Vulnerability Assessment Report

ACME - WebApp - VA-2011021543

Filename: SAMPLE-Report-VA_ACME_WebApp_VA-2011021543
Report Date: **Wed, 17-Feb-21** Organization: **ACME**
Report Status: **Draft** **Review** **Approved** Template: **204**
Classification: **Restricted** Link: Contents

Assessor Information

	Neumetric Computations Private Limited
	Neumetric
	www.neumetric.com
	infosec@neumetric.com

Assessee Information

	ACME Inc
	ACME
	Web Application
	WebApp
	NA
	NA
	NA

Report Information

	VA-2011021543
	Report-VA_ACME_WebApp_VA-2011021543
	Wed, 17-Feb-21
	Fri, 12-Jan-21 13:15
	Prakash V
	prakash.v@neumetric.com

Filename: SAMPLE-Report-VA_ACME_WebApp_VA-2011021543
Report Date: **Wed, 17-Feb-21** Organization: **ACME**
Report Status: **Draft** **Review** **Approved** Template: **204**
Classification: **Restricted** Link: Contents

Findings Stats

V0_Critical	
V1_High	
V2_Medium	
V3_Low	
VX_Info	

* See Appendix for explanation of Severity Rating System [Appendix]

Findings Summary

V001	V2_Medium	Error Message	HTTP 500 Error Message	4
V002	V0_Critical	Broken Authentication and Session Management	Clear-text Password returned in Login Response	5

Caution! Neumetric's Technical Security service follows internally defined procedure & guidelines which are based on standards & frameworks within the information security industry such as OWASP, NIST_SP_800-53, CWE, PCI_DSS & CIS that are well-defined, adequately vetted & undergo continuous improvement. Precautions are taken in the execution of the vulnerability assessment activity & preparation of this Report in accordance with these methodologies. Nevertheless, Neumetric and the Author request the User of this Report to permit some leniency for oversight errors & omissions. This Report assures the security of the tested Application as on the date of testing & is limited to the scope mentioned in suitable locations within this Report. Neumetric assures to promptly evaluate & correct any errors or omissions in this Report.

Detailed Technical Finding, Reproduction & Recommendation

Vulnerability ID: V001

Vulnerability Category: Broken Authentication and Session Management
Vulnerability Name: SQL Injection
CWE ID https://cwe.mitre.org/data/definitions/1027.html
CVSS Score **5.0**

Threat:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a

downgrade. This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

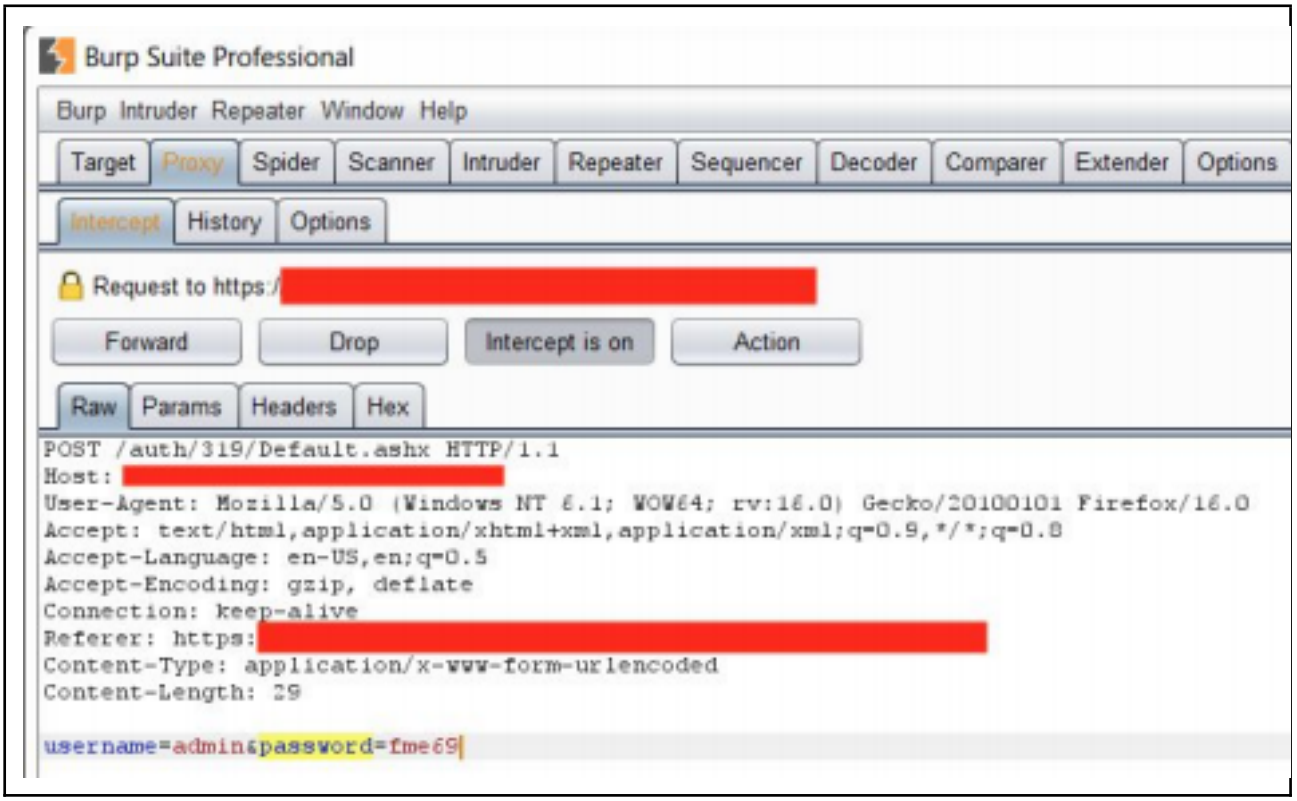
Impact:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

Reproduction:

1. Open Login page.
2. Add POST parameters.
3. Provide Username & Password.
4. Add an extra request parameter for Username.



Resolution:

1. Implement Password Policy to ensure that Admin password has a minimum length of 8 characters which includes special characters & numbers.
2. Conduct input validation for login form on Client-side.
3. Conduct input validation for login form on Server-side.
4. Reject invalid login input with a generic message.

Vulnerability ID: V002

Vulnerability Category: Broken Authentication and Session Management
Vulnerability Name: SQL Injection
CWE ID https://cwe.mitre.org/data/definitions/1027.html
CVSS Score **5.0**

Threat:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a

downgrade. This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

Impact:

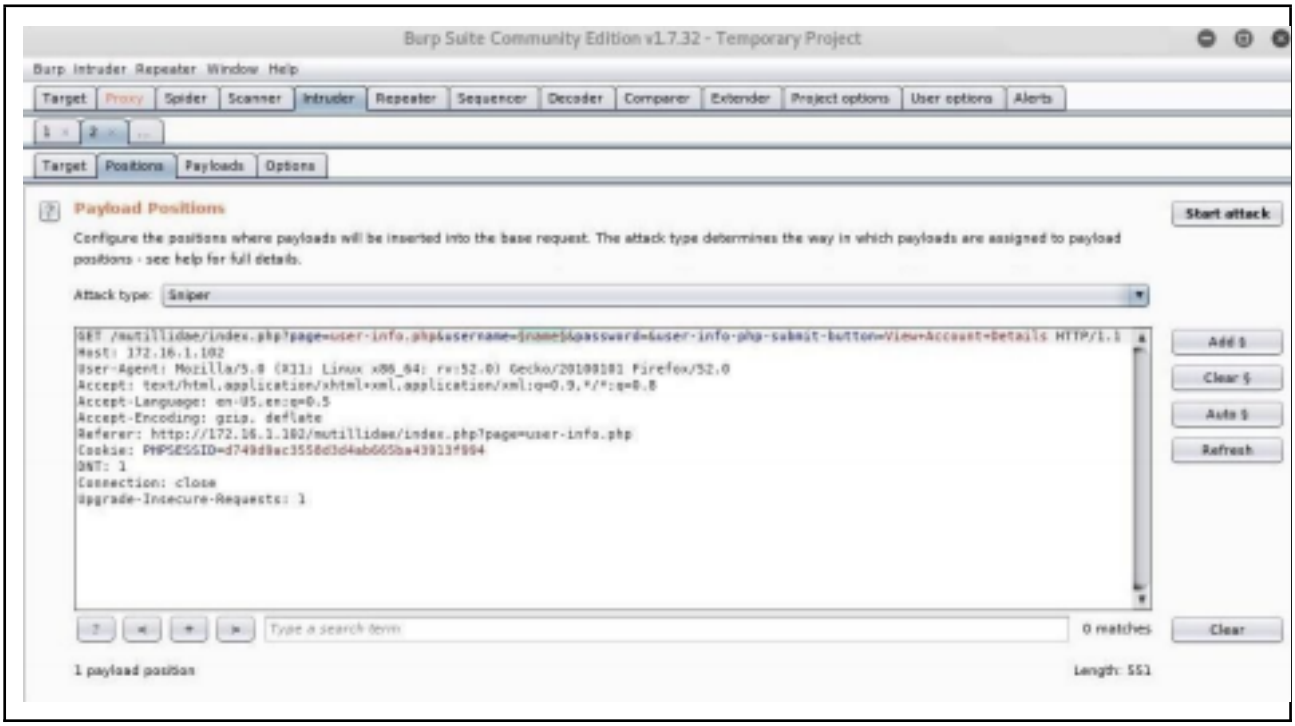
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

Reproduction:

1. Connect to login API.
2. Add POST parameters.
3. Provide Username & Password.
4. Add an extra request parameter for Username.

Filename: SAMPLE-Report-VA_ACME_WebApp_VA-2011021543
Report Date: **Wed, 17-Feb-21** Organization: **ACME**
Report Status: **Draft** **Review** **Approved** Template: **204**
Classification: **Restricted** Link: Contents



Resolution:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

Appendix

Web App Scan Checklist

1	Broken Authentication and Session Management	Cookie attribute not set to HTTPOnly
2	Broken Authentication and Session Management	Session non-expiry on Browser close
3	Broken Authentication and Session Management	Session token passed in other areas apart from Cookie
4	Broken Authentication and Session Management	Hijack of User Session through Session Fixation
5	Broken Authentication and Session Management	Application uses Basic or NTLM Authentication
6	Broken Authentication and Session Management	SQL Injection
7	Broken Authentication and Session Management	Command Injection
8	Broken Authentication and Session Management	CRLF Injection
9	Broken Authentication and Session Management	HTML Injection
10	Broken Authentication and Session Management	Iframe Injection
11	Broken Authentication and Session Management	XML Injection
12	Business Logic Flaw	Privilege escalation through Parameter Manipulation
13	Business Logic Flaw	Sensitive actions on behalf of another User
14	Business Logic Flaw	Parameter manipulation by exceeding Transaction Limits
15	Business Logic Flaw	Test for limits on the Functions usage
16	Business Logic Flaw	Authentication or Authorization Bypass through Session Puzzling
17	Error Message	HTTP 403 Error Message
18	Error Message	HTTP 500 Error Message
19	Insecure Direct Object Reference	Directory Listing enabled on Server
20	Insecure Direct Object Reference	Directory Traversal Attack
21	Insecure Direct Object Reference	HTTP Parameter Pollution
22	Insecure Direct Object Reference	Internal Page accessibility without Authentication

Caution! Neumetric's Technical Security service follows internally defined procedure & guidelines which are based on standards & frameworks within the information security industry such as OWASP, NIST SP 800-53, CWE, PCI DSS & CIS that are well-defined, adequately vetted & undergo continuous improvement. Precautions are taken in the execution of the vulnerability assessment activity & preparation of this Report in accordance with these methodologies. Nevertheless, Neumetric and the Author request the User of this Report to permit some leniency for oversight errors & omissions. This Report assures the security of the tested Application as on the date of testing & is limited to the scope mentioned in suitable locations within this Report. Neumetric assures to promptly evaluate & correct any errors or omissions in this Report.

23	Insecure Direct Object Reference	Missing URL or parameter referenced in robots.txt file causing exposure
24	Insecure Direct Object Reference	Improper implementation of Access Control
25	Insecure Direct Object Reference	Application allows simultaneous login using a Single User ID
26	Insecure Direct Object Reference	Application displays Runtime Error Message
27	Insecure Direct Object Reference	Application does not have Logout functionality
29	Insecure Direct Object Reference	Dangerous HTTP Method enabled on Server
34	Insecure Direct Object Reference	Local or Remote File Inclusion
35	Insecure Direct Object Reference	Critical information in URL
36	Insecure Direct Object Reference	Private IP Address disclosure
37	Insecure Direct Object Reference	Sensitive data accessible in Cache
38	Insecure Direct Object Reference	Sensitive data stored in Persistent Cookie on the User's local storage
39	Insecure Direct Object Reference	Sensitive information revealed in HTTP Response

40	Insecure Direct Object Reference	Credentials are transmitted to Server in Plain-text
41	Insecure Direct Object Reference	Sensitive data is transmitted to Server in Plain-text
42	Insecure Direct Object Reference	Clear-text Password returned in Login Response
43	Insecure Direct Object Reference	Original Password sent over SMS or Email in Forgot Password feature
44	Insecure Direct Object Reference	Password Reset link Token true randomization check
45	Cross-Site Scripting [XSS]	Cross-frame Scripting test
46	Cross-Site Scripting [XSS]	Cross Site Scripting test
47	Cross-Site Request Forgery [CSRF]	Cross-Site Request Forgery test
49	Change Password Functionality	Old Password not validated during 'Change Password' process
50	Weak Password Policy	Weak system-generated Password as initial Password for a new User
51	Weak Password Policy	Weak Password Policy
52	Weak Password Policy	Identical Login and Transaction password check
53	Weak Password Policy	Default Password assigned as initial password for a new User
54	Weak Password Policy	Password is not case-sensitive
55	Weak Password Policy	Auto-complete enabled for Sensitive Field

Caution! Neumetric's Technical Security service follows internally defined procedure & guidelines which are based on standards & frameworks within the information security industry such as OWASP, NIST_SP_800-53, CWE, PCI_DSS & CIS that are well-defined, adequately vetted & undergo continuous improvement. Precautions are taken in the execution of the vulnerability assessment activity & preparation of this Report in accordance with these methodologies. Nevertheless, Neumetric and the Author request the User of this Report to permit some leniency for oversight errors & omissions. This Report assures the security of the tested Application as on the date of testing & is limited to the scope mentioned in suitable locations within this Report. Neumetric assures to promptly evaluate & correct any errors or omissions in this Report.

56	Weak Password Policy	CAPTCHA is not implemented for Public Form
57	Weak Password Policy	Insecure Administrator login name
58	Remember Me Feature	Vulnerability related to "Remember Password" feature
59	Weak Cross Domain Policy	"Allow-Access-From Domain" in cross-domain.xml Policy file set to "*" or unauthorized domain
60	Weak Cross Domain Policy	"Origin" header in Client request validated at the Server
61	Weak Cross Domain Policy	"Access-Control-Allow-Origin" Header in Server response is set securely
62	Weak Cross Domain Policy	Cross-origin Resource Sharing (CORS)

Severity Rating System

V0_Critical	Extensive, serious, widespread risk to Application, Network, IT & Systems. Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.	**Urgency**: Immediate response is necessary. **Recommendation**: Remediate within 15 days.
V1_High	Heavy, significant, broad risk to Application, Network, IT & Systems. Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.	**Urgency**: Quick response is warranted. **Recommendation**: Remediate within 30 days.
V2_Medium	Medium, notable, ample risk to Application, Network, IT & Systems. Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.	**Recommendation**: Remediate within 60 days.

V3_Low	Minor, noticeable, trivial risk to Application, Network, IT & Systems. Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.	**Recommendation**: Remediate within 90 days.
VX_Info	Very low risk to Application, Network, IT & Systems. Intruders can collect information about the host (open ports, services) and may be able to use this information to find other vulnerabilities.	Remediating these vulnerabilities are part of good practices for improving security posture.

Tools Used

Qualys Express	VPC Scanning	Commercial	Web proxy and scanning tool used to intercept and analyze HTTPS-based communication.
Burp Suite Professional Edition	Web App & Mobile App	Commercial	Burp or Burp Suite is a graphical tool for testing Web Application Security. The tool is written in Java and developed by PortSwigger Web Security.
NMAP	Network Scanning	Open-source	Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Filename: SAMPLE-Report-VA_ACME_WebApp_VA-2011021543
Report Date: **Wed, 17-Feb-21** Organization: **ACME**
Report Status: **Draft** **Review** **Approved** Template: **204**
Classification: **Restricted** Link: Contents

Preliminary Information

1	Assessment Methodology	Black Box / Gray Box / White Box [see Definition for details of each term]	Gray Box
2	Assessment Depth	Invasive / Non-invasive [see Definition for details of each term]	
3	Assessment Capability	Active / Passive [see Definition for details of each term]	Passive. Scanning methodology will not resolve or fix the discovered vulnerabilities. These will need to be remediated as a separate activity.
4	Scanning Environment	UAT / QAT / Test / Staging / Production **Recommended** First Scan should **NOT** be conducted in Production environment. Rescan may be conducted in Production environment (restricted in scope to findings in First Scan). Written commitment is a must that the Staging & Production environment are mirrors of each other. **Example:** Production: prod.webapp.com Staging: staging.webapp.com - Must be a mirror of prod.webapp.com First Scan - x days - Staging - 5 days (with Report) - 10 vulnerabilities Remediation - y days - Done by internal Tech Team on Staging & then on Prod. Rescan - z days - Production - 2 days (with Report) - Scope is limited to the vulnerabilities found in First Scan.	
5	Web App	Number of Web Applications	
6	Web App	URL for Scanning Environment	
7	Web App	URL for Production Environment	
8	Web App	Protocol (http/https)	

9	Application Access (Web)	Web App is accessible from Internet or Intranet?	
10	1Application Access (Web)	If Web App is accessible only within Intranet, then will VPN access be provided?	
11		11 Web App - Web Services Number of Web Services (if applicable)	
12	Web App - Web Services (add multiple rows for each Web Services)	Type (REST/SOAP) & additional information listed below. REST: URL, Request Type (POST/GET/...), Request Body (if applicable) SOAP: URL, WSDL file, XML file	
13	Web App	Control Panel Admin credential for Control Panel.	username & password

14	Web App - Customer Web App	Admin credential for Customer Web App.	username & password
15	Web App - Privileges	User Access Privileges defined in the Web App	Control Panel: Customer Web App: Example: Administrator, User, Employee, Student, Controller, Operator, ...
16	Web App - MFA	Is Multi Factor Authentication enabled in Web App? If yes, then provide details.	Example: Email OTP, Mobile OTP, Authenticator, ...
17	Android App - Access	Android App APK file will be provided? (Yes / No / NA)	
18	Android App - Access	Playstore Account to be added to Beta version of Android App.	gaurav.bahl@neumetric.com
19	Android App - Access	Android App least compatible version.	Example: Android 6.0-6.0.1, Marshmallow Android 7.0-7.1.2, Nougat Android 8.0-8.1, Oreo Android 9.0, Pie Android 10, Q

Definition

Black Box	Black Box refers to a method where we will have no knowledge of the system. The goal of this type of scanning & testing is to simulate an external hacking or cyber warfare attack.
Gray Box	Gray Box Tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used. Gray Box Tester requires both high-level and detailed documents describing the Application, which they collect in order to define test cases.
White Box	White Box is a method of testing the application at the level of the Source Code. The test cases are derived through the use of the design techniques such as Control Flow testing, Data Flow testing, Branch Testing, Path testing, Statement Coverage and Decision Coverage as well as modified Condition/Decision Coverage. The whole point of White Box testing is the ability to know which line of the code is being executed and being able to identify what the correct output should be.
Invasive Scan	An invasive scanning technique attempts to inject malicious elements as payload or as separately active subsystems to enable discovery of vulnerability that a non-invasive method is unlikely to discover. Black Box testing always involves invasive techniques. Sometimes Gray Box testing will employ such a method. White Box testing usually does not require an invasive technique to be employed.
Active System	An Active vulnerability scanning method also identifies & deploys the remediation for a discovered vulnerability. This system is usually online in realtime.
Passive System	A Passive vulnerability scanning method identifies, but does not deploy the remediation for a discovered vulnerability. All discovered vulnerabilities need to be remediated as a separate activity later on. A Rescan is necessary to ensure that the vulnerability has been reliably fixed. This system is usually not online & is unlikely to work in real time. Typically, one-time activities such as a Manual or Automatic VA active is passive in nature.

- End of Report -