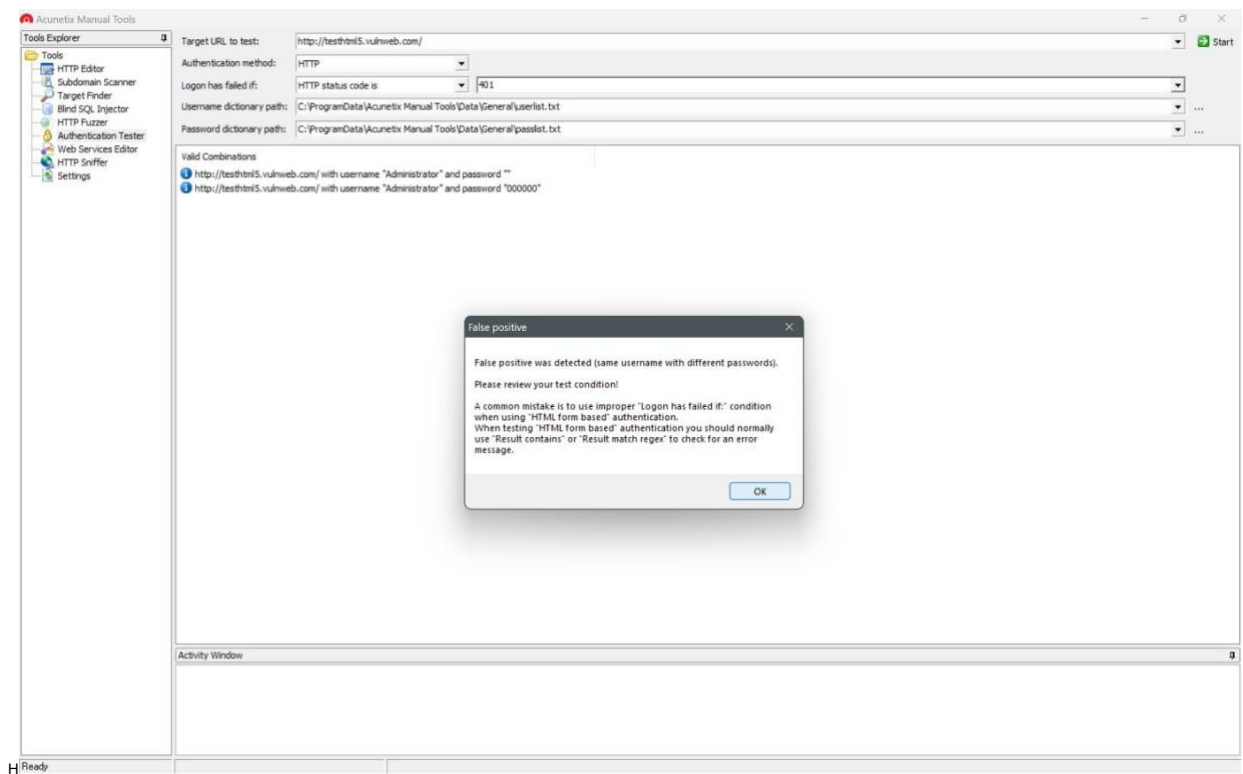
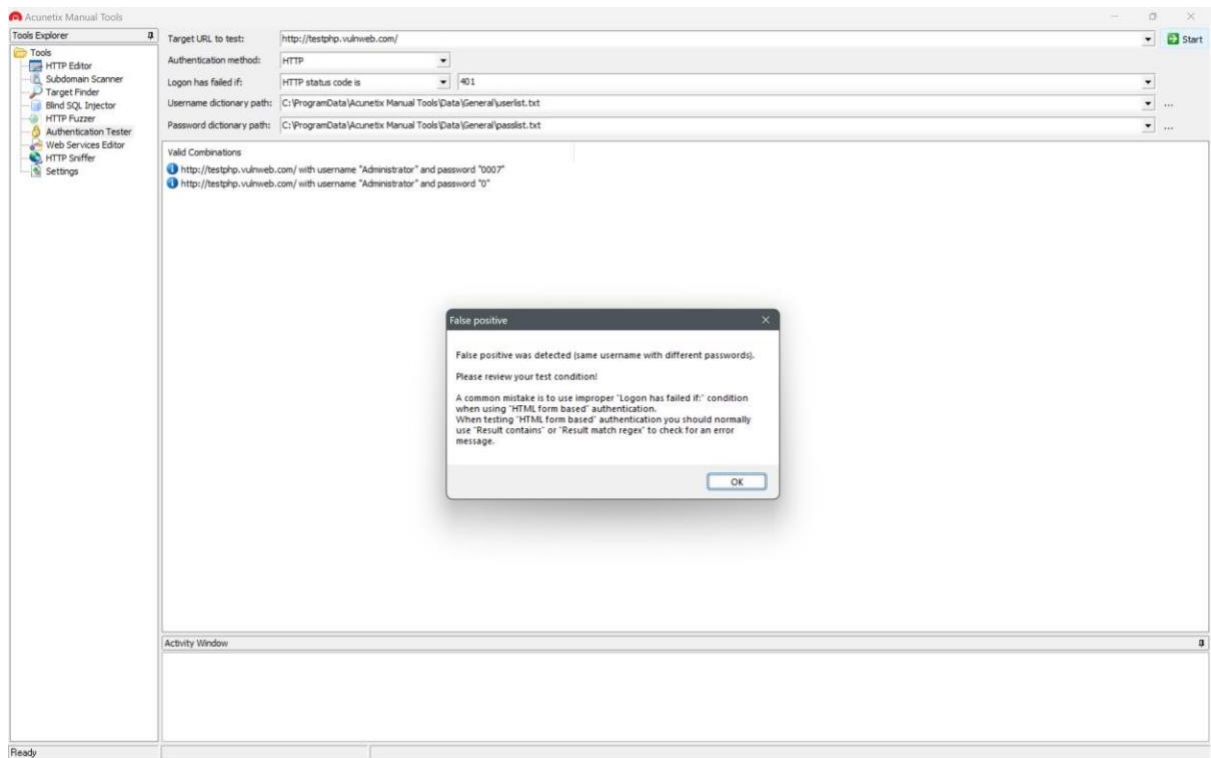
and other exploitable vulnerabilities.



The screenshot shows a web browser window with the address bar displaying "vulnweb.com". The page features the Acunetix logo at the top, followed by the text "Vulnerable test websites for Acunetix Web Vulnerability Scanner." Below this is a table with four columns: Name, URL, Technologies, and Resources. The table lists five test websites: SecurityTweets, Acuart, Acuforum, Acublog, and REST API. Each entry includes a brief description of the technologies used and a link to review or learn more about the scanner. A warning box at the bottom states: "Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help".

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testasnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help



Practical 7: browser inspect get password

Convert the password from "****" format to "text"

Go in inspect

Find the div of input type =password

Change it to 'text'

```
<input type="hidden" name="timeStmp" id="timeStmp" value>
<input type="hidden" name="secTok" id="secTok" value>
▶ <div class="email-div">...</div>
▼ <div class="passwd-div">
  ▶ <label for="Passwd">...</label>
  <input type="password" name="Passwd" id="Passwd">
</div>
<input type="submit" class="g-button g-button-submit" name="signIn"
"signIn" value="Sign in">
▶ <label class="remember" onclick>...</label>
<input type="hidden" name="rmShown" value="1">
```



```
<fieldset class="fields1">
  ▶ <dl>...</dl>
  ▼ <dl>
    ▼ <dt>
      <label for="password">Password:</label>
    </dt>
    ▼ <dd>
      <input type="text" tabindex="2" id="password" name="password" size="25"
    </dd>
    ▼ <dd>
      <a href="http://www.groovypost.com/forum/ucp.php?mode=sendpassword">I for
    </dd>
    ▶ <dd>...</dd>
  </dl>
  ▶ <dl>...</dl>
  <input type="hidden" name="redirect" value="./ucp.php?mode=login">
```

groovyPost.com