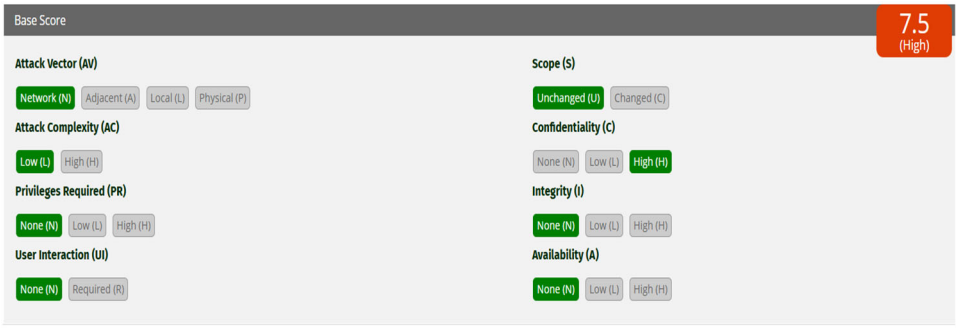
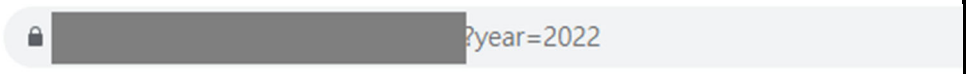
國家資通安全研究院
National Institute of Cyber Security

產品資安漏洞獵捕計畫活動
漏洞通報書

編號(主辦方填寫)：VR-R-1140922-01

基本資料	
姓名	王大明
常用暱稱	Ming
通報日期	114 年 12 月 17 日
標的資訊	
產品所屬公司	A 公司
產品名稱	無線路由器
產品型號	AA-123-456
測試使用 IP	162.120.2.3
漏洞類型	SQL Injection
漏洞成因	因管理者頁面未進行字元過濾，可進行注入攻擊
影響等級	□嚴重 ■高 □中 □低
CVSS 3.1 分數 (Base Score)	Base Score：__7.5__分 分數計算截圖(FIRST CVSS 計算機：https://www.first.org/cvss/calculator/3.1)： 

漏洞利用詳細步驟 (請自行增加長度，並附上必要截圖作為證據)	步驟 1：發現網址參數 year 圖片 1：  步驟 2：使用 SQLmap 工具進行攻擊，確認可執行注入攻擊。 指令：sqlmap -u "http://target.com/vuln.php?year=2022" --dbs 圖片 2：  步驟 3：進一步進行資料庫欄位內容獲取，可成功取得欄位儲存資料內容，但無法進行資料庫內容修改 圖片 3： 

漏洞利用使用工具	SQLmap
是否自行撰寫工具	□是，工具程式碼下載點為：_____ ■否
漏洞修補建議	
是否願意於廠商修補完成後協助進行複測	■是 □否

備註：

- 完成漏洞通報書後，請以約定密碼加密後寄送至指定信箱(bounty@nics.nat.gov.tw)。
- 信件大小超過 20MB 者，請分次寄送。
- 信件主旨須註明：「【產品資安漏洞獵捕計畫】OO 產品漏洞通報。