



THE ULTIMATE APPSEC CHALLENGE

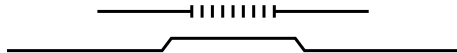


 Probely

E A S Y



**WHAT POSITION IS INJECTION ON
OWASP TOP 10 2021?**



E A S Y

ANSWER: 3RD

INJECTION VULNERABILITIES HAVE
BEEN IN THE OWASP TOP 10 SINCE
ITS CREATION.

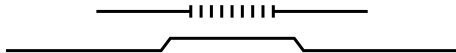


WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



**WHAT DOES OWASP
STAND FOR?**



E A S Y

OPEN WORLDWIDE APPLICATION SECURITY PROJECT

IN 2023 OWASP CHANGED ITS NAME FROM
OPEN WEB APPLICATION SECURITY
PROJECT, TO MAKE IT MORE INCLUSIVE
TO THE DIFFERENT ASPECTS OF
APPLICATION SECURITY.

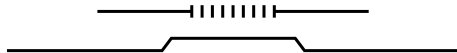


WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



**NAME A VULNERABILITY WITH A
HEART-SHAPED LOGO**



E A S Y

HEARTBLEED

HEARTBLEED IS A SERIOUS
VULNERABILITY AFFECTING THE OPENSLL
CRYPTOGRAPHIC SOFTWARE LIBRARY.

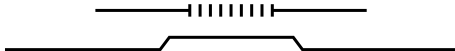


WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT WILL APPEAR ON THE PAGE?

1. `<hmtl><body>`
2. `<p>Hello <noscript>"><script>alert 'xss' </script><noscript/></p>`
3. `</body></html>`



ANSWER: HELLO

THE NOSCRIPT TAG PREVENTS THE SCRIPT
TAG FROM BEING INTERPRETED.

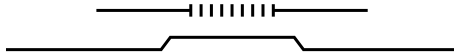


WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



XSS STANDS FOR?



E A S Y

CROSS-SITE SCRIPTING



WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



CIA STANDS FOR?



E A S Y

**CONFIDENTIALITY, INTEGRITY, AND
AVAILABILITY**



WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT IS THE NEWER NAME FOR IDOR VULNERABILITIES?

IBAS - INSECURE BYPASS OF
AUTHORIZATION SYSTEMS

OR

BOLA - BROKEN OBJECT LEVEL
AUTHORIZATION

**BOLA OR BROKEN OBJECT LEVEL
AUTHORIZATION**



WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



WHAT DOES CSRF STAND FOR?



E A S Y

CROSS-SITE REQUEST FORGERY



WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y



**IF AN UNAUTHENTICATED USER CAN
ACCESS A PRIVATE URL FROM A
PRIVILEGED USER, WHAT IS THE
ASSOCIATED OWASP TOP 10 RISK?**



E A S Y

A01 - BROKEN ACCESS CONTROL

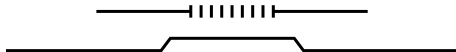


WEB APPLICATION AND API VULNERABILITY SCANNER

E A S Y

**IF YOUR APPLICATION LOGS CAN BE
TAMPERED WITH, WHICH OWASP TOP
10 RISK IS APPLICABLE?**

E A S Y



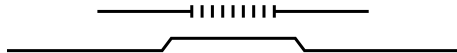
A09 - SECURITY LOGGING AND MONITORING FAILURES



WEB APPLICATION AND API VULNERABILITY SCANNER



**WHAT IS THE OTHER NAME FOR
CLICKJACKING?**



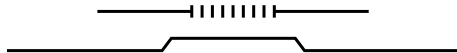
UI REDRESSING



WEB APPLICATION AND API VULNERABILITY SCANNER



**WHAT RISK IS IN THE LAST POSITION
OF THE OWASP TOP 10?**



A10 - SERVER-SIDE REQUEST FORGERY

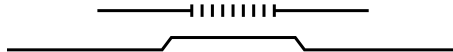


WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT IS THE VULNERABILITY?

```
1. IF (ACCESS("FILE", W_OK) != 0) {  
2.   EXIT(1);  
3. }  
4. FD = OPEN("FILE", O_WRONLY);  
   WRITE(FD, BUFFER, sizeof(BUFFER));
```



**TOCTOU, TIME-OF-CHECK TO TIME-OF-
USE, OR RACE CONDITION.**

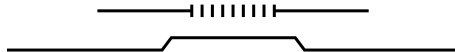


WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT IS THE VULNERABILITY?

```
IF (ACCESS("FILE", W_OK) != 0) {  
    EXIT(1);  
}  
FD = OPEN("FILE", O_WRONLY);  
WRITE(FD, BUFFER, sizeof(BUFFER));
```



**TOCTOU, TIME-OF-CHECK TO TIME-OF-
USE, OR RACE CONDITION.**



WEB APPLICATION AND API VULNERABILITY SCANNER



**YOU ARE USING WINDOWS XP. WHICH
OWASP TOP 10 RISK APPLIES HERE?**



A06 VULNERABLE AND OUTDATED COMPONENTS

WINDOWS XP SUPPORT ENDED IN 2014.



WEB APPLICATION AND API VULNERABILITY SCANNER



**YOU SEE THIS IN A BROWSER.
WHAT OWASP TOP 10 RISK
DOES IT REFER TO?**

```
EXCEPTION IN THREAD "MAIN" JAVA.LANG.NULLPOINTEREXCEPTION  
AT COM.EXAMPLE.PROJECT.CAR.GETMODEL(CAR.JAVA:18)  
AT COM.EXAMPLE.PROJECT.BUILDER.GETCARMODELS(BUILDER.JAVA:25)
```

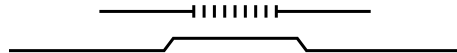
A05 - SECURITY MISCONFIGURATION



WEB APPLICATION AND API VULNERABILITY SCANNER




**IN WHICH YEAR WAS THE OWASP TOP
10 PUBLISHED FOR THE FIRST TIME?**




2 0 0 3



WEB APPLICATION AND API VULNERABILITY SCANNER



**THE USAGE OF “QUESTIONS AND
ANSWERS” IN A CREDENTIAL
RECOVERY WORKFLOW CAN BE
ASSOCIATED WITH WHICH OWASP TOP
10 RISK?**



A04 - INSECURE DESIGN

**VARIOUS INDUSTRY GUIDELINES AND
STANDARDS, SUCH AS OWASP ASVS,
OWASP TOP 10, AND NIST 800-63B
CONSIDER THIS AN INSECURE DESIGN.**



WEB APPLICATION AND API VULNERABILITY SCANNER

MEDIUM



RSA STANDS FOR?



MEDIUM

RIVEST, SHAMIR, AND ADLEMAN

**THESE ARE THE FIRST NAMES OF THE
THREE CREATORS OF THE WIDELY USED
RSA CRYPTOGRAPHIC ALGORITHM**

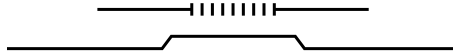


WEB APPLICATION AND API VULNERABILITY SCANNER

MEDIUM



NAME THE 3 TYPES OF XSS



MEDIUM

REFLECTED, STORED, AND DOM BASED



WEB APPLICATION AND API VULNERABILITY SCANNER



**A SOFTWARE DISTRIBUTION SYSTEM
THAT DOESN'T PROVIDE INTEGRITY
ASSURANCES IS VIOLATING WHICH
OWASP TOP 10 RISK?**



A08 - SOFTWARE AND DATA INTEGRITY FAILURES



WEB APPLICATION AND API VULNERABILITY SCANNER

MEDIUM



**A PADDING ORACLE VULNERABILITY
REFERS TO WHICH RISK OF THE OWASP
TOP 10?**



MEDIUM

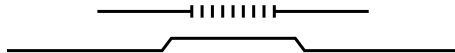
A02 - CRYPTOGRAPHIC FAILURES



WEB APPLICATION AND API VULNERABILITY SCANNER



**WHICH COOKIE ATTRIBUTE PREVENTS
CSRF?**



SAMESITE

**THIS ATTRIBUTE CAN PREVENT COOKIES
FROM BEING SENT DURING CSRF
ATTACKS.**



WEB APPLICATION AND API VULNERABILITY SCANNER

**WHAT IS THE AUTHENTICATION
ALGORITHM USED IN THE FOLLOWING
CIPHER SUITE:**

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

RSA.

**THE 1ST PART IS THE KEY EXCHANGE
ALGORITHM, 2ND, THE AUTHENTICATION,
3RD ENCRYPTION, AND 4TH IS THE MAC.**



WEB APPLICATION AND API VULNERABILITY SCANNER



SSDLC STANDS FOR?



SECURE SOFTWARE DEVELOPMENT LIFE CYCLE



WEB APPLICATION AND API VULNERABILITY SCANNER



THE HTTP 429 RESPONSE CODE MEANS?



TOO MANY REQUESTS



WEB APPLICATION AND API VULNERABILITY SCANNER



WILL THE ALERT EXECUTE?

HTTP/1.1 200 OK

DATE: THU, 06 APR 2023 21:53:38 GMT

STRICT-TRANSPORT-SECURITY: MAX-AGE=31536000; INCLUDESUBDOMAINS

VARY: ORIGIN,ACCEPT-ENCODING

CONTENT-TYPE: APPLICATION/JSON; CHARSET=UTF-8

X-CONTENT-TYPE-OPTIONS: NOSNIFF

X-FRAME-OPTIONS: DENY

X-XSS-PROTECTION: 1; MODE=BLOCK

<HTML><BODY><H1>HELLO <SCRIPT>ALERT(13)</SCRIPT></H1></BODY></HTML>

**NO, BECAUSE THE CONTENT-TYPE IS
APPLICATION/JSON, WHICH WILL NOT
BE RENDERED BY THE BROWSER.**

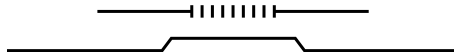


WEB APPLICATION AND API VULNERABILITY SCANNER

MEDIUM



CVSS STANDS FOR?



MEDIUM

COMMON VULNERABILITY SCORING SYSTEM

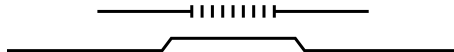


WEB APPLICATION AND API VULNERABILITY SCANNER

MEDIUM



WHAT IS THE PR IN CVSS?



MEDIUM

PRIVILEGES REQUIRED

**IT CAN HAVE THREE VALUES: NONE,
LOW OR HIGH**



WEB APPLICATION AND API VULNERABILITY SCANNER



NAME THE ATTACK

GET /?error=foobar%0d%0aSet-Cookie:+sessionid=abcdef
host: example.com

HTTP/1.1 301 Moved Permanently
Location: /index?error=foobar
Set-Cookie: sessionid=abcdef



HTTP RESPONSE SPLITTING

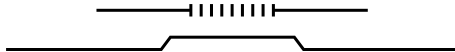


WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT VULNERABILITY IS THIS PAYLOAD USED FOR?

`${T(java.lang.System).getenv()}`



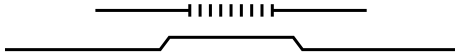
SSTI OR SERVER-SIDE TEMPLATE INJECTION



WEB APPLICATION AND API VULNERABILITY SCANNER



SQLMAP -D PARAMETER IS USED FOR:



SETTING THE DATABASE NAME



WEB APPLICATION AND API VULNERABILITY SCANNER



WHAT IS AWS METADATA IP:



1 6 9 . 2 5 4 . 1 6 9 . 2 5 4

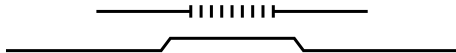


WEB APPLICATION AND API VULNERABILITY SCANNER

HARD



**HOW OLD CAN COOKIES BE BEFORE
THE SAMESITE LAX-ALLOWING-
UNSAFE ENFORCES THE LAX RULES?**



HARD

2 MINUTES

COOKIES NEWER THAN 2 MINUTES, CAN BE SENT ON REQUESTS CROSS-DOMAIN, JUST LIKE IN A SAMESITE=NONE SCENARIO. AFTER 2 MINUTES, THE LAX CONFIGURATION IS APPLIED.



WEB APPLICATION AND API VULNERABILITY SCANNER



**WHAT IS THE NAME OF THE FIRST
XSS WORM:**



S A M Y

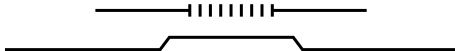
 **Probely**

WEB APPLICATION AND API VULNERABILITY SCANNER

HARD



WHAT DOES SBOM STANDS FOR?



HARD

SOFTWARE BILL OF MATERIALS.

SBOM'S ARE AN INVENTORY OF ALL THE
COMPONENTS OF A GIVEN SOFTWARE.



WEB APPLICATION AND API VULNERABILITY SCANNER



WILL THE ALERT EXECUTE?

```
GET /?NAME=<SCRIPT>ALERT(13)<%2FSCRIPT> HTTP/1.1
HOST: EXAMPLE.COM
```

```
HTTP/1.1 200 OK
DATE: THU, 06 APR 2023 21:53:38 GMT
CONTENT-SECURITY-POLICY: DEFAULT-SRC JS.EXAMPLE.COM;
X-CONTENT-TYPE-OPTIONS: NOSNIFF
X-FRAME-OPTIONS: DENY
X-XSS-PROTECTION: 1; MODE=BLOCK
REFERER: EXAMPLE.COM/?NAME=<SCRIPT>ALERT(13)<%2FSCRIPT>

<HTML><BODY><H1>HELLO <SCRIPT>ALERT(13)</SCRIPT></H1></BODY>
</HTML>
```

NO, BECAUSE THE CONTENT SECURITY
POLICY ONLY ALLOWS FOR JAVASCRIPT
FROM JS.EXAMPLE.COM

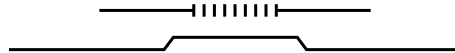


WEB APPLICATION AND API VULNERABILITY SCANNER

HARD



WHAT IS XKCD PASSWORD?



HARD

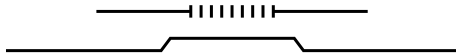
CORRECT HORSE BATTERY STAPLE
VISIT CHECK [HTTPS://XKCD.COM/936/](https://xkcd.com/936/) FOR
THE COMIC STRIP



WEB APPLICATION AND API VULNERABILITY SCANNER



**IN A SQL INJECTION PAYLOAD,
SPACES CAN BE REPLACED WITH?**



COMMENTS OR /**/



WEB APPLICATION AND API VULNERABILITY SCANNER

HARD



WHAT IS THE CVSS 3 RATING OF
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H?



HARD

9.8 OR CRITICAL



WEB APPLICATION AND API VULNERABILITY SCANNER

HARD



**WHAT IS THE E IN CVSS 3
TEMPORAL SCORE?**



HARD

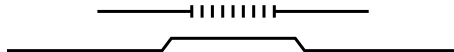
EXPLOIT CODE MATURITY



WEB APPLICATION AND API VULNERABILITY SCANNER



**THE “GOTO FAIL;” VULNERABILITY AFFECTED
WHICH FUNCTIONALITY?**



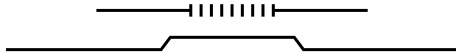
THE SIGNATURE VERIFICATION OF THE
SERVER KEY EXCHANGE IN THE SSL/TLS
PROTOCOL OF IOS DEVICES.



WEB APPLICATION AND API VULNERABILITY SCANNER



**LIST THE OWASP TOP 10 IN
ORDER, FROM A01 TO A10.**



A01 BROKEN ACCESS CONTROL
A02 CRYPTOGRAPHIC FAILURES
A03 INJECTION
A04 INSECURE DESIGN
A05 SECURITY MISCONFIGURATION
A06 VULNERABLE AND OUTDATED COMPONENTS
A07 IDENTIFICATION AND AUTHENTICATION FAILURES
A08 SOFTWARE AND DATA INTEGRITY FAILURES
A09 SECURITY LOGGING AND MONITORING FAILURES
A10 SERVER-SIDE REQUEST FORGERY (SSRF)



WEB APPLICATION AND API VULNERABILITY SCANNER