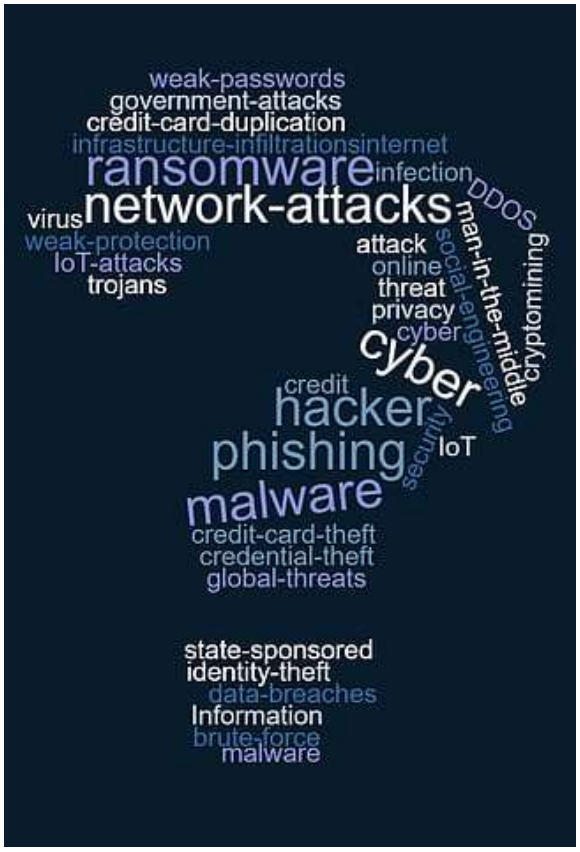


PROJECT REPORT

BY Team 1.1

VULNERABILITY ASSESSMENT

The project aim to practice and explore vulnerabilities in web security

Teen Hacker

AI for Cyber Security with IBM Qradar

Table of Content

Project Details

The project aim find and test vulnerabilities in websites that involves several key steps and considerations. Here are some project details include:

Objective and Scope Definition:

The mainly focus on testing OWASP TOP Ten vulnerabilities in practice to gain hands on experience in exploiting vulnerabilities. Later, use this skill to test it in main website to gain real world pentesting experience.

The practice web site chosen is a vulnerable website and main website is any real world website to test vulnerabilities.

Website Selection:

The practice website is chosen from open source vulnerable that is solely made for vulnerability concept learning.

The main website selection is entirely depend on us and all test were done without approvals. The purpose of this operation is only for learning with no intention to harm any companies.

Research and Tools:

Research common vulnerabilities and attack vectors in web applications.

Tools used in the project are available in Kali Linux like Nmap, nikto , DNSLookup except Tenable Nessus.

Vulnerability Identification:

Conduct automated vulnerability scans to identify common weaknesses like SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other OWASP vulnerabilities and mapping with CWE and OWASP category.

Perform manual testing is also done to exploit the vulnerabilities based on scanned result.

Documentation and Reporting:

Document each identified vulnerability, including its nature, severity, and potential impact.

Provide clear and detailed reports on how the vulnerabilities were found and exploited, along with suggestions for remediation.

Ethical and Legal Compliance:

During project, ethical considerations and compliance with legal regulations are ensured. Explicit permission to test and avoid causing any damage to the websites is taken.

Risk Analysis and Mitigation:

The potential risks associated with each vulnerability are analysed and suggest mitigation strategies to fix the issues.

Vulnerabilities are prioritized based on severity and potential impact on the website's security.

Abstract

In today's interconnected world, the rapid growth of technology has brought about numerous advantages, but it has also given rise to new security challenges. To counteract the increasing sophistication of cyber threats, the integration of Artificial Intelligence (AI) in Intrusion Detection Systems (IDS) has become imperative. This project, “Enhanced AI-Enhanced Intrusion Detection System," aims to explore and develop an IDS that leverages advanced AI techniques for more accurate and efficient threat detection. The primary objective of this project is to enhance traditional IDS capabilities by implementing cutting-edge AI algorithms. This will enable the system to not only detect known attack patterns but also identify emerging and previously unknown threats. Machine learning models, deep learning, and anomaly detection techniques will be employed to continuously adapt to evolving attack strategies.

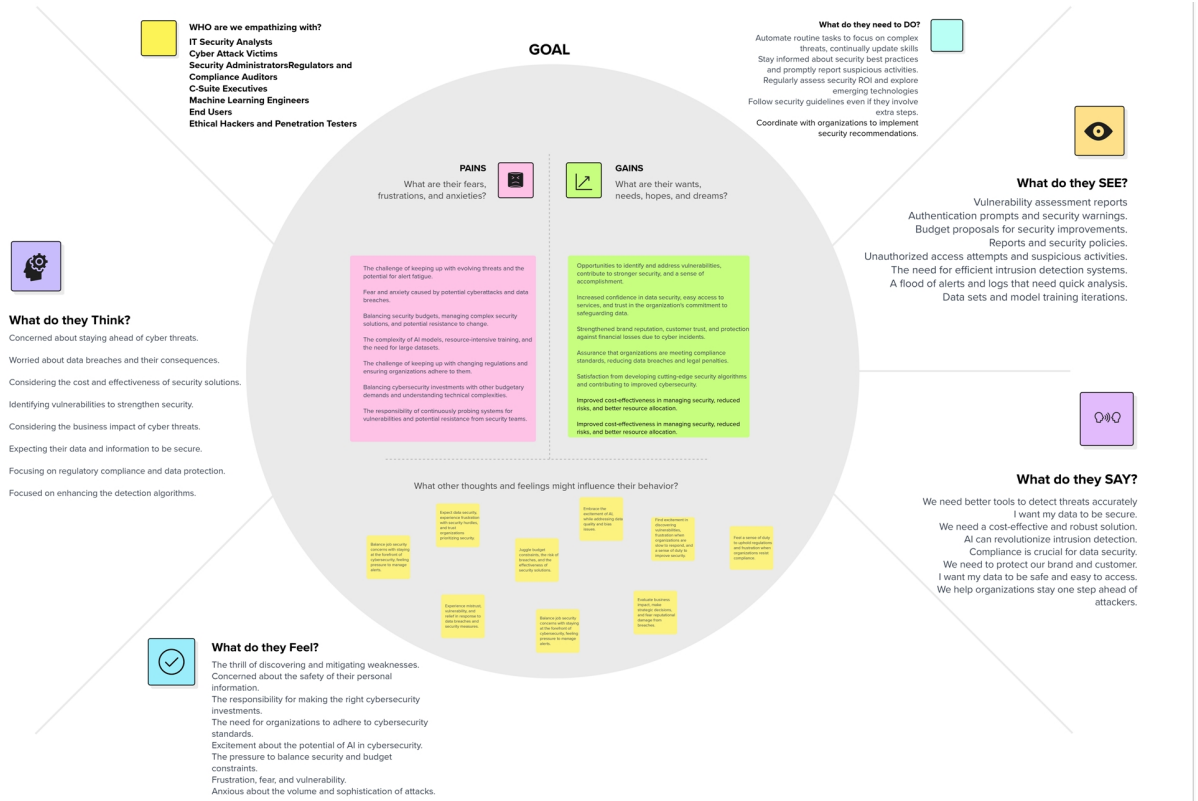
Key components of this project include:

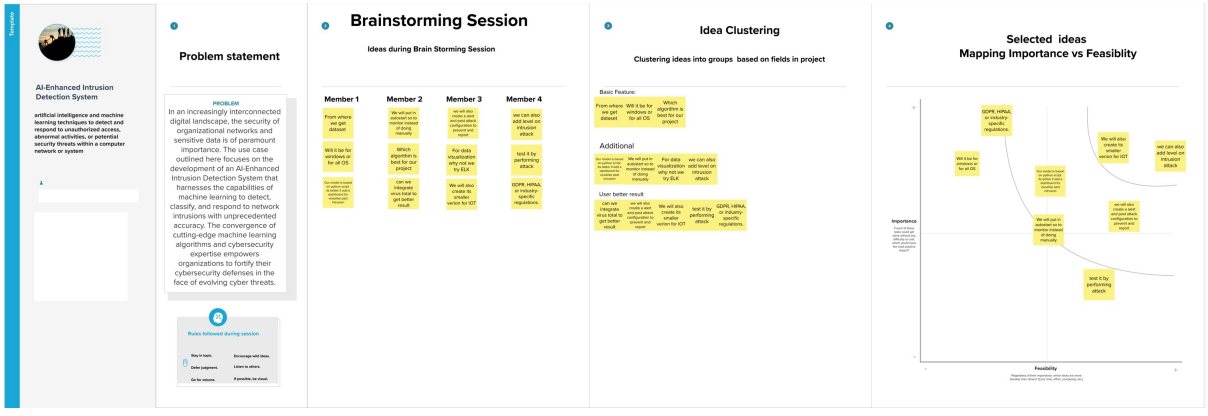
1. Data Collection and Pre-processing: Gathering and pre-processing network traffic data to create a clean and representative dataset for training AI models.

2. AI Model Development: Designing and training machine learning and deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and clustering algorithms, to identify patterns and anomalies in network traffic.

3. Real-Time Monitoring: Implementing a real-time monitoring system that continuously assesses network traffic for potential threats, providing immediate alerts and automated responses when anomalies are detected.

Supporting Documents





Stage 1

Overview:-

The project help us to understand the cyber security concepts and implement in real life. It provides a though understanding from basic to conceptual level and this project is an example of our hands on experience. It opens an opportunity to extend our carrier in field of cyber security in pentesting , security audits, security analyst, network security engineer, security consultant .We use our course knowledge to find analyse website using nmap, Tenable Nessus and Metaspoilt. Due to best understanding and knowledge in it, we are able to learn to exploit vulnerability from vulnerable website (mainly OWASP Top 10) and then implement it to analyse in our main website With the guidance our mentor, we are able to perform scans to check whether a particular website has vulnerabilities or not and based on result, we perform operation. It also gives the understanding of how to report bug when found in websites and its procedures. Analysing vulnerability is not only about tools and coding, it needs a basic understanding of programming language to know what developer did error in code handling to patch it.

List of teammates-

S. no	Name	College	Contact
1.	Tanishq Sati	VIT-AP	+91 7818026932
2.	Hrishik Manoj	VIT-AP	+91 8347136133
3.	Sheikha Farook Batha	VIT-AP	+91 9074251321
4.	Rishabh	VIT-AP	+91 8507480604

Vulnerability Table-

S.no	Vulnerability Name	CWE-No
1.	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE-89
2.	Improper input validation	CWE 20
3.	Sensitive data exposure	CWE 200
4.	Security misconfiguration	CWE-16 , CWE-611
5.	Broken access control	CWE-284
6.	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CWE-79
7.	Forged Feedback(data sent can't verified authentic or not)	CWE-345
8.	Broken Authentication	CWE-287
9.	Captcha Bypass(Broken Anti Authentication)	CWE-307
10.	Login Admin	CWE-89

Vulnerability Report

1)

Vulnerability Name: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CWE: CWE-89

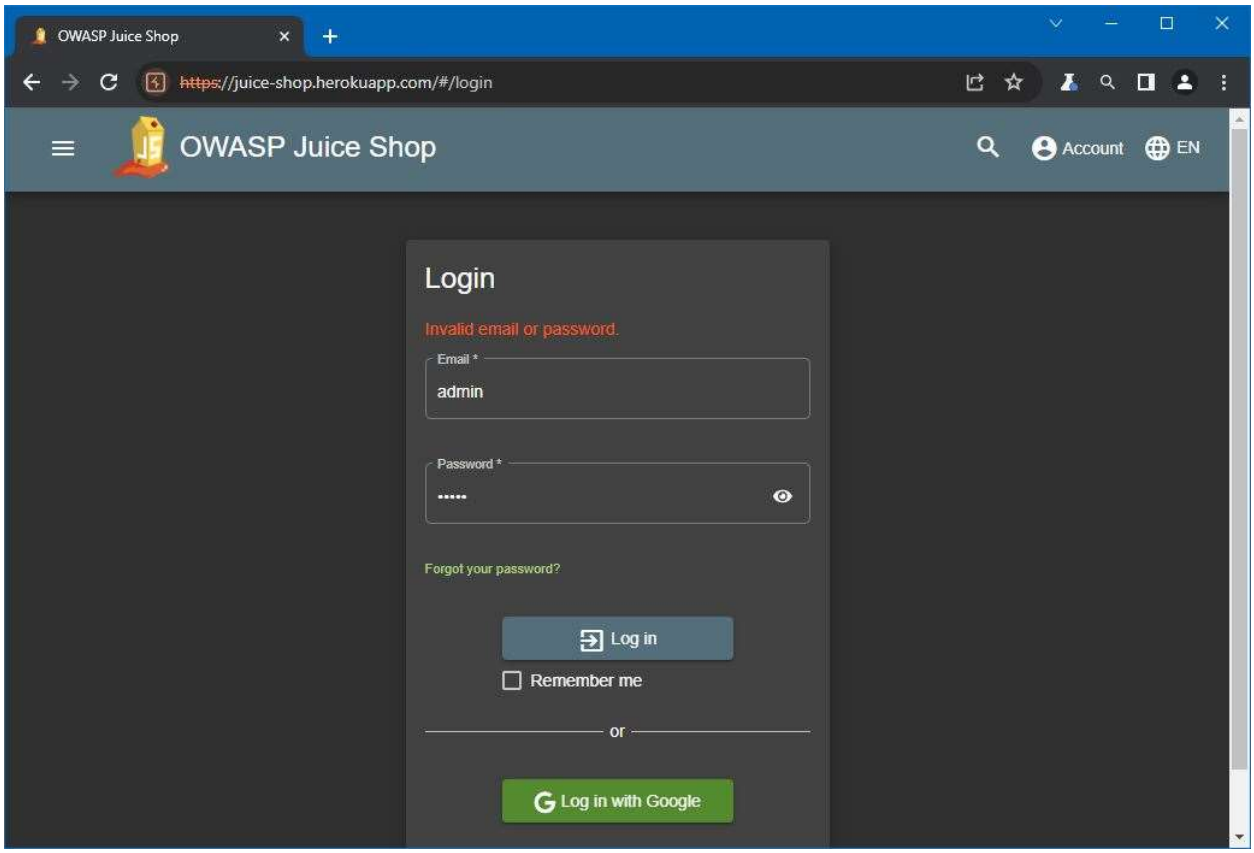
OWASP Category:-A03:2021

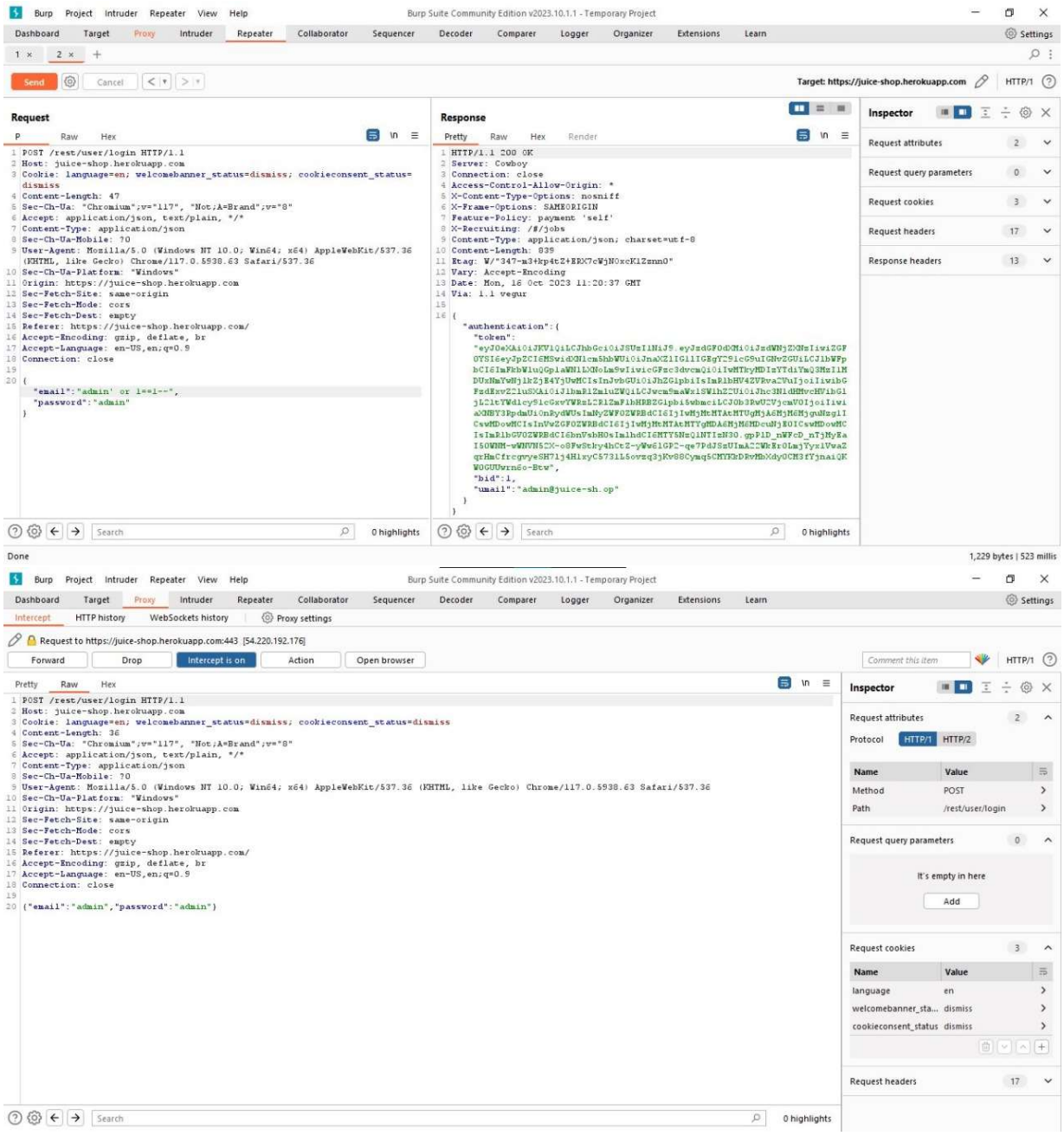
Description:

CWE-89, titled "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')," is a common software vulnerability that occurs when an application does not properly validate or sanitize user inputs before including them in SQL queries.

Business Impact:

CWE-89, or SQL injection, poses a severe business impact. This vulnerability can lead to data breaches, causing financial losses, legal repercussions, and reputational damage. Data theft compromises sensitive customer information and intellectual property, eroding trust and potentially triggering costly legal actions


OWASP Juice Shop
https://juice-shop.herokuapp.com/#/login
OWASP Juice Shop
Account
EN
Login
Invalid email or password.
Email *
admin
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google



2)

Vulnerability Name: Improper input validation

CWE: CWE 20

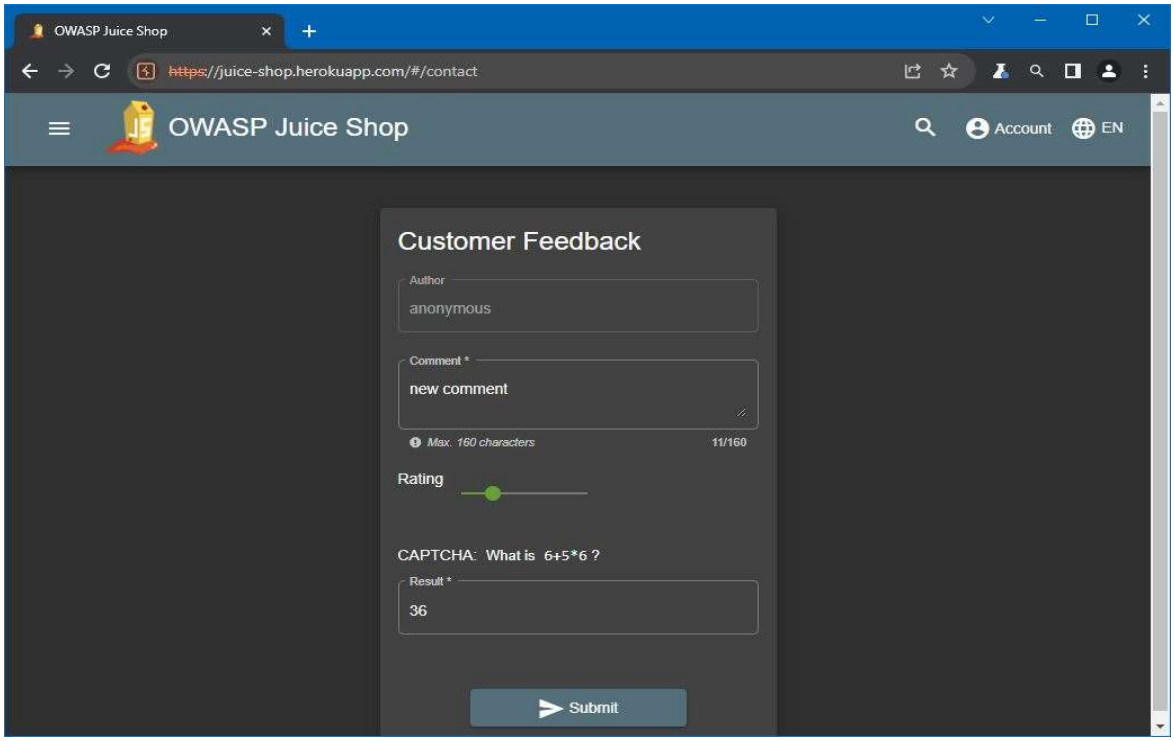
OWASP Category:-A03:2021, A04:2021, A05:2021

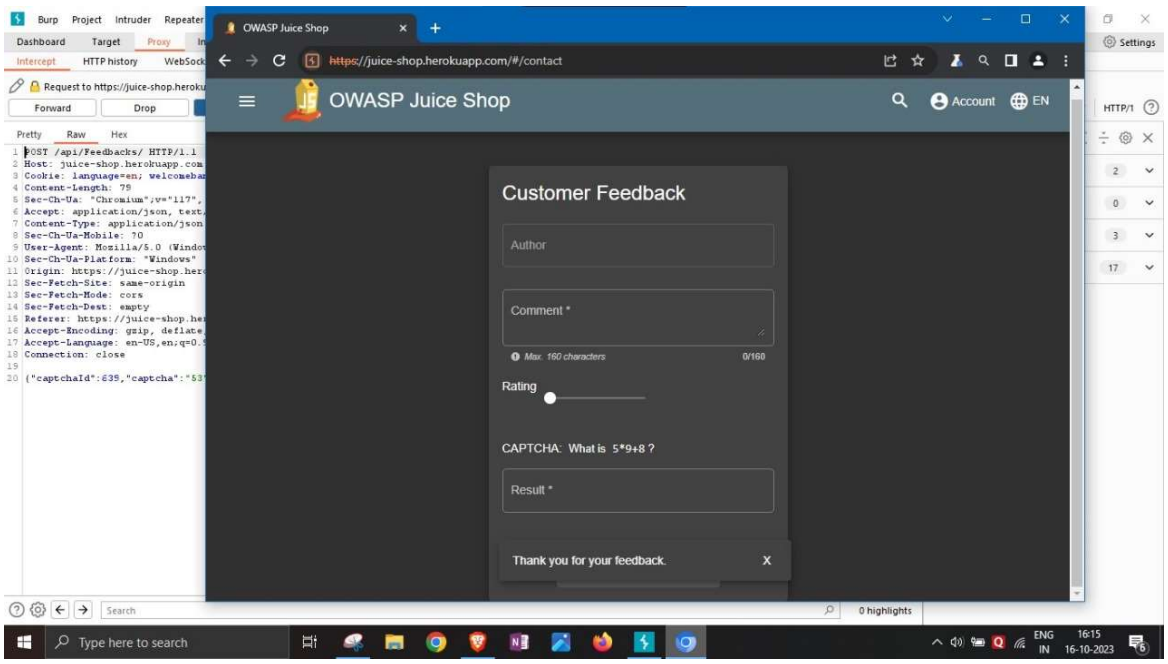
Description:

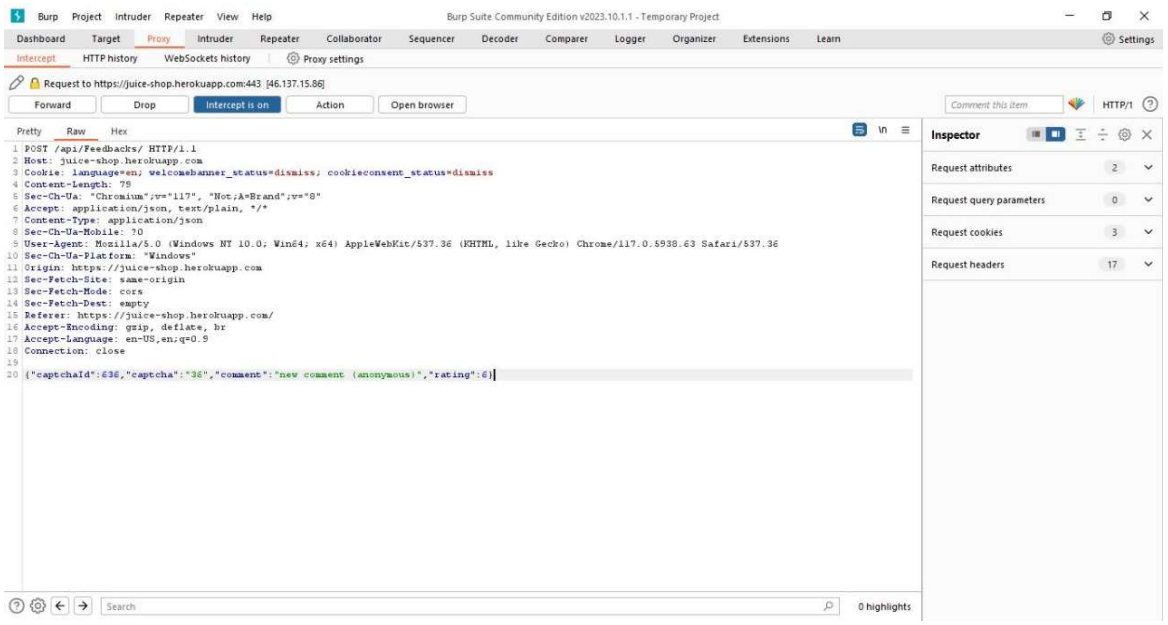
CWE-20, also known as "Improper Input Validation," is a software weakness that occurs when a program does not adequately validate and sanitize user inputs. This can lead to security vulnerabilities such as buffer overflows, SQL injection, and cross-site scripting.

Business Impact:

CWE-20 can have a significant business impact, including data breaches, financial losses, reputation damage, and legal liabilities. Vulnerabilities arising from improper input validation can allow attackers to exploit software, leading to unauthorized access, data theft, and service disruptions, potentially resulting in customer trust erosion and costly remediation efforts.







3)

Vulnerability Name: Sensitive data exposure

CWE: CWE 200

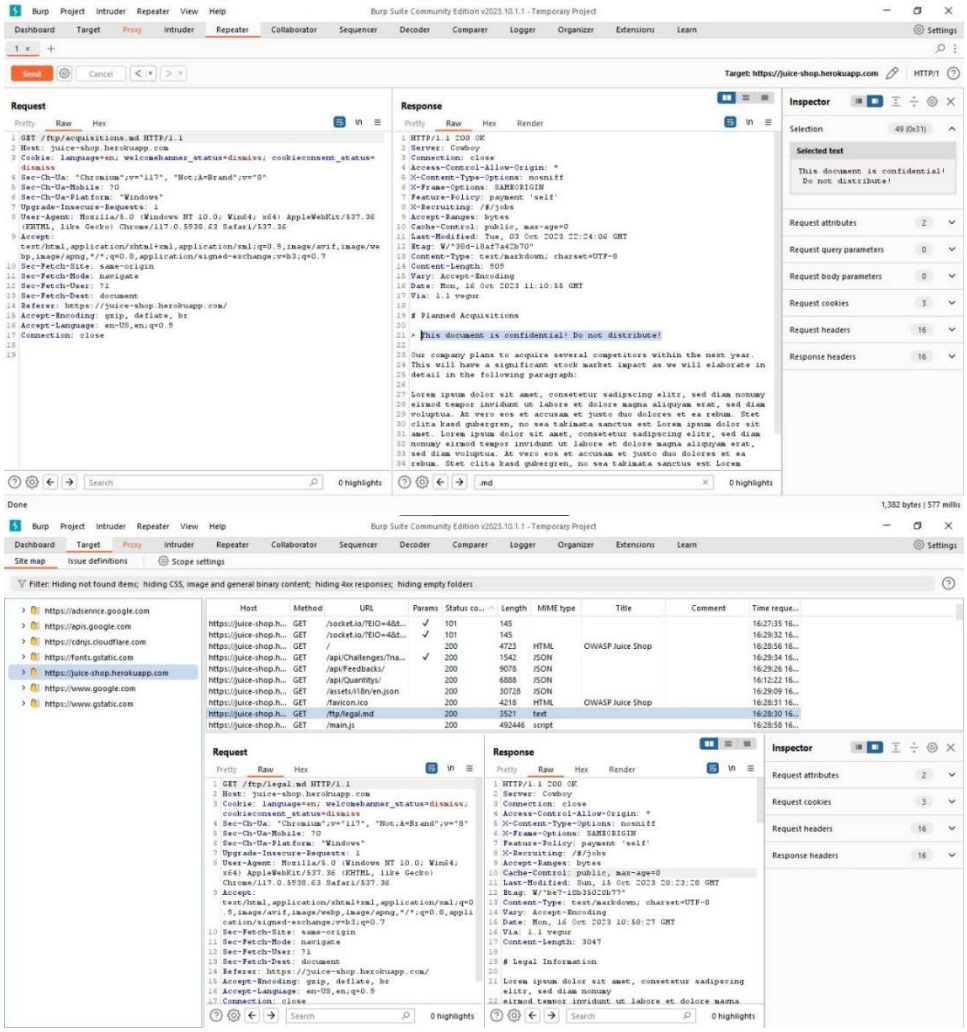
OWASP Category:- A02:2021

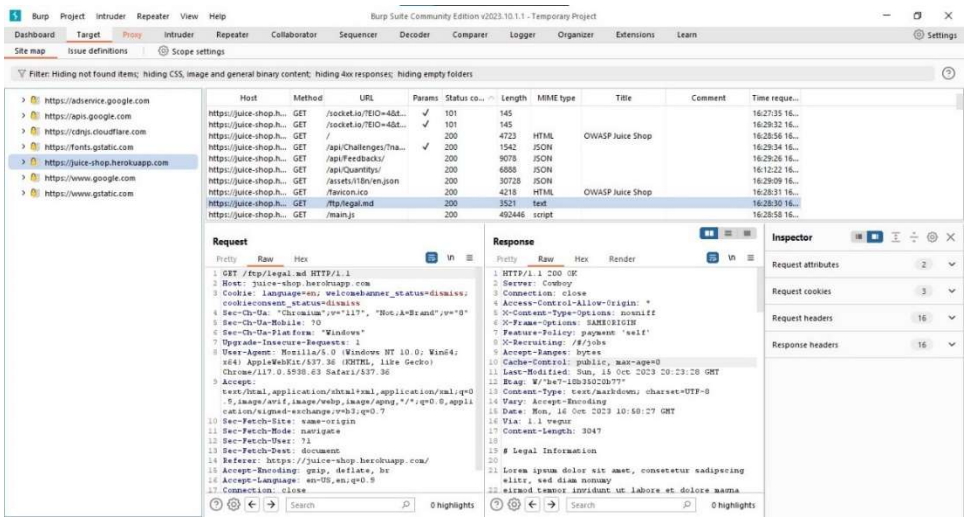
Description:

CWE-200, known as "Exposure of Sensitive Information to an Unauthorized Actor," represents a security weakness where sensitive data, like passwords, encryption keys, or personal information, is improperly disclosed to unauthorized individuals or systems. This vulnerability can lead to serious breaches, compromising privacy and security.

Business Impact:

CWE-200 can result in severe business consequences, including reputational damage, loss of customer trust, legal consequences, and financial losses. Exposing sensitive information to unauthorized actors can lead to data breaches and regulatory fines, impacting an organization's bottom line and causing long-term damage to its brand and operations.





4)

Vulnerability Name: Security misconfiguration

CWE:- CWE-16 , CWE-611

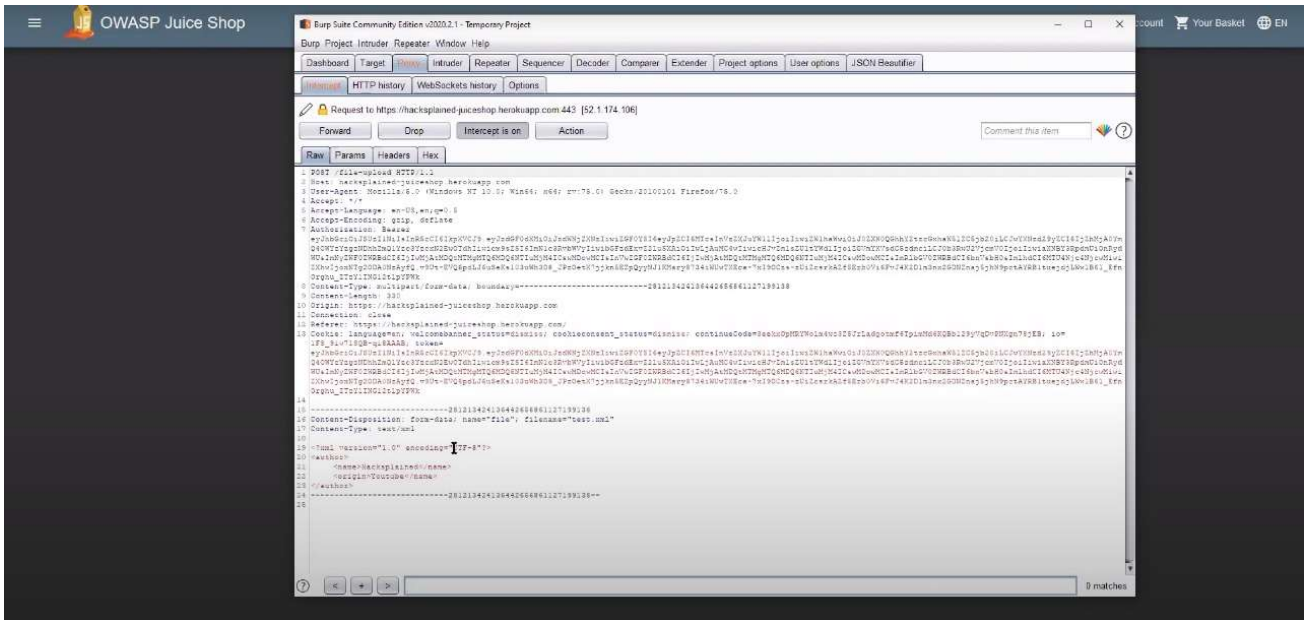
OWASP Category: - A05:2021

Description:

Security misconfiguration vulnerabilities occur when a system, application, or component is improperly set up, leaving it exposed to potential attacks. These weaknesses can lead to unauthorized access, data breaches, or other security incidents due to poorly configured permissions, default settings, or unnecessary features being enabled.

Business Impact:

Security misconfigurations can have significant business impacts, including data breaches, downtime, regulatory fines, and reputational damage. Improperly configured systems or applications can lead to unauthorized access, data exposure, and service disruptions. These incidents can result in financial losses, eroded customer trust, and legal consequences, affecting an organization's bottom line and market standing. Proper configuration management is essential to mitigate these risks.



5)

Vulnerability Name: Broken access control

CWE :- CWE-284

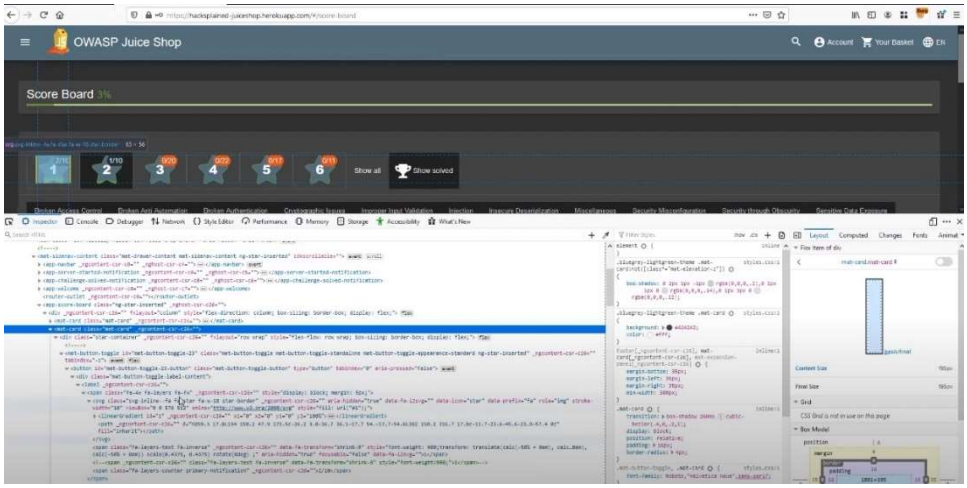
OWASP Category: - A01:2021

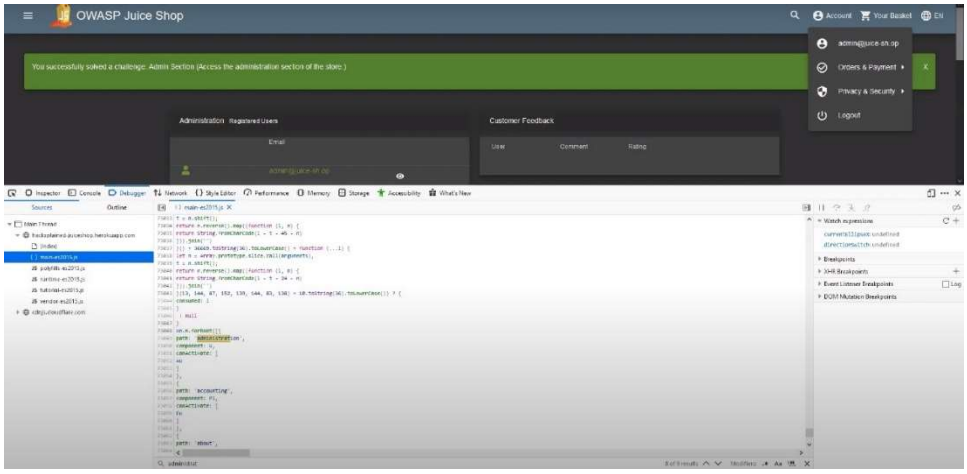
Description:

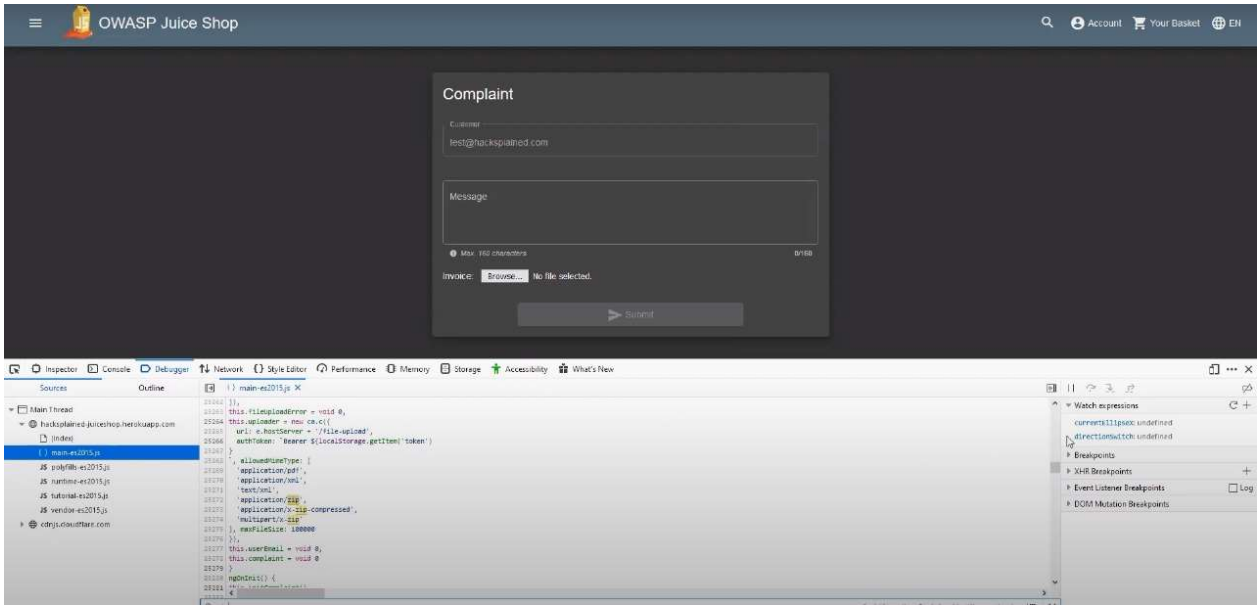
Broken access control is a security vulnerability that occurs when an application or system fails to enforce proper access restrictions. It allows unauthorized users to access sensitive data, perform actions, or modify resources they should not have permission to access. This issue can lead to unauthorized data exposure, data tampering, and pose significant security risks if not mitigated effectively through access control mechanisms.

Business Impact:

Broken access control can have serious business impacts, including data breaches, compromised privacy, regulatory fines, and damage to reputation. Unauthorized users gaining access to sensitive data or functionality can lead to information theft, legal liabilities, and a loss of customer trust. This can result in financial losses, costs associated with investigations, and remediation efforts, ultimately affecting the organization's financial stability and brand image.


OWASP Juice Shop
Score Board


OWASP Juice Shop
You successfully solved a challenge: Admin Section (Access the administration section of the store.)


OWASP Juice Shop
Complaint
test@hackspalined.com
Message
Invoice:
Browse...
No file selected.
Submit

6)

Vulnerability Name: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

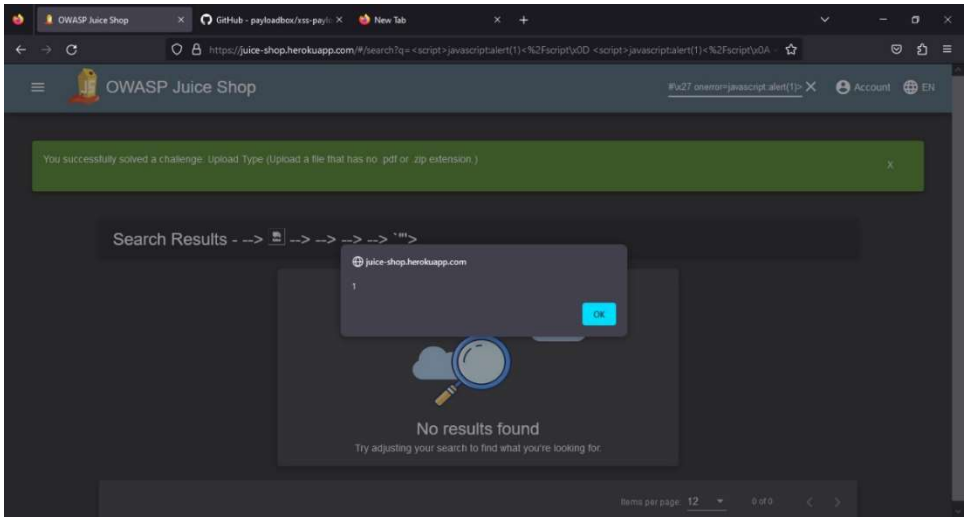
CWE: CWE 79

OWASP Category: - A03:2021

Description:

CWE-79, also known as "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')," is a security vulnerability where an application includes untrusted data in web pages without proper validation. Attackers can inject malicious scripts, enabling them to steal data or perform actions on behalf of users, compromising their security and privacy.

Business Impact:
CWE-79 can have significant business impact, including reputation damage, data breaches, and financial losses. Cross-site scripting vulnerabilities allow attackers to steal sensitive data, compromise user accounts, and deface websites, eroding customer trust and potentially leading to regulatory fines. Organizations may also incur costs for incident response, legal liabilities, and remediation, affecting their bottom line and market standing.



7)

Vulnerability Name: Forged Feedback

CWE:- CWE-345

OWASP category:- A05:2021, A08:2021, A09:2021

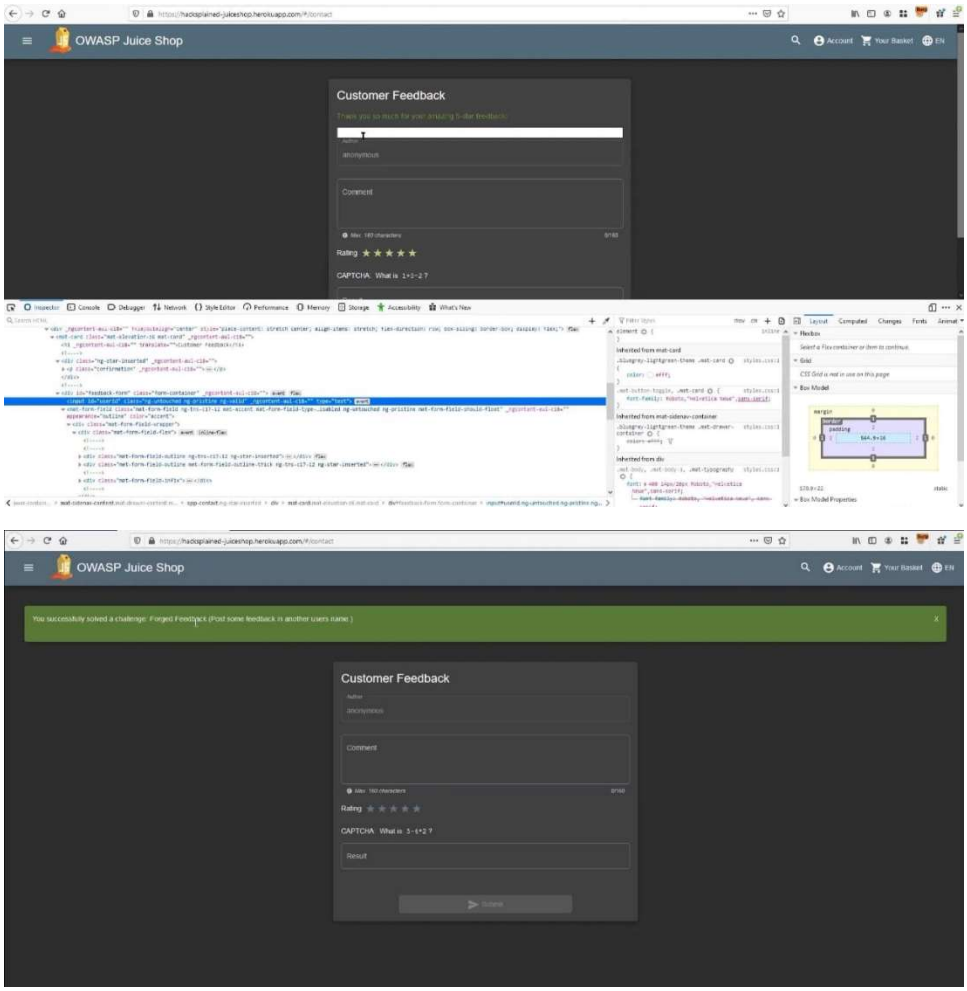
Description:

Forged feedback is a security vulnerability where attackers manipulate or counterfeit feedback or responses from a system to deceive users or systems. This can lead to misinformation, trust

erosion, and potentially security breaches when users make decisions or take actions based on the fraudulent feedback provided.

Business Impact:

Forged feedback vulnerabilities can have a significant business impact, including damage to an organization's reputation, financial losses, and a potential loss of customer trust. Attackers exploiting these weaknesses can deceive users and may lead to actions that compromise security, result in data breaches, or tarnish an organization's image. This can result in costs for incident response, legal liabilities, and long-term harm to the organization's market standing.



8)

Vulnerability Name: Broken Authentication

CWE :- CWE-287

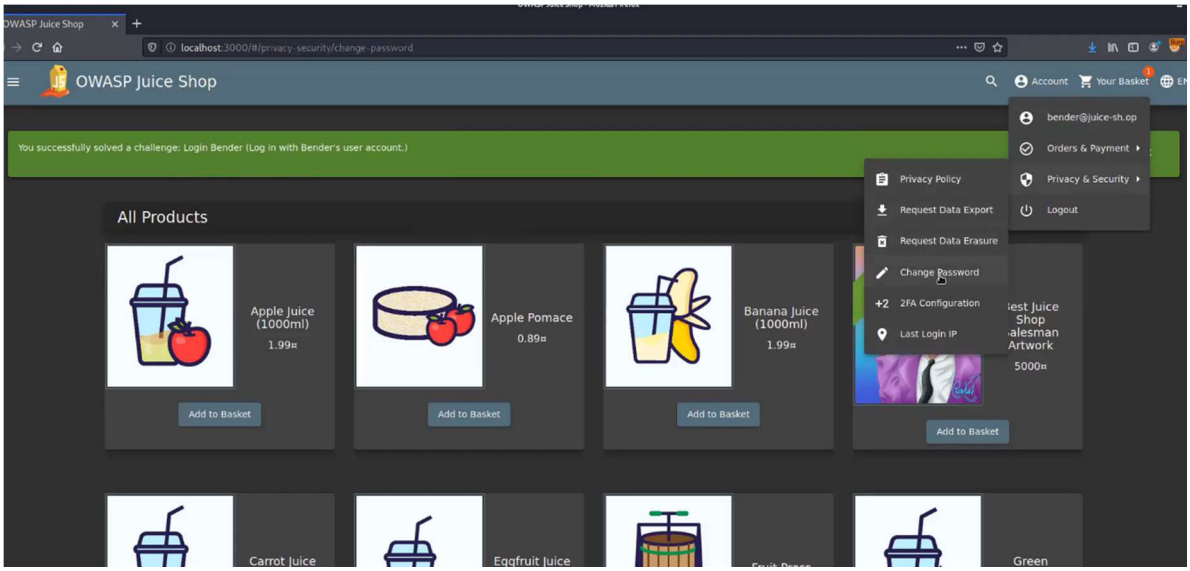
OWASP Category: A07:2021

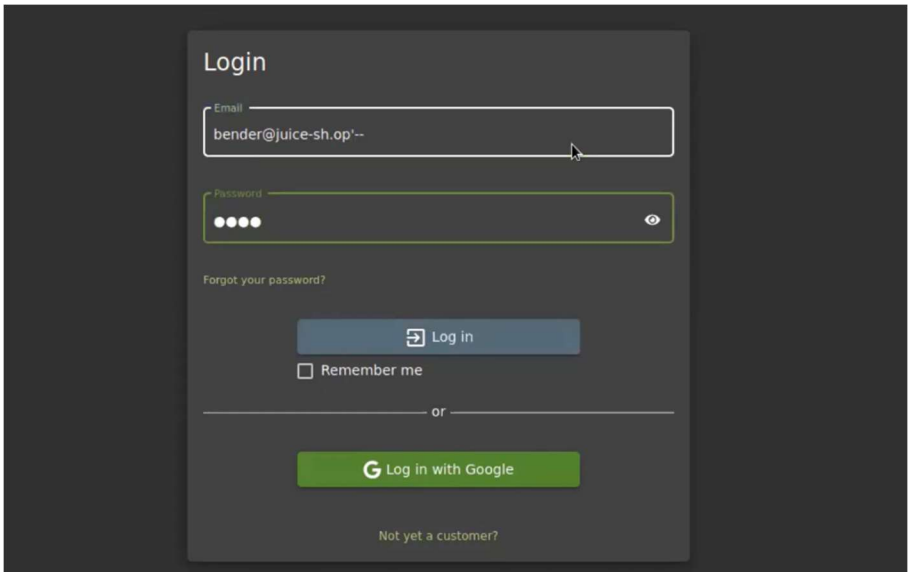
Description:

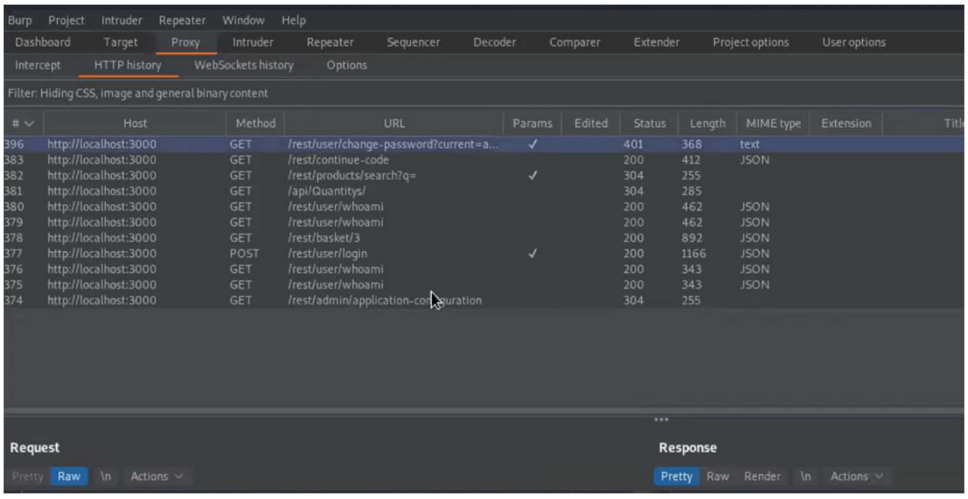
Broken authentication is a security issue where flawed or weak authentication and session management in an application enable unauthorized users to gain access to accounts and data. This can lead to data breaches, reputation damage, legal consequences, and financial losses.

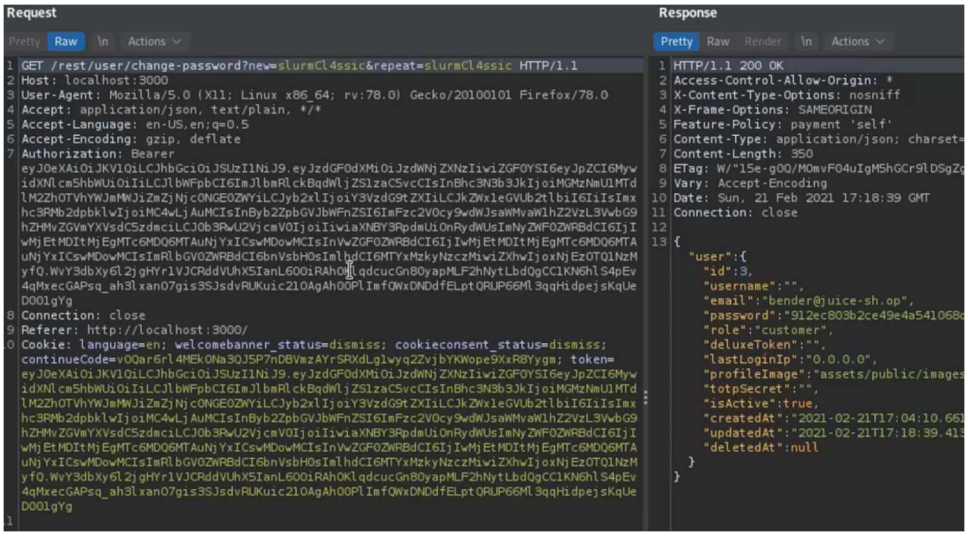
Business Impact:

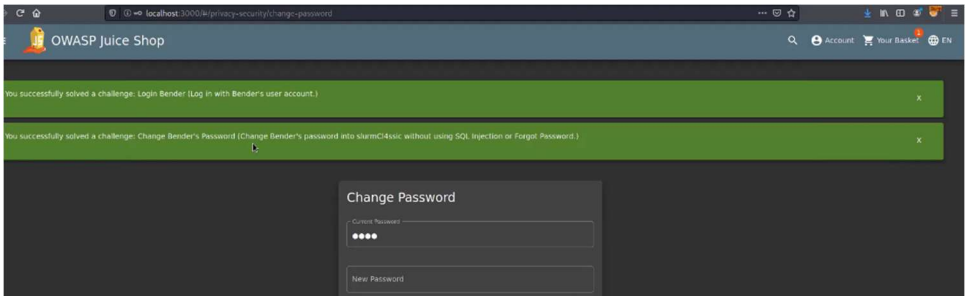
The business impact of broken authentication is significant. It can result in unauthorized access to user accounts and data, leading to data breaches and potentially severe financial losses. It also risks damaging a company's reputation and trust among its customers. Legal consequences and non-compliance with data protection regulations may further compound the impact, resulting in fines and legal actions.











9)

Vulnerability Name: Captcha Bypass(Broken Anti Authentication)

CWE:- CWE-307

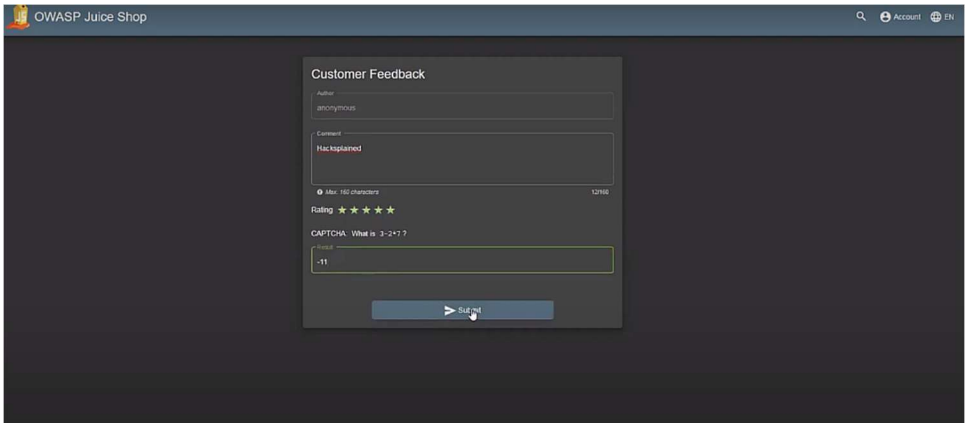
OWASP Category: A07:2021

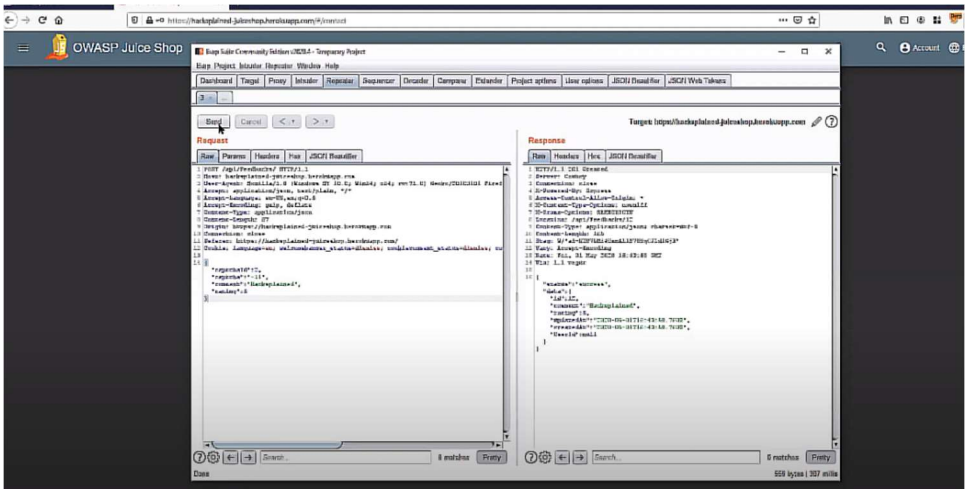
Description:

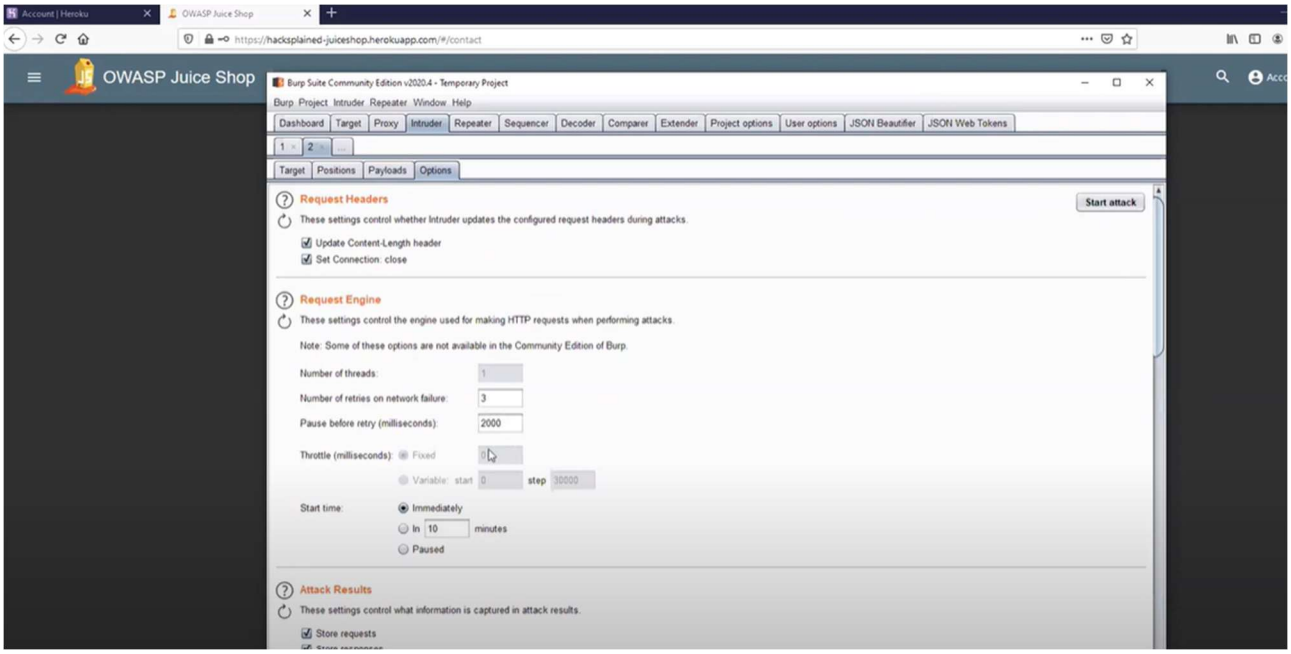
Captcha Bypass, a type of Broken Authentication, is a security vulnerability where automated scripts or attackers circumvent CAPTCHA challenges designed to prevent unauthorized access. By evading these safeguards, attackers can gain access to protected systems, potentially causing data breaches, fraud, or other malicious activities.

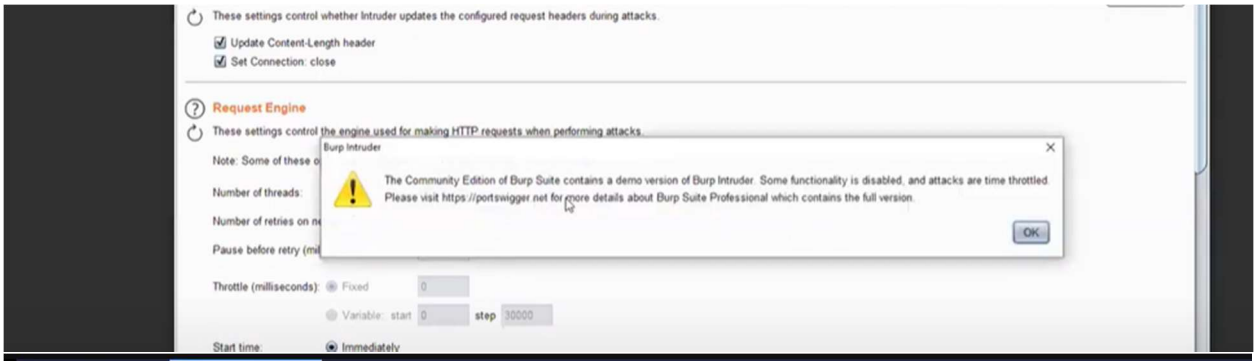
Business Impact:

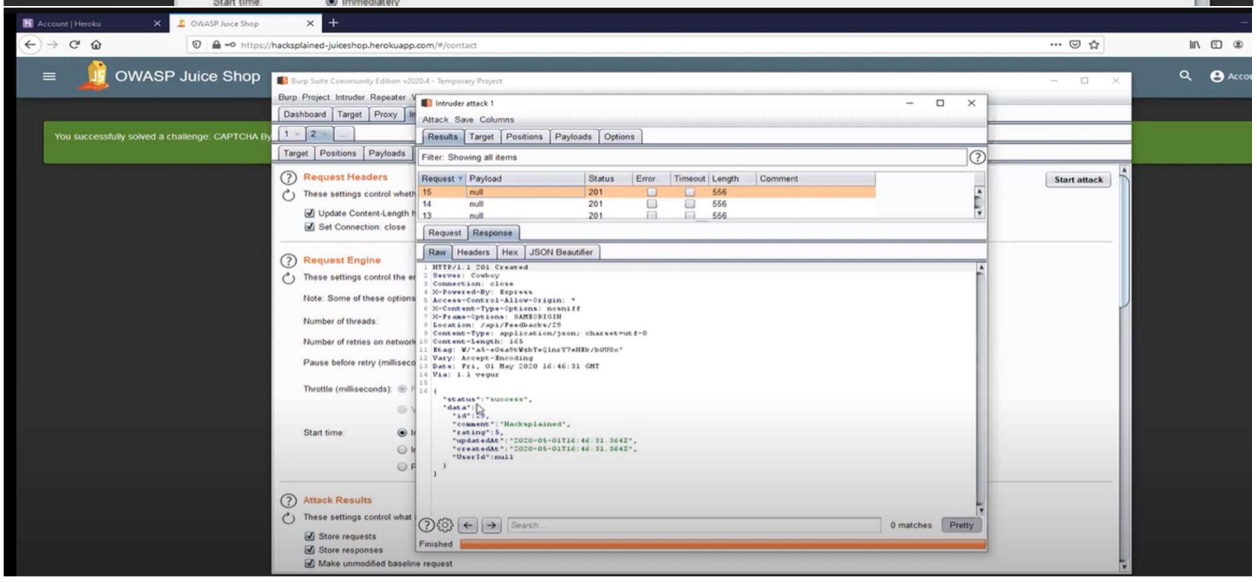
Captcha Bypass, a form of Broken Authentication, can have serious business consequences. By allowing unauthorized users to evade CAPTCHA challenges, it can lead to unauthorized access, fraud, spam, and account takeovers. This undermines user trust, increases operational costs for dealing with fraudulent activities, and may result in reputational damage. Companies may also face legal and regulatory issues if they fail to protect user accounts and data adequately.






OWASP Juice Shop
Burp Suite Community Edition v2020.4 - Temporary Project
Request Headers
Start attack
Update Content-Length header
Set Connection: close
Request Engine
Number of threads:
Number of retries on network failure:
Pause before retry (milliseconds):
Throttle (milliseconds):
Start time:
Immediately
Paused
Attack Results
Store requests


Burp Intruder
The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled.
Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.
OK


OWASP Juice Shop
Intruder attack 1
Results
Target
Positions
Payloads
Options
Request
Response
Raw
Headers
Hex
JSON Beautifier
Start attack

10)

Vulnerability Name: Login Admin(Injection)

CWE:- CWE-89

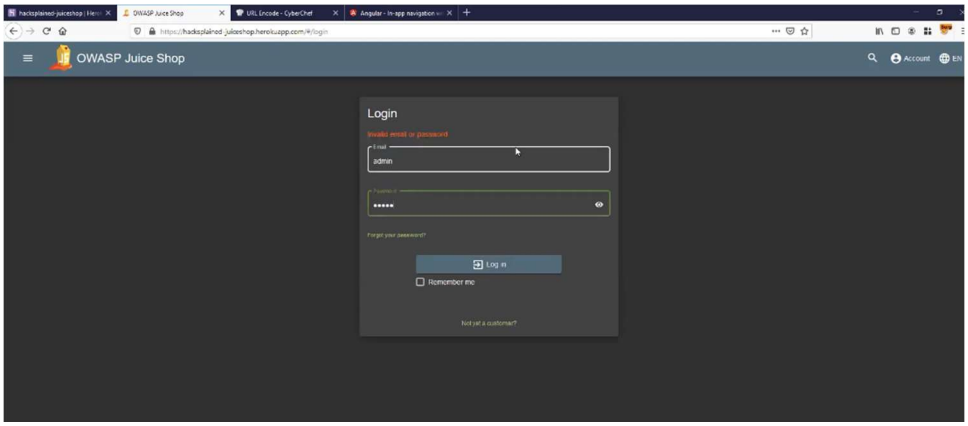
OWASP Category:- A03:2021

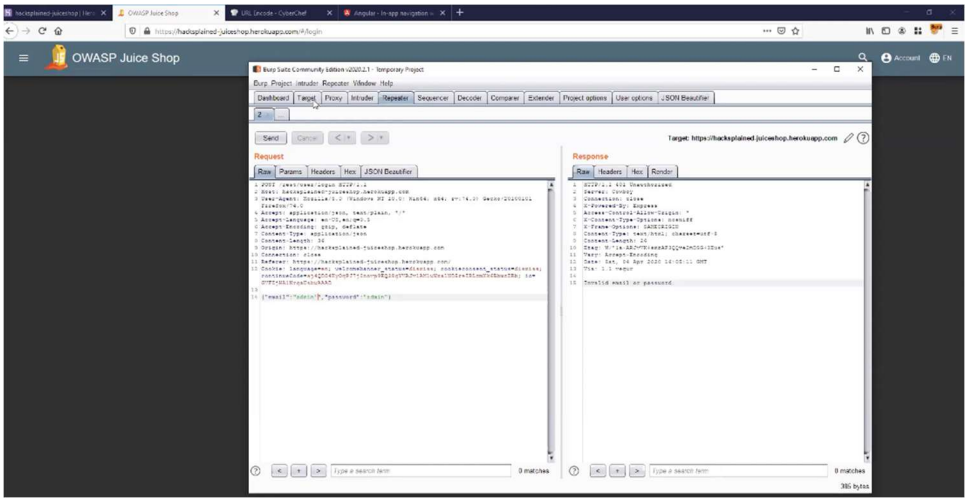
Description:

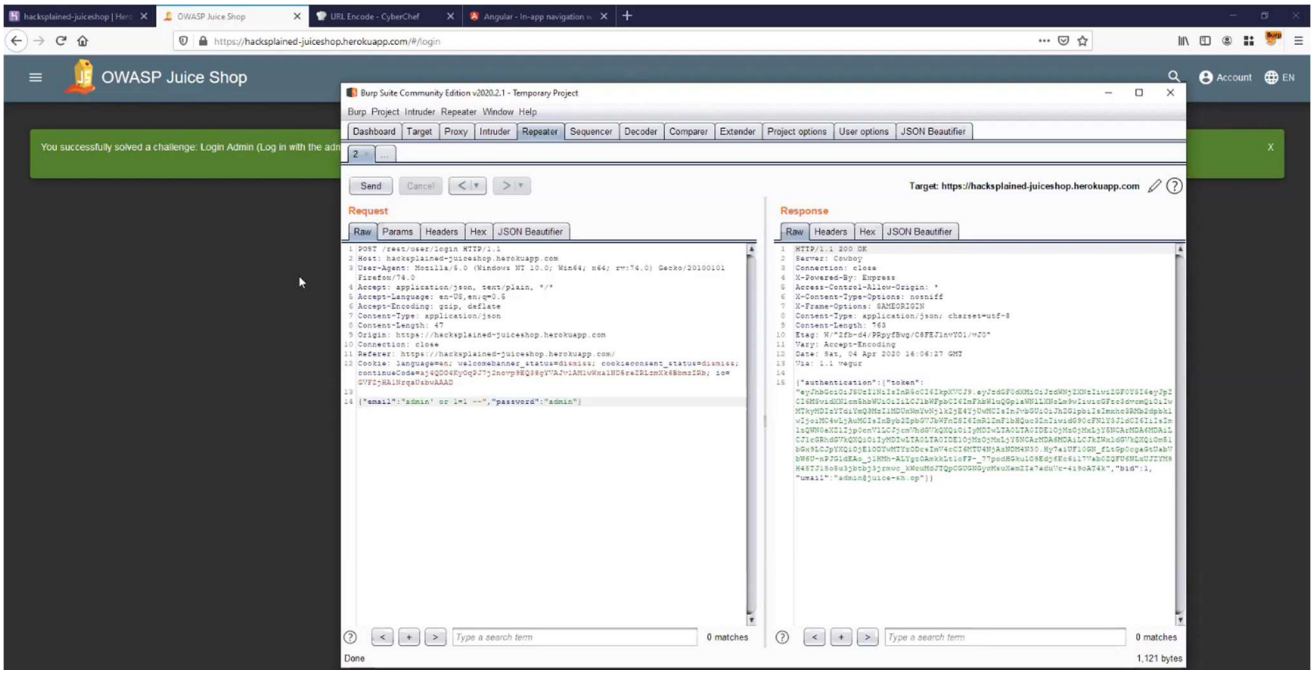
A "login admin(injection)" typically refers to a security vulnerability known as SQL injection, where an attacker manipulates input fields to gain unauthorized access to an admin account on a website or application. This technique involves injecting malicious SQL code, potentially leading to data breaches or system compromises.

Business Impact:

The business impact of a "login admin(injection)" attack can be severe. It can lead to unauthorized access to sensitive data, user accounts, and administrative controls. This can result in data breaches, loss of customer trust, legal repercussions, and financial losses due to legal actions, compliance fines, and costs associated with remediation efforts. It may also damage the company's reputation, affecting future business opportunities and partnerships.






OWASP Juice Shop
Account
EN
You successfully solved a challenge: Login Admin (Log in with the adm
Burp Suite Community Edition v2020.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier
Send
Cancel
Target: https://hacksplained-juiceshop.herokuapp.com
Request
Raw Params Headers Hex JSON Beautifier
Response
Raw Headers Hex JSON Beautifier
Type a search term
0 matches
Done
1,121 bytes


OWASP Juice Shop
Account
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

Tenable Nessus

Nessus is a tool developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

Nessus identifies software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws.

Nessus is known for its vast plugin database. These plugins are dynamically and automatically compiled in the tool to improve its scan performance and reduce the time required to assess, research and remediate vulnerabilities. Plugins can be customized to create specific checks unique to an organization's application ecosystem.

SCORE RANGE	SEVERITY CATEGORY
0.0	None
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

Nessus contains a feature called Predictive Prioritization, which uses algorithms to categorize vulnerabilities by their severity to aid IT teams in determining which threats are most urgent to address. Each vulnerability is assigned a Vulnerability Priority Rating (VPR), which uses a scale from 0 to 10, with 10 being the highest risk, to rate its severity: critical, high, medium or low.

Live Results performs intelligent vulnerability assessment in offline mode with every plugin update. It removes the need to run a scan to validate a vulnerability, creating a more efficient process to assess, prioritize and remediate security issues.

Nessus also provides the ability to create configurable reports in a variety of formats, including Hypertext Markup Language, comma-separated values and Nessus Extensbile Markup Language. Reports can be filtered and customized depending on what information is most useful, such as vulnerability types, vulnerabilities by host, vulnerabilities by client, etc.

Target Website:- http://testfire.net/

Target ip address:- 65.61.137.117

Vulnerability Table (Nessus)

65.61.137.117

0	0	2	1	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information

104743 (1) - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like
1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to anyknown exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk FactorMedium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

65.61.137.117 (tcp/443/www)

```
TLSv1 is enabled and the server supports at least one cipher.
```

157288 (1) - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk FactorMedium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

65.61.137.117 (tcp/443/www)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk FactorLow

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score4.5

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	74733
CVE	CVE-2015-4000
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2022/12/05

Plugin Output

65.61.137.117 (tcp/443/www)

```
Vulnerable connection combinations :SSL/TLS version  : TLSv1.0

  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHADiffie-Hellman MODP size (bits)
  : 1024

    Warning - This is a known static Oakley Group2 modulus. This may makethe remote host
    more vulnerable to the Logjam attack.

  Logjam attack difficulty : Hard (would require nation-state resources)


  SSL/TLS version  : TLSv1.0

  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHADiffie-Hellman MODP size (bits)
  : 1024

    Warning - This is a known static Oakley Group2 modulus. This may makethe remote host
    more vulnerable to the Logjam attack.

  Logjam attack difficulty : Hard (would require nation-state resources)


  SSL/TLS version  : TLSv1.1

  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHADiffie-Hellman MODP size (bits)
  : 1024

    Warning - This is a known static Oakley Group2 modulus. This may makethe remote host
    more vulnerable to the Logjam attack.

  Logjam attack difficulty : Hard (would require nation-state resources)
```

```
  SSL/TLS version  : TLSv1.1

  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHADiffie-Hellman MODP size (bits)
  : 1024

    Warning - This is a known static Oakley Group2 modulus. This may makethe remote host
    more vulnerable to the Logjam attack.
```

```
Logjam attack difficulty : Hard (would require nation-state resources)
```

22964 (4) - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sendswhen it receives an HTTP request.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output 65.61.137.117 (tcp/80/www)

```
A web server is running on this port.
```

65.61.137.117 (tcp/443/www)

```
A TLSv1 server answered on this port.
```

65.61.137.117 (tcp/443/www)

```
A web server is running on this port through TLSv1.
```

65.61.137.117 (tcp/8080/www)

```
A web server is running on this port.
```

10107 (3) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solutionn/a

Risk FactorNone

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output 65.61.137.117 (tcp/80/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

65.61.137.117 (tcp/443/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

65.61.137.117 (tcp/8080/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

11219 (3) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a

firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they mightcause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk FactorNone

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output 65.61.137.117 (tcp/80/www)

```
Port 80/tcp was found to be open
```

65.61.137.117 (tcp/443/www)

```
Port 443/tcp was found to be open
```

65.61.137.117 (tcp/8080/www)

```
Port 8080/tcp was found to be open
```

24260 (3) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output 65.61.137.117 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK


Protocol version : HTTP/1.1
SSL : no

Keep-Alive : no

Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS

Headers :


  Server: Apache-Coyote/1.1

  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked

  Date: Tue, 05 Sep 2023 08:44:47 GMT

  Connection: close

Response Body :
```

```
  <link href="/style.css" rel="stylesheet" type="text/css" />

</head>

<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">

  <form id="frmSearch" method="get" action="/search.jsp">

  <table width="100%" border="0" cellpadding="0" cellspacing="0">

  <tr>

      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif"
 width=283height=80/></a></td>

  <td align="right" valign="top">

    <a   id="LoginLink"   href="/login.jsp"><font   style="font-weight:   bold;   color:
red;">Sign          In</        font></a>          |          <a          id="HyperLink3"
href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a

 id="HyperLink4"           href="/feedback.jsp">Feedback</a>           |           <label
 for="txtSearch">Search</label>

          <input type="text" name="query" id="query" accesskey="S" />

          <input type="submit" value="Go" />

  </td>
```

```
  </tr>

  <tr>

  <td                align="right"                style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img     src="/images/header_pic.jpg"     alt=""
width=354

 height=60/></td>

  </tr>

  </table>

</form>

</div>

<table cellspacing="0" width="100%">

  <tr>

    <td    width="25%"    class="bt    br    bb"><div    id="Header1"><img    id="Image1"
 src="/images/pf_lock.gif"    width=12    height=14    style="vertical-align:    bottom;"
 alt="Secure Login"/>   <a id="AccountLink"href= [...]
```

65.61.137.117 (tcp/443/www)

```
Response Code : HTTP/1.1 200 OK


Protocol version : HTTP/1.1
SSL : yes

Keep-Alive : no

Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS

Headers :


  Server: Apache-Coyote/1.1

  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked

  Date: Tue, 05 Sep 2023 08:44:52 GMT

  Connection: close

Response Body :




<!-- BEGIN HEADER -->

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

```
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>

  <td align="right" valign="top">

    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a

 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>

          <input type="text" name="query" id="query" accesskey="S" />

          <input type="submit" value="Go" />

  </td>

  </tr>

  <tr>

  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354

 height=60/></td>

  </tr>
```

65.61.137.117 (tcp/8080/www)

```
Response Code : HTTP/1.1 200 OK


Protocol version : HTTP/1.1
SSL : no

Keep-Alive : no

Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS

Headers :


  Server: Apache-Coyote/1.1

  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked

  Date: Tue, 05 Sep 2023 08:44:43 GMT

  Connection: close

Response Body :




<!-- BEGIN HEADER -->

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >

<head>

<title>Altoro Mutual</title>

  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />

  <link href="/style.css" rel="stylesheet" type="text/css" />

</head>
          </td>

          </tr>

          <tr>

          <td align="right" style="background-image:url('/images/
        gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354

         height=60/></td>

          </tr>

          </table>

        </form>

        </div>
```

39446 (3) - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also https://tomcat.apache.org/

Solutionn/a

Risk FactorNone

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

Plugin Output 65.61.137.117 (tcp/80/www)

```
URL     : http://65.61.137.117/
Version : unknown
```

65.61.137.117 (tcp/443/www)

```
URL     : https://65.61.137.117/
Version : unknown
```

65.61.137.117 (tcp/8080/www)

```
URL     : http://65.61.137.117:8080/
Version : unknown
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output 65.61.137.117 (udp/0)

```
For your information, here is the traceroute from 192.168.43.223 to 65.61.137.117 :
192.168.43.223


An error was detected along the way.

An error was detected along the way.

An error was detected along the way.


An error was detected along the way.
192.168.43.1

192.168.27.237

192.168.27.49

?
192.168.31.213

182.78.194.61

116.119.35.52

62.115.42.118

62.115.124.56

62.115.122.159

62.115.138.71
Hop Count: 22
```

10863 (1) - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

65.61.137.117 (tcp/443/www)

```
Subject Name:

Common Name: demo.testfire.net

Issuer Name:

Country: GB

State/Province: Greater Manchester
Locality: Salford

Organization: Sectigo Limited

Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 CD 6B 11 69 04 55 82 D2 7C AC 39 7B 69 DA 0C 50

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 19 00:00:00 2023 GMT

Not Valid After: Jun 14 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
            7A 03 AD 37 3B 83 42 3A 07 18 2A C9 3B 3E 09 A5 06 83 B9 40

            9A 2F CD 34 CA 3F FE 8D 47 0E 8E E3 28 17 36 34 6C 2E 38 F8

            CF 3E E1 31 01 07 55 5C 3A 43 CB 36 17 28 16 16 9C 58 12 58

            95 74 B2 59 C9 CC 16 CF E5 AF 26 74 86 1D B8 E0 3E FE C6 3C

            8F 4D 00 4A 3A 0E 4F 7F C8 0B 12 0A DC 87 8F 26 8F 6D 39 7A

            33 BB 36 59 34 95 14 EE 94 CE D9 E2 9A 95 1F 19 75 FE 68 B6
            E6 B9 10 E7 AD CD 62 8A BE C4 E8 D2 AF 62 2F C5 0D

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 C0 AD 30 34 11 F1 FA E6 17 53 0F 49 30 C1 58 E6 17 42 42

           A4 46 88 E5 10 D2 8A 32 E1 C3 54 4F 44 C7 8C F2 A5 8C 62 36
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of theoperating system.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output 65.61.137.117 (tcp/0)

```
Remote operating system : Dell EMC VMX
Microsoft Windows Embedded Standard 7
Confidence level : 59

Method : SinFP


The remote host is running one of these operating systems :
Dell EMC VMX
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output 65.61.137.117 (tcp/0)

```
Information about this scan :


Nessus version : 10.6.0
Nessus build : 20103

Plugin feed version : 202309050602
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
```

```
Scan name : testfire

Scan policy used : Advanced Scan
Scanner IP : 192.168.43.223

Port scanner(s) : nessus_syn_scanner
Port range : default

Ping RTT : 374.165 ms

Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1

Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no

Patch management checks : None

Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled

Web application tests : disabled
Max hosts : 5

Max checks : 5
Recv timeout : 5
Backports : None
```

21643 (1) - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

65.61.137.117 (tcp/443/www)

```
  Here is the list of SSL ciphers supported by the remote server :Each group is reported per SSL Version.

  SSL Version : TLSv12
    High Strength Ciphers (>= 112-bit key)


      Name                          Code             KEX           Aut      Encryption             MAC
----------------------------------------------       ------------------h    ------------------      ------
      DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
   SHA256
      DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
   SHA384
ECDHE-RSA-AES128-SHA256             0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
   SHA256
ECDHE-RSA-AES256-SHA384             0xC0, 0x30       ECDH          RSA      AES-GCM(256)
   SHA384
      DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
   SHA1
      DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
   SHA1
      ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
   SHA1

      ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
   SHA1
      DHE-RSA-AES128-SHA256SHA256   0x00, 0x67       DH DH ECDHECDHRSA   RSAAES-CBC(128)AES-CBC(256)AES-
      DHE-RSA-AES256-SHA256SHA256
      ECDHE-RSA-AES128-SHA256SHA256 0x00, 0x6B                     RSARSA   CBC(128)AES-CBC(256)
      ECDHE-RSA-AES256-SHA384SHA384
                                    0xC0, 0x27

                                    0xC0, 0x28



  SSL Version : TLSv11
    High Strength Ciphers (>= 112-bit key)

      Name                          Code             KE            Auth     Encryption             MA
----------------------------        ----------       X---          ------------------------------   C---
      DHE-RSA-AES128-SHASHA1        0x00, 0x33       DH            RSA      AES-CBC(128)
      DHE-RSA-AES256-SHA
                                    0x00, 0x39       DH            RSA [...]
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is thatthe uptime of the remote host can sometimes be computed.

See Also http://www.ietf.org/rfc/rfc1323.txt

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output 65.61.137.117 (tcp/0)

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/ https://nvd.nist.gov/products/cpe

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2010/04/21, Modified: 2023/07/27

Plugin Output 65.61.137.117 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE matched on the remote system :

  cpe:/a:apache:tomcat -> Apache Software Foundation Tomcat
```

46180 (1) - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessushas generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk FactorNone

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output 65.61.137.117 (tcp/0)

```
The following hostnames point to the remote host :

  - demo.testfire.net
  - altoromutual.com
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: aprinter, router, general-purpose computer, etc).

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output 65.61.137.117 (tcp/0)

```
Remote device type : embedded
Confidence level : 59
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encryptingcommunications.

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

65.61.137.117 (tcp/443/www)

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. Thesecipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key iscompromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

65.61.137.117 (tcp/443/www)

```
  Here is the list of SSL PFS ciphers supported by the remote server :High Strength Ciphers (>= 112-bit

    key)

      Name                                Code              KEX           Aut      Encryption              MAC
                                                                          h
-------------------------------------------------------------------------------------------------------------
      DHE-RSA-AES128-SHA256               0x00, 0x9E        DH            RSA      AES-GCM(128)
   SHA256
      DHE-RSA-AES256-SHA384               0x00, 0x9F        DH            RSA      AES-GCM(256)
   SHA384
ECDHE-RSA-AES128-SHA256                   0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
   SHA256
ECDHE-RSA-AES256-SHA384                   0xC0, 0x30        ECDH          RSA      AES-GCM(256)
   SHA384
      DHE-RSA-AES128-SHA                  0x00, 0x33        DH            RSA      AES-CBC(128)
   SHA1
```

```
      DHE-RSA-AES256-SHA                  0x00, 0x39        DH       RSA           AES-CBC(256)
   SHA1
      ECDHE-RSA-AES128-SHA                0xC0, 0x13        ECDH     RSA           AES-CBC(128)
   SHA1
      ECDHE-RSA-AES256-SHA                0xC0, 0x14        ECDH     RSA           AES-CBC(256)
   SHA1
      DHE-RSA-AES128-SHA256               0x00, 0x67        DH       RSA           AES-CBC(128)
   SHA256
      DHE-RSA-AES256-SHA256               0x00, 0x6B        DH       RSA           AES-CBC(256)
   SHA256
ECDHE-RSA-AES128-SHA256                   0xC0, 0x27        ECDH     RSA           AES-CBC(128)
   SHA256
ECDHE-RSA-AES256-SHA384                   0xC0, 0x28        ECDH     RSA           AES-CBC(256)
   SHA384

  The fields above are :

    {Tenable ciphername}
    {Cipher ID code} Kex={key exchange} Auth={authentication}
    Encrypt={symmetric encryption method}MAC={message authentication code}
    {export flag}
```

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blockswith subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. Thesecipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leakinformation if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a https://www.openssl.org/~bodo/tls-cbc.txt

Solutionn/a

Risk FactorNone

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

65.61.137.117 (tcp/443/www)

```
Here is the list of SSL CBC ciphers supported by the remote server :High Strength Ciphers (>= 112-bit
  key)

   Name                          Code              KEX           Aut      Encryption              MAC
                                                                 h
-------------------------------  ----------        ----------    ---      ------------------------  -----
   DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
```

```
   DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
                                 0xC0, 0x27        ECDH          RSA      AES-CBC(128)
   ECDHE-RSA-AES128-SHA256
SHA256                           0xC0, 0x28        ECDH          RSA      AES-CBC(256)
   ECDHE-RSA-AES256-SHA384

The fields above are :


  {Tenable ciphername}

  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

84502 (1) - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk FactorNone

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

65.61.137.117 (tcp/443/www)

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

94761 (1) - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk FactorNone

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

65.61.137.117 (tcp/443/www)

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services

|-Issuer
 Services             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate

|-Signature Algorithm : SHA-1 With RSA Encryption
```

95631 (1) - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78 https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk FactorNone

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12
Plugin Output

65.61.137.117 (tcp/443/www)

```
The following known CA certificates were part of the certificate chain sent by the remote
host, but contain hashes that are consideredto be weak.


Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 CertificateServices

Signature Algorithm : SHA-1 With RSA EncryptionValid From: Jan 01 00:00:00 2004 GMT

Valid To            : Dec 31 23:59:59 2028 GMT

Raw PEM certificate :

-----BEGIN CERTIFICATE-----

MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciB
NYW5jaGVzdGVyMRAwDgYDVQQHDA

+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3
M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnM
lhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5k
BjHYpy

+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74
Klf9AwpLQwDgYDVR0PAQH/ BAQDAgEGMA8GA1UdEwEB/

wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVT
ZXJ2aWNlcy5jcmwwNqA0oDKGMGh

+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r

+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1O
UIJqsil2D4kF501KKaU73yqWjgo

+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==

-----END CERTIFICATE-----
```

121010 (1) - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk FactorNone

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

65.61.137.117 (tcp/443/www)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 (1) - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also https://tools.ietf.org/html/rfc5246

SolutionN/A

Risk FactorNone

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

65.61.137.117 (tcp/443/www)

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

156899 (1) - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended toonly enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure andcompatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk FactorNone

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

65.61.137.117 (tcp/443/www)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


           Name                                Code              KEX            Auth     Encryption              MAC
         ----------------------------------------------------   ----------------------  ------------------------  ----
           DHE-RSA-AES128-SHA                  0x00, 0x33        DH             RSA      AES-CBC(128)
         SHA1
           DHE-RSA-AES256-SHA                  0x00, 0x39        DH             RSA      AES-CBC(256)
         SHA1
           ECDHE-RSA-AES128-SHA                0xC0, 0x13        ECDH           RSA      AES-CBC(128)
         SHA1
           ECDHE-RSA-AES256-SHA                0xC0, 0x14        ECDH           RSA      AES-CBC(256)
         SHA1
           DHE-RSA-AES128-SHA256               0x00, 0x67        DH             RSA      AES-CBC(128)
         SHA256
           DHE-RSA-AES256-SHA256               0x00, 0x6B        DH             RSA      AES-CBC(256)
         SHA256
         ECDHE-RSA-AES128-SHA256               0xC0, 0x27        ECDH           RSA      AES-CBC(128)
         SHA256
         ECDHE-RSA-AES256-SHA384               0xC0, 0x28        ECDH           RSA      AES-CBC(256)
         SHA384

The fields above are :


  {Tenable ciphername}

  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

SOC/SIEM and its Application

SOC: A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.

An SOC also selects, operates, and maintains the organization's cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.

SOC Cycle: The SOC cycle is a continuous process that involves monitoring and analyzing security events, investigating potential threats, and responding to incidents. This cycle is a key component of a proactive security strategy, which enables organizations to adapt and improve their defenses based on evolving threats and the lessons learned from previous incidents.

SIEM: SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases.

SIEM has matured to become more than the log management tools that preceded it. Today, SIEM offers advanced user and entity behavior analytics (UEBA) thanks to the power of AI and machine learning. It is a highly efficient data orchestration system for managing ever-evolving threats as well as regulatory compliance and reporting.

SIEM Cycle: The SIEM cycle typically starts with data collection, followed by log normalization, correlation, threat detection, incident response, and reporting. It continually refines and updates its threat detection models based on the new information received.

MISP: A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks but also threat intelligence such as threat actor information, financial fraud information and many more.

MISP - Open Source Threat Intelligence and Sharing Platform allows organizations to share information such as threat intelligence, indicators, threat actor information or any kind of threat which can structured in MISP. MISP users benefit from the collaborative knowledge about existing malware or threats. The aim of this trusted platform is to help improving the counter-measures used against targeted attacks and set-up preventive actions and detection.

College Network Information: The college network has a gateway at end point then divide into two parts one for academic blocks and other for hostels. The college has two network connectivity in gateway primary-BSNL and secondary -JIO. The hostel has Sophos firewall and academic block has Fortigard firewall. From the firewall ,network is further divided into different building .When a device connected to internet it allocate an ip for 6 hours but internet speed is not provide it will provided when credential is entered. The whole network is under surveillance and in continuous monitoring .SOC , SIEM and IDS are properly implemented to collect log and to analyse data and post-exploit data collection, foot printing. Honeypot is also implemented to improve network security and network is properly maintained for better level of security.

Deployment of SOC in College: ELK (Elasticsearch, Logstash, Kibana) is a powerful combination of tools, often used together for log management, data visualization, and analysis. ELK can be used as a foundation for building a SIEM-like solution, as it provides capabilities for log collection, normalization, storage, and visualization. It can ingest vast amounts of data, process and analyse logs, and create visual representations. Logstash can be connected to firewall to send data to Elasticsearch to analyse to enhance level of searching then can be send to Kibana dashboard. The dashboard provide Data visualization, dashboard creation, customization, search query capabilities, integration, and sharing, security and access control.

Threat Intelligence: It is evidence-based information about cyber attacks that cyber security experts organize and analyze. This information may include:

- Mechanisms of an attack
- How to identify that an attack is happening

- Ways different types of attacks might affect the business
- Action-oriented advice about how to defend against attacks

Many forms of cyber attacks are common today, including zero-day exploits, malware, phishing, man-in-the-middle attacks, and denial of service attacks. Different ways of attacking computer systems and networks constantly evolve as cybercriminals find new vulnerabilities to exploit. Cyber Threat Intelligence (CTI) helps organizations stay informed about new threats so that they can protect themselves. Cyber security experts organize, analyse, and refine the information they gather about attacks to learn from and use it to protect businesses better.

Threat intelligence (or security intelligence) also helps stop or mitigate an attack that is in progress. The more an IT team understands about an attack, the better they will be able to make an informed decision about how to combat it.

Incident Response : Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

The SANS Institute provides six steps for effective incident response:

- **Preparation** : Preparation helps organizations determine how well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools, and training.
- **Identification**: Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages.
- **Containment**: The main purpose of containment is to contain the damage and prevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimize damage).

- **Eradication** - Eradication is the phase of effective incident response that entails removing the threat and restoring affected systems to their previous state, ideally while minimizing data loss.
- **Recovery** - Testing, monitoring, and validating systems while putting them back into production in order to verify that they are not re-infected or compromised are the main tasks associated with this step of incident response.
- **Lessons Learned** - Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed during the incident, plus complete documentation to provide information for future incidents.

IBM Qradar

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors. IBM QRadar then performs real-time analysis of the log data and network flows to identify malicious activity so it can be stopped quickly, preventing or minimizing damage to the organization.

The IBM QRadar SIEM can be deployed as a hardware, software or virtual appliance-based product. The product architecture includes event processors for collecting, storing and analysing event data and event collectors for capturing and forwarding data. The SIEM product also includes flow processors to collect Layer 4 network flows, QFlow processors for performing deep packet inspection of Layer 7 application traffic, and centralized consoles for Security Operations Center (SOC) analysts to utilize when managing the SIEM. Flow processors offer similar capabilities to event processors, but are for network flows, and consoles are for people to utilize when using or managing the SIEM.

IBM QRadar can collect log events and network flow data from cloud-based applications, and it can be deployed as a SaaS offering on the IBM cloud where deployment and maintenance is outsourced.

Additional security capabilities

An IBM QRadar SIEM can have a license extension purchased that enables use of IBM Security X-Force Threat Intelligence, which identifies IP addresses and URLs that are associated with malicious activity. For each identified IP address or URL, the threat intelligence feed includes a threat score and category, which can help an organization better analyse and prioritize threats.

Reporting capabilities

IBM QRadar provides support for several major compliance reporting requirements initiatives such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA), North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC), Sarbanes–Oxley (SOX) and more.

Conclusion

- **Web application testing:** Web application testing is like checking a website or online tool to make sure it works properly, is safe from hackers, and runs fast. Testers look at how it looks and works on different devices and browsers. They also try to find and fix any security issues that could be a problem. This testing helps make sure that websites and online tools are reliable, safe, and work well for people who use them. From our practice websites we chose a website that has multiple vulnerabilites and used to figured out the vulnerabilities using appropriate tools. It can be concurred from our report that the main website we chose has less vulnerabilities than the practice website which signifies that the security is more prominent on the website and is more secure and safe to hacker attacks.
- **Nessus Report :** A Nessus report is a comprehensive document generated by the Nessus vulnerability scanning tool, offering insights into the security posture of a computer system or network. This report identifies vulnerabilities, misconfigurations, and potential security risks within the scanned infrastructure. It categorizes findings by severity, providing detailed information on each issue, its potential impact, and suggested remediation steps. Nessus reports aid cybersecurity professionals in prioritizing and addressing vulnerabilities, enhancing system security. From the report we can incur that by knowing which vulnerabilities affect hosts on the network, security teams can coordinate their mitigation efforts more effectively. This report provides extensive data about vulnerabilities detected on the network. Charts illustrate the ratio of vulnerability severities and list the most vulnerable hosts by vulnerability score. Detailed information about every vulnerability detected on that host is listed, including plugin ID, plugin name, plugin family, severity, protocol, port, exploitability, host CPE, plugin text, first discovered, and last seen times. We can use this extensive data in order to identify vulnerabilities in their network and tailor their mitigation efforts accordingly

- **SOC / SEIM / Qradar Dashboard :** A Security Operations Center (SOC) is a place where experts monitor and respond to security threats. A Security Information and Event Management (SIEM) system, like IBM's QRadar, helps the SOC by collecting and analyzing data from various sources, identifying potential security issues. The QRadar Dashboard is a user-friendly display of this information, showing key insights and alerts in one place. It helps security teams quickly spot and address potential threats, making it easier to protect computer systems and networks from cyberattacks. In simpler terms, it's like a control center that uses QRadar to keep an eye on and manage security issues. These tools proved real helpful for helping us find the various vulnerabilities from different websites and from industrial point of view we can understand how it helps professionals spot security threats by enhancing threat detection, incident response, alert management, compliance, and overall security posture. It provides valuable insights and tools to defend against evolving cyber threats efficiently.

Future Scope

- **Web Application Testing:** The future scope of web application testing is expected to continue evolving and expanding as technology and software development practices advance. Automation of testing processes will continue to be a significant trend. Test automation frameworks, tools, and techniques will become more sophisticated, allowing testers to run tests more efficiently and frequently. This includes both functional and non-functional testing like performance, security, and usability testing.

  With the adoption of DevOps practices, testing is shifting left in the software development lifecycle. Testing is no longer a separate phase but is integrated from the beginning, with a focus on collaboration, automation, and quality assurance throughout the development process. As web applications become more complex, ensuring they can handle high loads and provide optimal performance is crucial. Performance testing tools and methodologies will continue to be in demand.

- **Testing Process**: The future scope of testing processes in cybersecurity, often referred to as cybersecurity testing or ethical hacking, is likely to grow in significance as cyber threats continue to evolve. The need for robust security measures and testing methodologies will be crucial to protect organizations and individuals from cyberattacks. Red teaming and penetration testing will remain vital for identifying vulnerabilities in systems, networks, and applications. These activities involve simulating cyberattacks to uncover weaknesses and improve defenses. As organizations become more security-conscious, the demand for skilled penetration testers and ethical hackers will rise.

- **SOC/SIEM**: The future scope of Security Operations Center (SOC) and Security Information and Event Management (SIEM) systems is expected to expand and evolve as the cybersecurity landscape becomes more complex and challenging. These technologies play a crucial role in monitoring, detecting, and responding to security incidents. The demand for more advanced threat detection capabilities will increase. SIEM systems will integrate machine learning and artificial intelligence to enhance their ability to identify complex and previously unseen threats.

  Behavioral analytics will become a significant part of SIEM systems. They will focus on user and entity behavior analytics (UEBA), which can help in identifying insider threats and unusual behavior patterns. SOC and SIEM solutions will increasingly incorporate automation and orchestration capabilities to streamline incident response. This will help SOC teams to respond more quickly and effectively to security events.

Topic Explored

- **OWASP Top Ten**: Explored the OWASP Top Ten, a comprehensive list of the most critical web application security risks. Investigated how these vulnerabilities, including injections, broken authentication, XSS, and others, could impact web applications and potential mitigation strategies.
- **ELK (Elasticsearch, Logstash, Kibana)**: Explored the ELK stack, a powerful data analytics tool used for log management, data analysis, and visualization. Investigated its functionalities in collecting, normalizing, and visualizing log data to identify potential security issues within web applications**.**
- **Vulnerable Websites**: Explored various vulnerable websites or simulated environments to understand common security flaws. Conducted analyses on these platforms to identify vulnerabilities, such as SQL injection, XSS, and misconfigurations, to comprehend their impact and potential exploitation.
- **Session Management**: Explored the security aspects related to session management within web applications. Investigated techniques to prevent session fixation, ensure proper session timeout, and protect against session hijacking to maintain the confidentiality and integrity of user sessions.
- **Pentesting (Penetration Testing)**: Explored the methodology and execution of penetration testing. Investigated the application of ethical hacking techniques to identify vulnerabilities within web applications and performed targeted simulated attacks to validate the effectiveness of security controls.
- **CIA (Confidentiality, Integrity, Availability)**: Explored the CIA triad's significance in the context of cyber security. Investigated the importance of maintaining the confidentiality, integrity, and availability of data within web applications and the impact of vulnerabilities on these critical security principles.

Tools Explored

- **Tenable Nesssus**: Nessus by Tenable is a widely-used vulnerability scanner that identifies vulnerabilities, misconfigurations, and potential threats across networks, systems, and applications. It performs comprehensive scans, offering detailed reports and prioritizing remediation efforts.
- **IBM Qradar**: QRadar is an advanced security information and event management (SIEM) solution. It collects and analyses log and event data from various sources to detect anomalies, threats, and potential security breaches. It offers real-time visibility and aids in incident response.
- **Kali Linux**: Kali Linux is a powerful, open-source penetration testing platform used by cyber security professionals. It comes pre-installed with numerous tools for security testing, forensics, and ethical hacking, making it a go-to choice for vulnerability assessments.
- **Burp Suite**: Burp Suite is an integrated platform for security testing of web applications. It helps identify security flaws such as Cross-Site Scripting (XSS), SQL injection, and more. Its features include a web vulnerability scanner, proxy, and various tools for manual testing.
- **Nslookup**: Nslookup is a command-line tool used to query DNS (Domain Name System) to obtain information about domain names, IP addresses, and mail exchanges. It helps in the reconnaissance phase by providing DNS-related information during security assessments.
- **NMap**: NMap is a versatile network scanning tool used to discover hosts and services on a network. It performs various types of scans (e.g., port scanning, OS detection) and provides detailed information about network hosts, aiding in vulnerability discovery.
- **Metasploit framework**: Metasploit is a penetration testing and exploit development tool. It assists in identifying and exploiting vulnerabilities to test systems' security. The framework includes a database of known vulnerabilities and exploits, making it a valuable tool for security assessments.

----------XXXXX----------