APPLICATION ETHICAL HACK

Scope guideline

Date: 25/04/2022

Do the below keywords ring a bell?

- Disrupted elections
- State-sponsored attacks
- Ransomware
- International bank heists

Most likely they do, as most of us have read about these in the past few months with the intensity and sophistication of cyber crimes on the rise. Here are some statistical data to help us understand the depth of what is at stake and how big a problem it is.

$10 trillion	$1.7 trillion	3.5 million	5 billion	$265 billion
Annual cyber crime damage costs by 2025	Cybersecurity spending by 2025	Unfilled cybersecurity jobs by 2022	People online worldwide in 2022	Predicted global ransomware damage by 2031

Regulatory authorities expect all companies small and big to do more to protect their systems and data, and now penalise them if there is evidence that enough steps were not taken by an organisation to prevent a hack which caused a data leak.

We at sapna security understand that

- Security can be daunting for both small and big companies
- Organisations may not know what they are expected to do
- Huge costs may keep them from conducting security audits

Accordingly sapna security attempts to offer security assistance at reasonable price to match your needs.

For application ethical hack we have a team which has experience over several years in web programming, database, network architecture, server hosting, security audits, and security testing. We use both automated and manual ethical penetration testing methods to give you the best results. Our Assessment approach, our findings will ensure you get a detailed idea of the issues. We will be available for help and discussions at each step. Our work does not stop only at report generation on findings, but we will offer 1 free retest of P1, P2, or P3 issues if completed within the recommended date as detailed in "Vulnerability threat category"

1. Our Assessment approach

The web application ethical hack includes the following areas:

- Injection
- Authentication
- Session Management
- Cross Site Scripting (XSS)
- Insecure Direct Object References
- Sensitive Data Exposure
- Access control
- Cross-Site Request Forgery (CSRF)
- Unvalidated Redirects and Forwards
- Input validation
- Cryptography

Since there is a limited window for test, every instance of a specific finding might not be uncovered. Eg if the assessor discovers SQL injection in a specific section, it may not uncover all the sections which are affected by it. Similarly it may be possible that some findings may be missed out because of the limited window and scope of the test. Accordingly “sapna security”/sapnagroup does not guarantee that it will find all vulnerabilities, and hence is not liable for such issues.

2. Our assessment findings and recommendations example

Below is a sample findings and recommendations chart.

No	Type	Issue	Vulnerability	Recommendations
1	P1	SQL injection	SQL construction is not correct and can allow a hacker to potentially get more sensitive information out by manipulating the parameters being sent url: https://sampledomain/account/login/ parameter: email	Raw user input should not be utilized in SQL construction. Prepared Statements should be used to prevent user input from altering the execution of the SQL query. Additionally, input filtering to remove unnecessary and potentially dangerous characters (<>;'"-), and output URL encoding to neutralize necessary but potentially dangerous characters, can be used to minimize the

				occurrence of SQL injection. See: https://www.sapnasecurity.com/common-vulnerabilities.html#SQL-injection
2	P2	XSS	Cross-site scripting (XSS) enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls. Url: https://sampledomain/trackorder/ Hack entry: /trackorder/1"%20sapnasecurity_xss_in_tag="58a0ee529d94f7b6e2865f2a8ee05786"%20blah="/ HTTP/1.1	Use proper encoding/escaping method to prevent XSS vulnerabilities. This includes eg using html encoding etc https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

3. Vulnerability threat category

Rating	Definition	Impact
Priority 1 (P1)	Issues that pose a clear and present danger to the confidentiality, availability and integrity of the system or data. Any existing mitigating controls are ineffective or insufficient. Includes readily exploitable issues that pose severe financial, brand image, or regulatory impact if discovered/exploited. Any issue that poses a direct and probable threat to the company's confidential information or customer NPI falls into this category.	For PRIORITY 1 vulnerabilities modifications, e.g. security patches, fixes, etc. MUST be deployed within 4 calendar days from date of Notification. Needs to be re-tested. Confirmation on deployment on live server needed.
Priority 2 (P2)	Issues that pose the highest and/or significant immediate risk to the confidentiality, availability and integrity	For PRIORITY 2 vulnerabilities modifications, e.g. security patches, fixes, etc. MUST be deployed

	of the system or data. Any existing mitigating controls are ineffective or insufficient. Includes readily exploitable issues that pose significant financial, brand image, or regulatory impact if discovered/exploited. Any issue that allows compromise of the infrastructure or allows anonymous access to authenticated systems fall into this category. Any issue that has a high probability of occurrence.	within 45 calendar days from date of notification. Needs to be re-tested. Confirmation on deployment on live server needed.
Priority 3 (P3)	Issues that pose a moderate risk to the confidentiality, availability and integrity of the system or data, and mitigating controls that are either nonexistent or ineffective. Includes readily exploitable issues that pose moderate business impact if discovered/exploited.	For PRIORITY 3 vulnerabilities modifications, e.g. security patches, fixes, etc. MUST be deployed within 100 calendar days from date of notification. Needs to be re-tested. Confirmation on deployment on live server needed.
Priority 4 (P4)	Issues that pose a low risk to the confidentiality, availability, and integrity of the system or data, but could make the application less safe or introduce a problem in the future. This includes potentially dangerous issues that are not directly exploitable. Includes readily exploitable issues that pose low business impact if discovered/exploited. Any issues that have existing effective mitigating controls.	For PRIORITY 4 vulnerabilities it is recommended that modifications, e.g. security patches, fixes, etc. may be remediated based on system maintenance schedules. No retest required
Priority 5 (P5)	Anomalous items that either do not pose apparent security risks to the confidentiality, availability and integrity of the Systems or data. These computing system vulnerabilities rated Priority 5 are provided for general improvement suggestions or simply to share information which may be of interest to the technology owners. Priority 5 advisories are not tracked or notified.	For Priority 5 vulnerabilities remediation is not required or monitored. No retest required

4. Next steps

If you have any P1, P2, P3 issues then the following sequence of events need to be undertaken

a. Vulnerability discussion: Vulnerability assessment team will go through the report with the client team to explain the issues, and answer any queries the client team might have.
b. Remediation: Remediation steps are necessary for all P1, P2 and P3 issues and remediation dates have been advised above. Client needs to get back on remediation plan including timelines so that these issues can be tested. Retesting request is a part of remediation stage and when getting back to us on retesting please clearly mention vulnerability number, Type (P1-P5), likely remediation date, and fix details (i.e. detailed description on how the issue was fixed) eg

   Vulnerability: 2
   Type: P1
   Remediation date: 15/10/2017
   Fix details: PDO was used to prevent MySQL injection and the parameter email was sent as a separate parameter

c. Retesting: Retesting will be conducted for all P1, P2 and P3 issues. As per the retest result the issues will be either closed, remain open, or reassigned another priority level.
d. Publishing to live: All successful retest issues have to be confirmed that they have been published to the live environment. A confirmation email is required from the client side indicating the exact date for fixing the issue on live environment.
e. Closing the assessment: The assessment will be closed after all P1, P2 and P3 issues have been resolved/closed successfully, and fixes for all these issues have been published to the live environment.
f. You can also hire us to perform a non intrusive security audit which includes, data classification, data flow diagram, network diagram, security fact finding questionnaire which checks for various security requirements like employee training to hardware firewall. Please contact us at info@sapnasecurity.com for more information.